UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE DIREITO

MARI HELEN FLORIANO SERAFIM ALVES

A IMPLEMENTAÇÃO DE PONTOS DE INTERNET GRATUITOS NO MUNICÍPIO DE CRICIÚMA FRENTE AO REGIME JURÍDICO DO MARCO CIVIL DA INTERNET

CRICIÚMA

2017

MARI HELEN FLORIANO SERAFIM ALVES

A IMPLEMENTAÇÃO DE PONTOS DE INTERNET GRATUITOS NO MUNICÍPIO DE CRICIÚMA FRENTE AO REGIME JURÍDICO DO MARCO CIVIL DA INTERNET

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

Orientador: Prof. Mateus Back

CRICIÚMA

2017

MARI HELEN FLORIANO SERAFIM ALVES

A IMPLEMENTAÇÃO DE PONTOS DE INTERNET GRATUITOS NO MUNICÍPIO DE CRICIÚMA FRENTE AO REGIME JURÍDICO DO MARCO CIVIL DA INTERNET

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

Criciúma 28 de novembro de 2017

BANCA EXAMINADORA

Prof. Mateus Back – UNESC – Orientador

Prof. Leandro da Rosa – UNESC

Prof. Luiz Eduardo Conti – UNESC

Dedico esse trabalho primeiramente a Deus que me iluminou nesta caminhada, aos meus pais que me apoiaram durante toda a graduação, ao meu Marido que esteve comigo nos dias bons e ruins, me acolhendo em seus braços quando tudo parecia desandar. Amo vocês de todo meu coração. Nada faria sentido se eu não tivesse vocês em minha vida.

AGRADECIMENTOS

Já dizia Yoko Ono "Um sonho sonhado sozinho é um sonho. Um sonho sonhado junto é realidade''. Foram anos de conquistas dia após dia. Ingressar no ensino superior era uma realidade distante, mas foi possível graças a Deus que colocou pessoas maravilhosas em meu caminho para sonhar o meu sonho e me ajudou a realizá-lo.

Primeiramente agradeço a Deus de todo o meu coração por tudo que me proporcionou nesses últimos 5 anos, agradeço pelas derrotas e pelas vitórias, pois tiro disso tudo os mais belos ensinamentos.

Agradeço também aos meus pais que me incentivaram dia a dia, essa graduação está sendo concluída porque eu tinha uma dívida com vocês, em honrar e respeitar por toda minha vida e proporcionar o primeiro ingresso da família a um curso superior, meu diploma é de vocês.

Agradeço a minhas irmãs e meu irmão que me apoiaram, cada um a seu modo, mas me ajudaram de uma forma especial. Aos meus sobrinhos, que tanto amo, e que tem por um mim sentimento puro e recíproco. Agradeço aos pais de meu Marido, meu sogro e minha sogra que me apoiaram e sempre tiveram uma palavra de carinho comigo nesses últimos anos.

Aos meus amigos de trabalho, que compreenderam a minha falta na empresa nos últimos dias, e também, me deram um apoio fundamental em atitudes e em palavras.

Agradeço aos meus professores maravilhosos do Curso de Direito da UNESC, sem exceção, todos me ensinaram muito, inclusive a ser uma pessoa melhor.

Agradeço em especial ao meu Orientador, Professor Mateus Back, que foi surpreendido, assim como eu, com a minha orientação aos 45 do segundo tempo (risos). Obrigado Professor pelo incentivo e paciência comigo e com a minha vida corrida e também ao professor Maurício Filó, que me acompanhou no início do projeto.

Aos meus amigos, colegas de sala de aula, uns mais chegados, outros nem tanto, mas, uma família que formamos nos últimos 5 anos, sorrimos e choramos

juntos e eu tenho certeza que crescemos muito. Serei grata para sempre por esse tempo de aprendizado com vocês.

Em especial e com lágrimas nos olhos, agradeço ao meu Amor, o mais lindo da vida, meu marido, aquele que nos últimos dias me consolou sabendo que eu já não aguentava mais a pressão do TCC, provas, OAB, estágio e trabalho. Obrigada, amor, por renunciar a tua vida para viver a minha nesse último ano. Obrigada por estudar comigo, obrigada por compreender que as vezes eu não consigo realizar todas as tarefas sozinha, obrigada por cobrar de mim notas boas, obrigada pelo incentivo em tudo, com toda certeza esse meu diploma é metade seu (risos). És meu presente mais precioso e é por você que concluo essa graduação.

Todos vocês de uma forma especial contribuíram para que eu pudesse realizar o meu sonho e é por isso que dedico esse trabalho a vocês. Obrigada a todos. Amo-os.

“[…] fundamental que os operadores das ciências criminais tenham (cons)ciência de que os riscos da sociedade pós-industrial (riscos catastróficos e imensuráveis) estão para além da capacidade de controle penal, e que a era da segurança (jurídica) foi soterrada pelo próprio projeto que a construiu: a Modernidade.”
(Salo de Carvalho)

RESUMO

A presente pesquisa consiste na apresentação das características do uso da internet em pontos públicos disponibilizados pelo município de Criciúma. Locais onde não há fiscalização apropriada podem estar propensos a crimes digitais. Dispõe o Marco Civil a respeito da obrigatoriedade dos provedores de conexão e aplicação a internet em guardar os *Logs* de acesso de cada usuário através de um IP individual para uma possível investigação em caso de *cybercrimes*. Entretanto a lei apresenta-se obscura no que tange a responsabilidade do compartilhamento do IP de acesso à internet via Wi-Fi. A problemática do tema é na investigação dos crimes cometidos pela internet, pois em casos de compartilhamento, há uma dificuldade na investigação. O que se busca com o referido trabalho é localizar a responsabilidade do compartilhamento de Wi-Fi em pontos públicos. A vulnerabilidade da internet compartilhada é alta, diante disso, a pesquisa tem por objetivo esclarecer a respeito da responsabilidade do Município em caso de crimes cometidos pela internet. O método de pesquisa utilizado foi dedutivo em pesquisa teórica e qualitativo com os entendimentos jurisprudenciais acerca dos crimes cometidos pela internet e da responsabilidade e obrigatoriedade do provedor de internet armazenar os *Logs* de acesso e conexão de cada usuário.

Palavras-chave: Marco Civil da Internet. Responsabilidade. Provedores. Usuário. Cybercrimes.

ABSTRACT

The present research consists in the presentation of the characteristics of the use of the internet in public places made available by the municipality of Criciúma. Places where there is no proper enforcement may be prone to digital crime. It provides the Civil Registry regarding the obligatoriness of the connection providers and application to the internet in storing the Logs of access of each user through an individual IP for a possible investigation in case of cybercrimes. However, the law is obscure regarding the responsibility of sharing the Internet access IP via Wi-Fi. The major problem of the subject is in the investigation of the crimes committed by the Internet, because in cases of sharing there is a difficulty in the investigation. The aim of this work is to locate the responsibility of sharing WI-FI in public places. The vulnerability of the shared internet is high, in front of this, the research aims to clarify about the responsibility of the Municipality in case of crimes committed by the internet. The research method used was deductive in theoretical and qualitative research with the jurisprudential understandings about the crimes committed by the internet and the responsibility and obligation of the internet provider to store the Logs of access and connection of each user.

Keywords: Civil Internet Framework. Responsibility. Providers. User. Cybercrimes

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ANATEL	Agência Nacional de Telecomunicações
ARPANET	Advanced Research Projects Agency Network
AS	Sistema Autônomo
CERT	Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores
CGI	Centro Gestor da Internet
CNPJ	Cadastro Nacional de Pessoa Jurídica
CPF	Cadastro de Pessoas Físicas
DDOS	Distributed Denial of Service
ECA	Estatuto da Criança e do Adolescente
e-PROC	Sistema de Transmissão Eletrônica de Atos Processuais da Justiça Federal Online
e-SAJ	Sistema de Automação da Justiça Online
FAPESP	Fundação de Amparo à Pesquisa do Estado de São Paulo
IFSC	Instituto Federal de Santa Catarina
IP	Internet Protocol
ONU	Organização das Nações Unidas
PL	Projeto de Lei
PROCON	Programa de Proteção e Defesa do Consumidor
SAGE	Sistema de Apoio à Gestão
SCM	Supply Chain Management
SSID	Service Set Identifier
STF	Superior Tribunal Federal
STJ	Superior Tribunal de Justiça

TCP	Transmission Control Protocol
TI	Tecnologia da Informação
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity

SUMÁRIO

1 INTRODUÇÃO

O acesso à internet teve início na era da Guerra Fria, sua função principal era a troca de informações e seu uso era estritamente militar. Passados os anos, o crescimento tecnológico avançou e com isso a internet passou a fazer parte do cotidiano. Há inúmeras funcionalidades promovidas pela internet, a comunicação é ágil, independentemente da distância entre os usuários.

Apesar dos benefícios promovidos pela rede mundial de internet, riscos são rotineiramente proporcionados aos usuários. Sendo eles contra as pessoas, destruindo vidas e contra sistemas causando *cyberguerras.*

Com base no crescimento exponencial da internet, criou-se a necessidade de delimitar direitos e deveres dos usuários. Partindo disso, no Brasil, no ano de 2014, surgiu o Marco Civil com o objetivo de regulamentar o acesso a internet, os direitos e os deveres de cada usuário da rede.

A lei n 12.965 de 23 de abril de 2014 regulamenta o uso da internet dispondo a respeito da privacidade do usuário, da neutralidade da rede, da liberdade de expressão, que são fundamentados como os princípios básicos do acesso à internet no Brasil. Outrossim, em seus dispositivos o Marco Civil traz a obrigatoriedade do armazenamento de *Logs* de cada usuário, para fins de investigação e responsabilização no caso de ilícitos cometidos pela internet.

O objetivo deste trabalho subdivide-se em geral e específico. Na forma geral, delimita-se o tema na historicidade da evolução da internet no mundo e no desenvolvimento de projetos de lei bem como as normas existentes que regulamentam o acesso do usuário.

Como objetivo específico o estudo do tema traz os crimes cometidos pela internet e a vulnerabilidade do Marco Civil analisado na forma técnica no âmbito de TI, no que se refere aos armazenamentos de IP, e a conexão WI-FI na proteção do usuário no acesso à internet em locais públicos onde não há como identificar o delituoso.

Os métodos utilizados no estudo do tema foram o dedutivo, e qualitativo. O primeiro no que se refere a pesquisa teórica, tanto em nível de

legislação, em nível de histórico e em análise da tecnologia da internet, na finalidade de esclarecer a respeito do fundamento do IP, que passa a ser o principal objeto de estudo no tema, pois através dele se dá a identificação de cada usuário na rede mundial de internet.

Na forma qualitativa, o tema traz em pauta análises de crimes em entendimentos de jurisprudências atuais aduzidas por nossos tribunais superiores.

No primeiro capítulo discorre-se a respeito da evolução tecnológica que se desenvolveu entre o século passado e o século atual. Inicialmente a internet tinha fins militares e poucas universidades possuíam o direito de uso para promover pesquisas de âmbito acadêmico. Com o passar dos anos surgiu a comutação de pacotes promovendo o acesso facilitado aos usuários através de ligações ponto a ponto via *Backbones* de grandes desenvolvedores de internet via satélite.

O segundo capítulo traz como pauta o desenvolvimento dos crimes cometidos pela internet. O Código Penal Brasileiro tem como dispositivos penas para cada crime cometido, entretanto não há legislação em vigor que pleiteie penas para os crimes da internet, o que na prática se aplica as penas previstas nos crimes no âmbito do Código Penal Brasileiro. Subdivide-se o segundo capítulo em crimes contra a honra, sendo especificados como de calúnia, injúria e difamação; crimes contra o patrimônio, sendo o furto mediante fraude, a receptação, a extorsão e estelionato; crimes de dano, sendo a violação de sistema, ataques a banco de dados e terrorismo; crimes sexuais, sendo a pedofilia, a pornografia infantil e a vingança pornográfica; e os perfis falsos, que são basicamente os meios onde todos os crimes acontecem, pois o criminoso da internet dificilmente mostra seu rosto.

No terceiro capítulo enfrenta-se a problemática da competência do órgão que possa julgar cada crime cometido pela internet e adentra-se ao ponto principal do tema que é a implementação de pontos de internet pelo município de Criciúma, onde há locais que possuem a disponibilidade de pontos públicos de internet espalhados para a população. Provedores de internet tem o dever estabelecido pelo Marco Civil em armazenar os dados de *Logs* IP de cada usuário, isso se dá porque cada conexão é identificada por um protocolo, assim, quando há uma conexão via internet de um determinado

ponto, tudo que o usuário fizer ficará armazenado. No que tange aos pontos públicos, o IP identificador é o da base onde direciona o sinal para a rede *wireless,* que pode ser segura caso haja identificação de cada usuário que irá dispor da rede Wi-Fi cadastrada.

A inclusão digital traz a necessidade de os governos disponibilizarem internet à população em locais onde há um grande fluxo de pessoas. Contudo, para a implementação de internet em pontos públicos, é necessário que haja medidas para assegurar a segurança na conexão.

2 A HISTÓRIA DA REDE MUNDIAL DE INTERNET

A tecnologia está presente no desenvolvimento humano. Isso se demonstra nas relações pessoais e profissionais. Máquinas são projetadas para serem utilizadas no campo, na pesca, na indústria e para a substituição da mão de obra humana. Atualmente sistemas são projetados e utilizados em universidades, hospitais e até mesmo no judiciário através da internet. O avanço tecnológico atual implica nos relacionamentos e a internet possuí uma grande importância nisso. Com intuito de pesquisa e ação militar, surgiu as redes de comutação de dados, que transmitia informações o que alavancou a era digital.

2.1 A REVOLUÇÃO DA REDE COMO ASPECTO MILITAR E O SURGIMENTO DAS CONEXÕES TCP/IP

O uso da internet atualmente está elencado como um princípio básico da necessidade humana. Atualmente a rede informatizada está presente em todas as áreas da vida comum, mas, poucos sabem quando, onde e porque surgiu o uso de pacotes dados que transportava informações.

Em sua dissertação, Carvalho (2006), corrobora que no período da Guerra fria foi iniciada a sistemática de dados, onde os informatizava. Os Estados Unidos investiram suas pesquisas incessantemente para o desenvolvimento da tecnologia de computadores a fim de buscar segurança contra-ataques de países inimigos nas guerras. Criaram um sistema denominado como *Semi Automatic Groud Environment (SAGE)*, que foi um meio de investigação de rotas de ataques inimigos. Com o SAGE, vieram as inovações tecnológicas como o software, a computação gráfica, o transporte de dados por linhas telefônicas, dentre outras tecnologias abrangentes da época.

> A Força Aérea dos Estados Unidos, impulsionada pela repercussão da explosão da primeira bomba de hidrogênio soviética em 1953, deu início, no Laboratório Lincoln, a um projeto ambicioso chamado *Semi-Automatic Ground Environment* (SAGE).
> I para criação e implantação de um sistema de defesa contra aviões bombardeiros de inimigos. Esse sistema operava de maneira distribuída por vinte e três centros de processamento de dados

> instalados em *bunkers* gigantescos, cada qual contendo dois computadores de grande porte.
> II O sistema processava informações oriundas de milhares de radares, calculava rotas aéreas e comparava com dados armazenados para viabilizar tomada de decisões, que, de forma rápida e confiável, viabilizassem a defesa contra aviões bombardeiros, carregados de artefatos nucleares altamente destrutivos. Seu primeiro computador foi instalado em 1957 e o último em 1961, todos interligados entre si através de linhas telefônicas (CARVALHO, 2006).

Segundo Carvalho, posteriormente, foi criado nos Estados Unidos o departamento de *Advanced Research Projects Agency* Network (ARPANET), que servia para administrar computadores a base de comutação de pacotes. Neste período, alguns países começaram a implementar a sistemática informatizada, lançando pequenos projetos de redes computadorizadas, e sentiu-se a necessidade de melhorar a transmissão de dados para a informação imediata. Diante disso criou-se a comutação de pacotes imediatos, que servia para informar instantaneamente um possível ataque ao país. O foco da criação de redes informatizadas era para exercer funções militares (CARVALHO, 2006, p. 27).

Historicamente as atividades computadorizadas existiam apenas em universidades, órgãos públicos e militares na era da Guerra Fria. Após o início das atividades da ARPANET, os órgãos militares iniciaram uma medida para melhorar a segurança da informação via comutação de pacotes. Partindo disso, criou-se a transmissão de rádio via TCP/IP que proporcionou uma divisão entre uma rede militarizada, utilizada para fins militares e uma rede civil/comercial, para pesquisas e estudos universitários.

Em um periódico da Folha de São Paulo, Leonardo Werner da Silva, corrobora que no ano de 1969 foi criada a internet através do uso de dados em transmissão através da ARPANET. Neste sentido, a intercomunicação era restrita a universidades e órgãos militares. Sua função era interligar laboratórios de pesquisas (SILVA, 2001).

No ano de 1987 foi liberado o uso comercial da rede de internet através de protocolos de TCP/IP, que são um conjunto de protocolos para comunicação entre computadores. Segundo Spancer Sydow, o TCP/IP ‘’nada mais é do que uma série de mecanismos desenvolvidos para interconectar e compartilhar dispositivos através das redes’’ (SYDOW, 2015, p. 29)

O TCP/IP funciona como um correspondente de informações, através de um *modem* que distribui mensagens e arquivos instantâneos.

Nesse sentido, Marcel Leonardi explana que:

> O Protocolo de Controle de Transmissão (TCP) divide os dados a serem transmitidos em pequenos pedaços chamados de pacotes e, após efetuar a transmissão, reúne-os para formar novamente os dados originalmente transmitidos. O Protocolo de Internet (IP) adiciona a cada pacote de dados o endereço do destinatário, de forma que eles alcancem o destino correto. Cada computador ou roteador participante do processo de transmissão de dados utiliza o endereço constante dos pacotes, de forma a saber para onde encaminhar a mensagem.
> [...]. Os pacotes e dados contêm os endereços IP do remetente e do destinatário dos dados. Um endereço IP identifica determinada conexão à Internet em um determinado momento. Toda vez que um usuário se conecta à rede, seu computador recebe automaticamente de seu provedor de acesso um endereço IP que é único durante aquela conexão. Sem conhecer tal endereço IP, um pacote de dados não tem como chegar a seu destino (LEONARDi, 2012, p. 80-81).

Para se interligar a rede de computadores é necessário um protocolo de IP que o conecte na rede e faça enlaces com o *backbone*, que é o local que armazena todas as informações da rede de dados via rádio ou cabo e as envia. Nesse sentido:

> [...] a rede passou a ser um ambiente de intercomunicação (mediata e imediata), de relacionamento, de pesquisas, de troca de informações, programas, arquivo, multimídia, de divulgação de produtos, de autopromoção, enfim, uma verdadeira ferramenta de comunicação, interação, criação transformação e busca [...] (SYDOW, 2015, p. 21).

Com a implementação dos protocolos TCP/IP, diversas informações eram repassadas instantaneamente aos usuários, o que gerou um avanço tecnológico mundial. A ideia da interconexão imediata transformou a informação e a vida das pessoas. As universidades poderiam obter um avanço ainda maior em suas pesquisas, as pessoas poderiam se comunicar instantaneamente entre si independentemente do local e horário em que estavam.

No Brasil o uso por conexão internacional via internet deu-se em meados de 1989, através da FAPESP, Fundação de Amparo à Pesquisa do Estado de São Paulo. Atualmente são cerca de 117 milhões de usuários de

internet no Brasil (BARRETO & BRASIL, 2016, p. 5-6). Um número em constante crescimento.

2.2 A INFORMAÇÃO IMEDIATA E A DEPENDÊNCIA DO USO DA INTERNET

A internet no século atual tem sido a principal ferramenta de comunicação mundial. A sociedade globalizada está cada vez mais dependente do mundo digital, sejam para compras, informações, relacionamentos ou viagens. A rede cibernética une pessoas de diferentes regiões em uma única esfera, o mundo digital. Segundo Barreto e Brasil:

> A revolução tecnológica, que ainda está em curso, não só no Brasil, como em todo mundo, tem como características principais a diminuição das distancias, com a extinção das fronteiras no mundo virtual; a multiplicidade de receptores, já que a informação pode atingir milhões de pessoas; e a instantaneidade, ou seja, tudo pode ser transmitido em tempo real (*online*) (BARRETO & BRASIL, 2016, p. 5-6).

O crescimento exponencial do uso da internet tem pontos positivos onde possibilita inúmeros benefícios aos usuários. Atualmente vivemos na era do conhecimento. A informação está diretamente ligada a conexão à internet. A tecnologia permite o compartilhamento de informações em segundos, o que nos faz cada vez mais dependentes do mundo virtual.

Para Barreto e Brasil, a supervalorização da informação e do conhecimento avança com a necessidade de regulamentação jurídica das novas relações advindas (BARRETO & BRASIL, 2016, p. 6).

Crianças de 5 (cinco) anos possuem dispositivos ligados a internet e esse é o meio de diversão. Adolescentes de 15 (quinze) anos já utilizam redes sociais constantemente. Adultos estão conectados às informações diariamente.

Os conteúdos utilizados na internet atendem a esfera cultural e econômica e contribuem para o enriquecimento e desenvolvimento do mercado. Partindo desse contexto, Neto, Santos e Gimenes corroboram que atualmente os computadores fazem parte da maioria dos afazeres das pessoas, tornando-as dependentes. A venda de passagens aéreas, a compra em um supermercado ou até mesmo a contabilização das atividades realizadas

em uma instituição bancária, estão sendo feitas online através da internet (NETO, SANTOS & GIMENES, 2012, p. 13).

Spencer Sydow contribui aduzindo que a tecnologia toma espaço na vida do cidadão, tornando-se fundamental que o usuário da internet esteja apto a adquirir conhecimento para lidar com as modernidades (SYDOW, 2015, p. 20).

Apesar das inúmeras versatilidades com o uso da internet, há um evidente número de riscos que os usuários estão sendo expostos no mundo virtual. Algumas autoridades mundiais estão em alerta sobre os problemas enfrentados no que tange a segurança da rede. Atualmente há escolas policiais pelo mundo que estão habilitandos profissionais para a investigação de crimes cometidos pela internet.

> The increasing use of technology and the Internet in all aspects of daily life puts everyday citizens at risk of becoming targets of cybercriminals.
> As society comes to rely more and more on the Internet, the dangers posed by different types of cybercrime have become very real threats. These threats come in a variety of forms and target different features of the Internet, technological devices and their users.
> Cyberthreats are constantly evolving and changing, therefore the types of threats outlined here should not be considered as an exhaustive or absolute list. See our advice on how to stay safe online.
> In addition to the threats posed by cybercrime itself, cyber-enabled crimes such as financial crime, crimes against children and fraud also pose distinct threats to the public (INTERPOL, 2017).[1]

Assim, há um alerta no que tange a segurança de uma possível falta de controle para identificar usuários que cometem atividades criminosas. A identificação de um criminoso virtual é um trabalho delicado que envolve autarquias, entes de segurança e a sociedade em geral.

---

[1] O crescente uso da tecnologia e da Internet em todos os aspectos do cotidiano coloca os cidadãos todos os dias em risco de ser alvo de *cibercriminosos*.
A medida que a sociedade vem confiar cada vez mais na Internet, os perigos colocados por diferentes tipos de *cibercrimes* tornaram-se ameaças muito mais reais. Essas ameaças vêm em uma variedade de formas e segmentam diferentes recursos da Internet, dispositivos tecnológicos e seus usuários.
As ameaças cibernéticas estão em constante evolução e mudança, portanto, os tipos de ameaças aqui descritos não devem ser considerados como uma lista exaustiva ou absoluta (Tradução nossa).

Para Barreto e Brasil, é preocupante a situação de *cibercrimes* no Brasil, pois há uma alta taxa de lucratividade nas relações criminosas no campo virtual, isso porque as leis ainda não são tão severas, o que contribui para a impunidade dos atos criminosos cometidos via internet (BARRETO & BRASIL, 2016, p. 16).

O uso exacerbado da internet ocasiona medidas a serem tomadas pelos legisladores. Leis no mundo todo estão sendo aplicadas, para que hajam medidas em possíveis infrações ou crimes. Há um preocupante crescimento no número de atos terroristas e crimes em geral cometidos pela internet. No Brasil alguns projetos de lei já foram implementados, dentre eles, o Marco Civil da Internet, que define medidas, direitos e impõe deveres aos indivíduos na esfera virtual.

2.3 A EVOLUÇÃO DOS CRIMES DIGITAIS E OS PROJETOS DE LEI ANTERIORES AO MARCO CIVIL DA INTERNET

Com o crescimento das relações em ambiente virtual, crimes digitais passam a ser cometidos com mais frequência. Os crimes informáticos ou tecnológicos em suma são os que necessitam de um meio digital para a sua consumação. Nesse sentido Barreto e Brasil conceituam os crimes tecnológicos como

> Aqueles que envolvem o uso de tecnologias (computador, internet, caixas eletrônicos) sendo, em regra, crimes meios -ou seja, apenas a forma em que são praticados é que é inovadora. Têm como subespécie os crimes virtuais, informáticos ou cibernéticos (praticados pela internet), onde, apesar de se concretizarem em ambientes virtuais os delitos trazem efeitos no mundo real (BARRETO & BRASIL, 2016, p. 16).

Partindo desse pressuposto, entende-se por crime digital todo ato ilícito que traz dano a outrem, onde seu início e fim se dão através de meios eletrônicos, e em sua maioria por meio de internet. Pode-se complementar como crime digital os *cibercrimes,* os crimes telemáticos, os crimes em caixas eletrônicos, crimes eletrônicos entre outros que abrangem todo meio digital e tecnológico.

Segundo Barreto e Brasil, os crimes digitais podem ser diferenciados como próprios, que são os crimes onde ataca-se banco de dados para acesso a informações através de softwares maliciosos que infectam o dispositivo da vítima em busca de dados; e, impróprios, que são aqueles onde se utiliza uma rede de interação com a vítima. Nesse sentido, podemos exemplificar as redes sociais como um meio de crimes digital impróprio (BARRETO & BRASIL, 2016, p. 18-19).

Em outras palavras, tem-se por crime digital próprio aquele que é cometido para infringir sistemas de comunicação. Os ataques de *Hackers* por exemplo. Aqui, o ato criminoso afeta apenas o computador, ataca-se o sistema para destruir informações ou derrubar protocolos. Já os crimes digitais impróprios são aqueles que o infrator utiliza-se de um meio digital para cometer um dano a outrem, a exemplo disso temos a divulgação de material pornográfico. Nesse sentido, o ato é cometido através do computador para afetar diretamente a vítima.

Antonio Heli Mazoni Saraiva colabora com o tema aduzindo a respeito dos tipos de crimes digitais próprios e impróprios.

> No primeiro caso, temos o crime de informática propriamente dito, sendo o computador o meio de execução e o alvo, podendo ser objetos de tais condutas o computador, seus periféricos, os dados ou o suporte lógico da máquina e as informações contidas em sua memória de armazenamento. No segundo caso, o computador é apenas o meio de execução, para que se consiga o resultado-crime, sendo as práticas ilícitas de natureza patrimonial as mais comuns nesta espécie, principalmente as que atenta, contra o direito de autor, o patrimônio financeiro e a liberdade individual (SARAIVA, 2010, p. 20).

Neste sentido, temos como crimes contra o sistema de informação, os crimes impróprios, que são aqueles que invadem os dados de uma máquina a fim de obter informações sobre determinada conta bancária ou até mesmo de softwares de empresas que destroem arquivos confidenciais e, para exemplificar os crimes cometidos através de um sistema, são os crimes próprios, podemos citar a calúnia ou injúria cometida contra alguém em rede social.

No âmbito Nacional diversos projetos de lei foram iniciados a fim de combater os crimes digitais, porém, é importante frisar que há uma convenção

ao qual o Brasil não é signatário, onde estabelece aspectos e dispositivos acerca dos c*ibercrimes,* e que poderia dar um impulso ainda maior no que tange as investigações dos crimes digitais no Brasil.

A Convenção de Budapeste foi iniciada no ano de 2001, tendo como seu principal objetivo a proteção da sociedade contra riscos promovidos pela internet, através da cooperação internacional de países signatários a ela (MAZONI, 2010, p. 31).

20 países aderiram a Convenção de Budapeste a fim de combater a criminalidade virtual através de leis próprias e severas no ciberespaço. O Brasil não estava entre os países signatários a Convenção e para poder aderir a ela teria que ser convidado pelos países participantes, o que até o momento não ocorreu.

Apesar disso, surgiu em nosso ordenamento alguns projetos de lei que combatem a criminalidade virtual, tendo como escopo inicial a Constituição Federal e o Código Penal Brasileiro, contudo, há de se mencionar, que se o Brasil estivesse entre os 20 países participantes da Convenção de Budapeste, o processo de leis mais severas para criminalizar os delitos virtuais seria mais célere.

O acesso à internet possibilita ao usuário o livre acesso a informação e está garantido na Carta Magna Brasileira da Constituição Federal de 1988, onde dispõe em seu artigo 5º, IX que “[...] é livre a expressão da atividade intelectual, artística, científica e de comunicação, independente de censura ou licença” (BRASIL, 2017a).

Nesse sentido Neto Monteiro preceitua que

> O direito à informação é um direito fundamental do homem, de forma que está vinculada à democracia moderna. A implantação dos demais direitos se materializa a partir da garantia constitucional da liberdade de informação. Mormente, é importante salientar que a ordem jurídica constitucional brasileira reservou em seu texto pétreo um Título destinado aos direitos e garantias fundamentais, ligados à ideia de pessoa humana e seus atributos de personalidade, como a liberdade, por exemplo, não podendo, o titular de tais direitos, dispor deles (NETO, 2008, p. 57-60).

Os usuários possuem garantidos o livre acesso a todas informações contidas no mundo digital. Diante disso, criou-se a necessidade de

regulamentar através de lei os direitos, que já estão em parte garantidos na Constituição, e os deveres ou obrigações de cada indivíduo no mundo virtual.

> A Constituição da República Federativa do Brasil, de 1988, prevê em diversos de seus dispositivos, princípios e garantias do uso da tecnologia pelos cidadãos em suas mais diversas relações e para o desenvolvimento do país (atrs. 1º, 3º, 4º, 5º, 6º, 215, 218, 219, 220, etc.), visando garantir a liberdade e os direitos fundamentais dos indivíduos no *ciberespaço*, permitindo-lhes participação democrática nele e fora dele (BARRETO & BRASIL, 2016, p. 6).

A regulamentação do acesso à internet traz vários pontos a serem analisados pelos legisladores, dentre eles o acesso aos dados particulares de terceiros, a invasão da privacidade, a disseminação de vírus e materiais ofensivos.

Segundo Monteiro Neto, a informação através da internet para a sociedade surgiu através de atividades de uso informatizadas, sejam dispositivos móveis, computadores dentre outros mecanismos eletrônicos. Nessas atividades informatizadas há muitos bens jurídicos a serem cuidados, como a saúde e a intimidade. Isso faz com que a sociedade se vincule cada vez mais as tecnologias da informação, necessitado assim, de um cuidado maior do Estado (NETO, 2008, p. 06).

No Brasil surgiram inicialmente alguns projetos com intuito de regulamentar a internet. O primeiro projeto surgiu em 1999. A proposta era conhecida como a PL 84/99, a PL dos Crimes Digitais, que caracterizava os ataques praticados por *hackers* como crimes informáticos ou crimes virtuais. O projeto de lei dispunha “como crime informático ou virtual os ataques praticados por *hackers* [2]e *crackers*[3], em especial as alterações de *home pages*[4] e a utilização indevida de senhas” (BRASIL, 2017c).

O segundo projeto de lei foi proposto em 2000, a PL 151/00, estabelecia a guarda dos registros de conexão de cada usuário na internet. Em 2003 surgiu um novo projeto e em 2008 ele sofreu uma alteração, onde considerava-se crime digital a alteração de senhas, a disseminação de vírus e

[2] Denomina-se HACKER aquele que possui condutas capaz de desenvolver ou modificar softwares e hardwares de computadores.
[3] Denomina-se CRACKER aquele que invade sistemas de segurança com intuito de destruí-los.
[4] Home Page é a sigla em inglês que denomina a página inicial da internet, que dá acesso ao site e todo seu conteúdo

a invasão de privacidade, assunto que ganhou destaque após o incidente com a atriz Carolina Dieckmann, que sofreu com a divulgação de fotos particulares sem seu consentimento. Invasores adentraram em sua conta de e-mail hackeando-a e publicando fotos contidas em sua conta em sites de conteúdo pornográfico. Esse fato deu repercussão nacional e dele surgiu um novo projeto de lei, a PL 2.793/11 que posteriormente, em 2012, foi aprovado na câmara.

> A atriz Carolina Dieckmann sofreu com um crime cibernético, onde 36 fotos íntimas suas vazaram e foram parar na internet, fazendo com que essas fotos chegassem a diversos locais e vistas por qualquer pessoa com acesso a internet. A lei levou como apelido o nome da atriz e prevê pena de seis meses até dois anos de reclusão em casos de invasão de privacidade e principalmente, que envolvem comunicações, conversas privadas e segredos comerciais e/ou industriais (DIÁRIO OFICIAL DA UNIÃO, 2016)

Após a aprovação da Lei dos crimes virtuais ocorreram vários embates a respeito da criminalização na internet. O resultado destes questionamentos foi a iniciativa do Ministério da Justiça em propor uma nova regulamentação da internet, discorrendo a respeito de direitos e deveres dos usuários da rede virtual.

2.4 A REGULAMENTAÇÃO DO MARCO CIVIL, OS DIREITOS E OBRIGAÇÕES DE USUÁRIOS E TERCEIROS

O Marco Civil da internet foi sancionado no ano de 2014 trazendo o acesso à internet como uma garantia essencial a qualquer cidadão, como dispõe o artigo 7º ‘’ [...] O acesso à internet é essencial ao exercício da cidadania’’ (BRASIL, 2014). O direito à informação estabelece aos usuários, limites que envolvem a segurança e são geridos pelo Marco Civil. Da mesma forma que a lei garante direito ao uso da internet, ela também determina deveres a serem cumpridos pelos usuários e também terceiros no que pulsa a esfera comercial da internet. Nesse sentido Barreto e Brasil corroboram que:

> O projeto do Marco Civil da Internet foi iniciado com a parceria da Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL-MJ)

> e a fundação Getúlio Vargas, através do Centro de Tecnologia e Sociedade da Escola de Direito.
> Desde o início a proposta visou a garantia de direitos e não a restrição de liberdades. (BARRETO & BRASIL, 2016, p. 9).

A iniciativa de regulamentação da Lei n° 12.965/14 foi do Ministério da Justiça, que sentiu a necessidade de regular ainda mais as garantias aos usuários da internet no Brasil. Além dos direitos e garantias, o Marco Civil também inseriu uma força no que tange as necessidades de investigação no caso de crimes cibernéticos. Aliado ao Código Penal Brasileiro, as medidas estabelecidas pelo Marco Civil abrangem a responsabilização dos pelos atos ilícitos praticados pelos usuários da internet.

Neste sentido, de acordo com Barreto e Brasil, como fundamento, o Marco Civil abrange a regulamentação das relações no ambiente virtual com a preservação e o respeito da liberdade de expressão (BARRETO & BRASIL, 2016, p. 10).

Os princípios que norteiam a Lei n° 12.965/14 são: a) a garantia à liberdade de expressão; b) a proteção à privacidade; c) a proteção dos dados pessoais; d) a neutralidade da rede; e) a preservação da estabilidade, segurança e funcionalidade da rede; f) a responsabilização dos atos praticados pela internet; g) a preservação da natureza participativa da rede e; h) a liberdade dos negócios promovidos pela rede (BRASIL, 2017b).

Pode-se dizer que o Marco Civil estabelece vieses de princípios. No primeiro viés, estabelece a proteção ao usuário de internet, onde visa que este tenha garantida a sua liberdade de pensamento para dispor sobre assuntos e opiniões públicas, desde que não ofendam a integridade de terceiros. Vale ressaltar que a garantia da liberdade de expressão determina que os conteúdos publicados só sejam retirados mediante autorização de quem os escreveu, o que cada usuário expressa em rede é personalíssimo, não podendo o provedor de acesso remover, exceto por determinação judicial. Nessa linha de proteção ao usuário, o Marco Civil estabelece ainda proteção aos dados pessoais e a proteção à privacidade, onde determina que os provedores devem ter os dados de seus clientes e não podem usá-los para fins comerciais. Igualmente, os provedores devem guardar os acessos de seus usuários por um período, para fins judiciais, caso ocorram. O ponto principal

desse princípio é a guarda dos *Logs*, sendo ele obrigatório para empresas nacionais ou internacionais que tenham seus datacenters no Brasil. Para Spencer Sydow, a lei busca atribuição a margens seguras para deveres e responsabilidades – no caso concreto, aos usuários e aos prestadores de serviço na internet (SYDOW, 2015, p. 274).

Outrossim, o Marco Civil adentra na esfera consumerista, estabelecendo que a rede de internet seja segura e que mantenha sua funcionalidade de acordo com o que contrata o consumidor. Nesse sentido, a lei firma ainda mais a obrigatoriedade de um relacionamento entre o provedor de internet e o consumidor seja claro, neutro e tenha a proteção necessária aos dados de cada usuário e que seja garantida a cada um a estabilidade da rede de internet.

Nesse sentido, Barreto e Brasil, corroboram que:

> A preocupação com a proteção dos usuários da internet mais uma vez é manifestada no diploma legal, seja garantindo-lhes voz (expressão, comunicação, manifestação do pensamento e participação) na rede, seja protegendo-lhes a intimidade e a privacidade, ou, ainda, assegurando-lhes acesso seguro e de qualidade ao mundo digital (BARRETO & BRASIL, 2016, p. 11).

Esclarecendo ainda mais a respeito da Neutralidade da rede, o Marco Civil visa à rede neutra, sem obscuridade, que atinge basicamente a área comercial, sendo que os provedores de acesso à internet não podem cobrar valores diferenciados para os usuários em virtude do que utilizam. Ou seja, não pode haver pacotes diferenciados na rede, todos devem acessar o todo virtual, devendo o provedor cobrar apenas pela conexão e velocidade da internet contratada.

Criado para determinar regras no uso e na distribuição da internet, o Marco Civil busca a segurança da rede e a proteção dos seus usuários, seja no âmbito civil, consumerista e até mesmo na esfera criminal. Na esfera comercial, impõe regras para distribuidores da internet, provedores de acesso, como a neutralidade da rede, que implica que o estabelecido em contrato deve ser priorizado. Os provedores de acesso, que fornecem o acesso à internet a seus clientes, não podem limitar ou interferir na velocidade que estes contratam. Nesta lei não há limitação de banda ou acesso, sendo que o proposto em

contrato deve ser respeitado pelos provedores sob sanção regulatória da Agência Nacional de Telecomunicações.

2.5 A REVOLUÇÃO DIGITAL COMO AVANÇO TECNOLÓGICO E OS RISCOS AO USUÁRIO DA REDE

O crescimento da internet tem avançado muito rapidamente. A cada 6 (seis) meses surge uma nova descoberta que a torna ainda mais ágil e atrativa. Não houve nenhum outro meio de comunicação que expandiu tão rapidamente. Da leitura ao entretenimento, a internet traz o mundo para dentro dos lares, trabalhos e universidades.

> Entende-se por Revolução Digital o movimento de inserção na sociedade de novas tecnologias e serviços que utilizam desenvolvimentos recentes e que modificam a forma como o cotidiano progride. A popularização do computador por conta de seu barateamento e melhor acessibilidade (maior velocidade de conexão, maquinas mais potente e protocolos mais leves) contribui para que a cada dia mais pessoas ao largo do planeta tenham acesso a informática e, consequentemente, a rede mundial de computadores (SYDOW, 2015, p. 20)

Com a mudança no cotidiano das pessoas através da internet, tudo passa a ser informatizado e as facilidades são muitas. Contudo, apesar dos benefícios no mundo virtual, há um temor quanto ao crescimento da criminalidade, o qual, apesar das novas leis trazerem algumas sanções aos crimes e delitos cibernéticos, ainda não estamos preparados a combater. Nas palavras de Spancer Sydow:

> O avanço e a polarização da tecnologia aliada a informática fizeram com que surgissem novos hábitos e, com eles novos valores. Na medida em que tais valores adquirem relevância social e econômica, surgem também problemas quanto a sua preservação (SYDOW, 2015, p. 21)

Um dos grandes benefícios que a internet traz é a facilidade de comportar todo conteúdo de entretenimento e profissionalíssimo em um único local. Música, fotos, sons, planilhas, arquivos, contas bancárias, tudo se tem acesso por um único computador ou dispositivo móvel, onde quer que esteja o

utilizador. Indubitavelmente isso é um avanço que promove a vida das pessoas no século atual.

Atualmente softwares são projetados para comportar todo cotidiano de um usuário. Aplicativos são desenvolvidos para indicação dos melhores restaurantes, para publicar em instante o que fazem ao dia, para consultar médicos, advogados e professores, enfim, para controlar as atividades pessoais ou profissionais de cada um.

Há inúmeros benefícios oferecidos através da internet, de acordo com Luiz Ribeiro:

> De um simples site a um mega portal de conteúdo há muitas coisas parecidas que em pouquíssimos ambientes pode-se encontrar. Da mesma forma, blogs, sites, portais, sistemas, etc, são parte da mesma matéria-prima e por mais que tenham propósitos e fins diferentes, acabam por convergir e fazendo uma mistura que muitos procuram entender (RIBEIRO, 2010).

Pode-se dizer que este avanço traz valores diferenciados e muitos benefícios. Em contrapartida a isso, surgem ameaças tecnológicas que fazem com que diversos setores da sociedade fiquem atentos a possíveis crimes e condutas antiéticas como pornografia infantil, racismo, crimes contra a honra, disseminação de vírus, terrorismo, ataques a bancos de dados, tráfico de entorpecentes e golpes comerciais (NETO, SANTOS & GIMENES, 2012, p. 15).

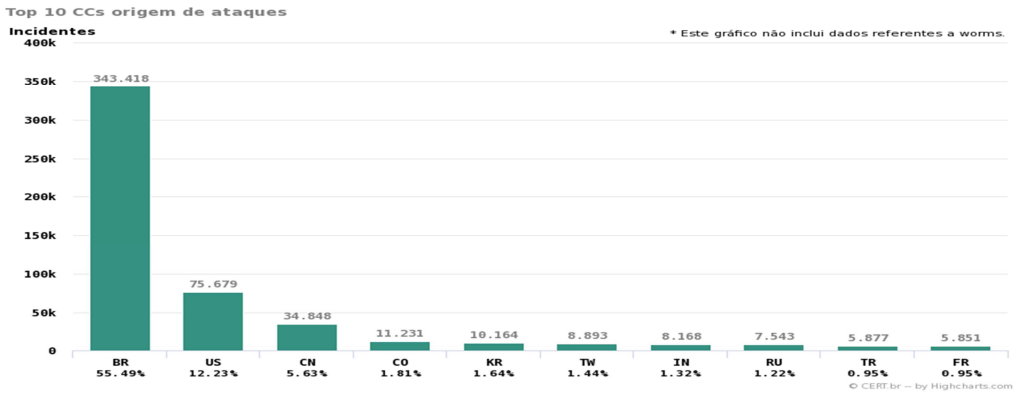
Segundo dados do Centro de Estudos, Respostas e Tratamento de Incidentes da Segurança Nacional (CERT.br[5]), podemos obter estatísticas de atos cometidos pela internet que desencadeiam diversos crimes em sequência. Como exemplo, a subtração de dados conhecida como *scan,* que são notificações de varreduras em redes de computadores que buscam verificar a vulnerabilidade dos arquivos ou software contidos em determinado computador; ou ainda o *worn* que são atividades para a propagação de códigos maliciosos na rede*; DoS,* que são ataques que resultam a queda de um serviço que pode ser dentro de um servidor de conteúdo, a um computador ou rede*; invasão,* que trata-se de um acesso não permitido pelo usuário a seu computador para subtrai-lhe os dados, ou o que estiver contido na sua rede a

[5] Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, gerido pelo núcleo de apoio a internet no Brasil através do comitê gestor de internet.

exemplo de fotos, senhas bancárias, arquivos pessoais e profissionais e*; fraude,* um ato de má-fé para lesar alguém.

No ano de 2016 os índices de ataques a redes e computadores pessoais foram em um percentual espantoso. O Brasil esteve à frente na origem de ataques virtuais, conforme apresentado na Figura 1.

Figura 1 - Origem dos ataques reportados ao CERT.br no ano de 2016.



Fonte: CERT.br (2017).

Outro fato importante foram os números de ataques, sendo em sua totalidade 647.112 (seiscentos e quarenta e sete mil cento e doze) ataques durante o ano de 2016, como é observado na Figura 2.

Figura 2 - Total de ataques reportados ao CERT.br no ano de 2016.

Tabela: Totais Mensais e Anual Classificados por Tipo de Ataque.

Mês	Total	worm (%)		dos (%)		invasão (%)		web (%)		**scan** (%)		**fraude** (%)		outros (%)	
jan	**54781**	4994	9	942	1	272	0	2266	4	32959	60	11846	21	1502	2
fev	**57041**	4176	7	137	0	95	0	1422	2	40911	71	8783	15	1517	2
mar	**92852**	3886	4	12851	13	106	0	4526	4	58962	63	10573	11	1948	2
abr	**44352**	1170	2	6147	13	126	0	1637	3	22531	50	11681	26	1060	2
mai	**49228**	3186	6	338	0	125	0	2361	4	27496	55	14456	29	1266	2
jun	**59266**	2041	3	823	1	126	0	1554	2	41210	69	12646	21	866	1
jul	**38402**	1766	4	1676	4	116	0	1804	4	25763	67	6252	16	1025	2
ago	**49596**	1927	3	260	0	137	0	10802	21	27970	56	7402	14	1098	2
set	**45472**	1583	3	9171	20	145	0	6027	13	21596	47	6082	13	868	1
out	**35372**	1293	3	410	1	86	0	5050	14	23257	65	4182	11	1094	3
nov	**57345**	1018	1	15735	27	320	0	7758	13	25858	45	5277	9	1379	2
dez	**63405**	1208	1	11942	18	41	0	10234	16	35390	55	3538	5	1052	1
Total	**647112**	28248	4	60432	9	1695	0	55441	8	383903	59	102718	15	14675	2

Fonte: CERT.br (2017)

A internet como ferramenta para o uso comum traz benefícios a seus usuários, contudo, partindo de dados e da fragilidade da rede, é necessário que se crie instrumentos que tragam segurança aos usuários ou fornecedores da rede.

3. CRIMES COMETIDOS ATRAVÉS DA INTERNET

O Código Penal Brasileiro em seu artigo 1º estabelece que não há crime sem lei anterior que o defina (BRASIL, 2017d). Partindo dessa premissa, entende-se que o crime só se configura ilícito penal quando há uma lei estabelecida prevendo-o.

No que tange aos crimes informáticos, os primeiros casos sugiram em meados de 1960 quando houve os primeiros registros do uso de computador para práticas ilícitas. Os atos foram manipulações sistêmicas, sabotagens e espionagens (NETO, SANTOS & GIMENES, 2012, p. 25).

Com a crescente evolução tecnológica, mais crimes foram surgindo e com isso à necessidade de regulamentação mais precisa com profissionais da área para a investigação e resolução destes crimes.

Segundo Neto, Santos e Gimenes, podemos definir delitos eletrônicos em três categorias.

> a) Os atos que utilizam a tecnologia eletrônica como método, ou seja, condutas criminais nos quais os indivíduos utilizam métodos eletrônicos para obter resultados ilícitos;
> b) Os que utilizam a tecnologia como meio, ou seja condutas criminais em que para a realização de um delito utilizam o computador como meio; e
> c) Os que utilizam a tecnologia eletrônica como fim, ou seja, condutas dirigidas contra a entidade física do objeto ou maquina eletrônica ou seu material com o objetivo de danificá-lo (NETO, SANTOS E GIMENES, 2012, p. 31)

Nesse sentido, a diferenciação de crime informático se define quando o agente comete o crime contra um dispositivo eletrônico e quando comete o crime através de um dispositivo eletrônico, utilizando-o para o ato ilícito.

3.1 CRIMES CONTRA A HONRA: CALÚNIA, INJÚRIA E DIFAMAÇÃO

O Código Penal Brasileiro aduz a respeito de crimes contra a honra, quais sejam: Calúnia, Injúria e Difamação. Vale ressaltar que delitos dessa espécie afetam um bem disponível fundamental, que é a honra da pessoa. Nesse sentido temos delitos que ofendem a honra de terceiros através de dispositivos informáticos, como computador, tablet, celulares ou qualquer outro meio tecnológico em que se propague uma notícia.

O Código Penal Brasileiro em seu artigo 138 dispõe:

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime.
> Pena - detenção, de seis meses a dois anos, e multa.
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propaga ou divulga.
> § 2º - É punível a calúnia contra os mortos (BRASIL, 2017d).

Calúnia é um ato danoso a honra de outrem, uma ofensa criminosa destinada a alguém. Segundo Neto, Santos e Gimenes:

> Significa acusar falsamente alguém da prática de fato definido como crime, colocando em dúvida a sua credibilidade no meio social, atingindo, de tal forma, sua honra objetiva, isto é, o conceito externo que os outros tem da pessoa caluniada (NETO, SANTOS & GIMENES, 2012, p. 42).

Os elementos que a classificam são em regra a ação ou a omissão de um único sujeito, podendo ser praticada através de um ou vários atos contínuos.

Podemos classificar calúnia como um crime comum, formal de forma livre, comissivo (excepcionalmente omissivo impróprio), unissubjetivo, unissubsistente ou plurisubsistente, caso em que se admite uma tentativa (NETO, SANTOS & GIMENES, 2012, p. 43).

A Calúnia por acusações criminosas pode ocorrer virtualmente em dispositivo eletrônico para ofender a integridade de uma pessoa. Um exemplo bem comum nos Tribunais são os fatos contados em redes sociais acusando alguém de uma conduta ilícita, vista como crime.

Neste sentido correlaciona-se um entendimento jurisprudencial elencado na obra de Jair Lot Vieira

> APELAÇÃO CRIMINAL - QUEIXA-CRIME - CALÚNIA - RECURSO ACUSATÓRIO - AUSÊNCIA DE DOLO ESPECÍFICO - NÃO-OCORRÊNCIA - AUSÊNCIA DE TIPIFICAÇÃO DO CRIME IMPUTADO FALSAMENTE - DESNECESSIDADE - MEIO QUE FACILITA A DIVULGAÇÃO DA CALÚNIA - SITES DE INTERNET - ART. 141 , III , CP - RECURSO PROVIDO.(TJMS, 2009)
> Não se fala em ausência de dolo específico do querelado que admite ter apontado irregularidades na Prefeitura, mas nega que visasse atingir a honra do Prefeito.
> A ausência de tipificação expressa do crime, que o querelado teria imputado falsamente ao querelante, não impossibilita a procedência da Queixa-crime, pois na Ação Penal Privada, assim como na Pública, o réu se defende dos fatos.
> A divulgação da calúnia por meio de sites de Internet configura causa de aumento, estabelecida no art. 141, III, do CP (VIEIRA, 2009).

Ressalta-se a calúnia proferida através da internet é tipificada no Código Penal Brasileiro como uma agravante, por ser considerada a internet um meio de rápido acesso e fácil divulgação.

No que tange a Difamação, o contexto é semelhante. Contudo não há a imputação de crime à vítima, há um fato desonroso sendo proferido contra alguêm. Nesse sentido ataca-se a reputação de alguém perante a sociedade através de fato ofensivo (NETO, SANTOS & GIMENES, 2012, p. 44).

O artigo 139 do Código Penal traz prescrito o texto e as penas cabíveis:

> Art. 139- Difamar alguém, imputando-lhe fato ofensivo a sua reputação:
> Pena- detenção, de três meses a um ano, e multa.
> Exceção da verdade
> Parágrafo Único- A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções (BRASIL, 2017d).

Na difamação a lei prevê sua tipicidade como uma contravenção penal, o fato será somente doloso, com a intenção de manchar a honra de alguém. Sua consumação se dá no momento em que a vítima descobre o ato (NETO, SANTOS & GIMENES, 2012, p. 44).

Para exemplificar e relacionar aos crimes cibernéticos, a difamação ocorre quando o agente utiliza-se de um dispositivo tecnológico para imputar falsamente sobre a reputação de um terceiro, causando-lhe um dano.

Outrossim, é importante frisar que é possível que calúnia ou difamação contra empresas sendo a diferenciação feita apenas quando o dolo

se relaciona a um crime ou a um ato que impute a honra do estabelecimento (CNPJ).

Nesse sentido podemos colacionar um entendimento jurisprudencial que vislumbre o entendimento de Tribunais no que tange a difamação ocorrida por meio de dispositivos eletrônicos.

> AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS. Pretensão de compensação por palavras e frases ofensivas postadas no *Facebook*. Sentença de improcedência, sob fundamento de que se tratavam de "desabafo, lançado no contexto de desentendimento entre as partes, relativamente à possibilidade ou não de utilização de sobrenome político local". Apela a autora sustentando ter sido caluniada pelas rés, que a acusaram de ter se apropriado do veículo de uma delas e que devia dinheiro e respeito a todos da família; houve difamação quando as recorridas disseram que a apelante seria louca, desequilibrada, agonizante, aspirante à primeira dama entre outras ofensas imputadas; crimes contra a honra praticados pela internet. Contrarrazões com preliminar de intempestividade. Cabimento do reclamo.
> Preliminar. Intempestividade. Insubsistência. Recurso protocolado no prazo legal. Publicação ocorre no dia útil seguinte à disponibilização no DJE. Início da fluência do prazo no dia útil posterior ao da publicação. Inteligência dos §§ 2º e 3º do art. 224 do CPC/2015. Preliminar rejeitada.
> Qualificação pejorativa da autora e em tom ameaçador contra os seus atributos personalíssimos. Revide desproporcional das rés na discussão iniciada pela autora quanto à utilização política de sobrenome. Insultos foram lançados não como uma mera retorsão imediata, mas para menoscabar a imagem da vítima perante familiares e terceiros, ante o desgosto pelo esclarecimento quanto ao político que estava utilizando do sobrenome comum. Ofensas lançadas na rede mundial de computadores com repercussão na cidade em que residem. Obrigação de indenizar. A indenização do dano moral deve ser arbitrada por equidade, consideradas as circunstâncias do caso, em valor que sirva a um só tempo, de punição ao lesante e compensação ao lesado, sem que acarrete enriquecimento sem causa. Fixação em R$ 10.000,00. Aplicação dos princípios da proporcionalidade e da razoabilidade. Recurso provido para condenar as rés solidariamente a compensar danos morais no importe de R$ 10.000,00. Sucumbência invertida. Verba honorária arbitrada em 15% sobre o valor atualizado da condenação (TJSP, 2017, grifou-se).

No caso acima houve a ofensa a honra da vítima, causando-lhe dano a sua personalidade, por meio de postagem em rede social, configurando o crime de difamação por meio eletrônico.

A injúria encontra-se prevista no artigo 140 do código penal brasileiro:

> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:

> Pena - detenção, de um a seis meses, ou multa.
> § 1º - O juiz pode deixar de aplicar a pena:
> I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;
> II - no caso de retorsão imediata, que consista em outra injúria.
> § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:
> Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.
> § 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião ou origem: (Incluído pela Lei nº 9.459, de 1997)
> § 3° Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência (BRASIL, 2017d).

Podendo ser tipificada apenas na forma dolosa, a injúria é um ato com a finalidade de insultar alguém a sua honra subjetiva (NETO, SANTOS & GIMENES, 2012, p. 45).

Na injúria, ataca-se a dignidade da pessoa. A forma subjetiva da honra da pessoa está relacionada a suas qualidades. Relacionando a injúria aos crimes cometidos pela internet, esta passa a ser uma ofensa a dignidade da pessoa na forma virtual, geralmente cometida através de redes sociais. Como forma mais gravosa da forma da injúria temos a injúria discriminatória, que ofende a cor, raça ou etnia da pessoa.

Os delitos contra a honra acima citados, podem ser praticados por meio de dispositivo eletrônico contra pessoas físicas e, com a exceção da injúria, contra pessoas jurídicas, atingindo-se a forma subjetiva ou objetiva.

3.2 CRIMES CONTRA O PATRIMÔNIO: FURTO MEDIANTE FRAUDE, RECEPTAÇÃO, EXTORSÃO, ESTELIONATO.

O Código Penal Brasileiro traz diversos crimes cometidos contra o patrimônio, que são crimes comuns na forma dolosa. Neste aspecto, serão demonstradas as formas dos crimes digitais contra o patrimônio de terceiros e as sanções previstas.

O Furto está previsto no artigo 155, parágrafo 4º, do Código Penal e é praticado quando o agente subtrai de alguém coisa alheia móvel (BRASIL, 2017d). Já a Fraude é um ato de engano praticado pelo agente. Ou seja, é uma conduta do agente para ludibriar uma vítima.

Partindo do disposto em lei, o crime de furto mediante a fraude por dispositivo eletrônico ocorre quando há a subtração de dados de alguém para fins econômicos.

Os dados geralmente estão armazenados em arquivos da agência bancária ou até mesmo no computador da vítima, nesse segundo, a prática do ilícito ainda é maior, pois as vítimas geralmente são induzidas a baixar materiais da internet carregados de vírus[6] que infectam suas máquinas com o objetivo de subtrair os dados confidenciais.

Um dos grandes exemplos que pode ser citado é o Cavalo de Troia[7], que quando instalado o arquivo, as portas de acesso aos bancos de dados são abertas, permitindo a subtração de informações confidenciais como arquivos e/ou senhas (NETO, SANTOS & GIMENES, 2012, p. 30).

Além do uso de vírus para acesso a banco de dados, outros mecanismos são utilizados para a pratica de furto de dados como os *sniffers*[8], que são programas que visam, através de e-mails, vigiar os acessos da vítima, sendo ela pessoa física e, na maioria das vezes, jurídica (NETO, SANTOS & GIMENES, 2012, p. 30).

No crime de furto mediante fraude a finalidade do agente criminoso é econômica, ou seja, seu único intuito é subtrair dinheiro de contas bancárias, sem que haja contato com a vítima.

A extorsão está tipificada no artigo 158 do Código Penal e se dá pela ameaça ou violência com intuito de obter valores econômicos. Na maioria das vezes a extorsão tem cunho sexual.

Para exemplificar, colaciona-se um caso ocorrido no Brasil no ano de 2011:

> 04/08/2011 - Mulher é condenada a 6 anos de reclusão por crime de extorsão pela Internet
> [...] a denúncia do MP, os fatos ocorreram no período de maio a julho de 2010, quando a vítima (do sexo masculino, idade 40,

[6] VIRUS é um dispositivo malicioso que infecta computadores e sistemas, pode ser também usado para danificar sistemas operacionais de dispositivos móveis. O vírus que infecta sistemas se espalham com facilidade, ocasionando perda de pacotes de dados e captura e informações confidenciais.
[7] CAVALO DE TROIA conhecido como TROJAN é um vírus utilizado para infectar dispositivos em busca de captura de informações.
[8] SNIFFERS, são sistemas utilizados por hackers para capturar o trafego de um usuário, quais sites são acessados e o que determinado dispositivo utiliza na internet.

> casado) conheceu a denunciada em uma sala de bate-papo do provedor UOL. Ela se identificou como Amanda, 22 anos, *nick name*: gatinhamanhosa. Os encontros virtuais eram, a princípio, através de MSN, depois por e-mails, ligações e mensagens telefônicas. Fotos sensuais foram trocadas e por diversas vezes o internauta tentou marcar um encontro presencial, mas a "gatinhamanhosa" se esquivava.
> Passado algum tempo, a idade dela mudou. Confessou meio constrangida, que tinha apenas 19 anos. Contou que passava por dificuldades financeiras, pois não tinha mãe e morava com pai bravo e avó muito doente. O homem, solícito, ofereceu-lhe dinheiro. O primeiro depósito, segundo afirmou em depoimento, foi espontâneo. Os seguintes foram a pedido da "gatinha". De maio a junho de 2010, ele depositou R$ 5.060,00 para a moça numa conta na Caixa Econômica Federal. Enfim, cansado das desculpas e dos encontros desmarcados, o homem informou que não faria mais depósitos. Foi então, que as extorsões começaram.
> A moça de supostos 19 anos decidiu abrir o jogo: "Tinha 16 e ia contar para todo mundo que o homem era pedófilo!" As chantagens começaram e depois disso o internauta depositou na conta dela, de 2 de julho a 29 de julho, mais R$ 10 mil, sob pena de ser denunciado à polícia e à esposa. O homem recebeu diversas ameaças, não só da mulher como de comparsas.
> Amedrontado, decidiu, ele mesmo, procurar ajuda em uma delegacia. O flagrante foi armado no Shopping do Valparaíso, local da agência bancária na qual os depósitos eram efetuados. A mulher foi presa enquanto falava ao orelhão próximo à CEF. Nome: Francisca; idade: 40 anos (TJDF, 2011, grifou-se).

Nota-se com esse exemplo que a vítima foi enganada e houve a extorsão no momento em que foi ameaçada para depositar os valores. Neste sentido, configurou-se a extorsão pela ameaça ocorrida.

No estelionato a vítima é induzida a cometer determinado ato a fim de atingir a vontade do criminoso, onde ocorre o engano. Apesar de a finalidade ser a mesma pretendida pelo criminoso, o estelionato não pode ser confundido com o crime de furto mediante fraude.

Há uma ação voluntária da vítima. Um exemplo são os sites de produtos onde a vítima compra através de cartão de crédito ou boleto bancário e não recebe a mercadoria, ou sites onde há o acesso da vítima no momento em que o mesmo acessa contas bancárias via internet.

É válido ressaltar que, além do furto mediante fraude, estelionato e extorsão, tem-se o crime de receptação pela internet, que é o ato praticado pelo agente que adquire, transporta ou comercializa produtos provenientes de furtos ou roubos, que está previsto no artigo 180 do código penal. Neste sentido, cola-se o entendimento do Tribunal de Justiça do Distrito Federal a respeito do tema:

> A 3ª Turma Criminal do Tribunal de Justiça do Distrito Federal e dos Territórios, por unanimidade, negou provimento ao recurso do réu e manteve a sentença que o condenou pela prática do delito de receptação de um *notebook* furtado.
> Segundo a denúncia oferecida pelo Ministério Público do Distrito Federal e dos Territórios, o acusado teria adquirido um *notebook*, o qual sabia que era proveniente de um crime de furto, objeto que foi reconhecido pela vítima em um anúncio de um site de venda *online*, feito em nome do acusado. A vítima, então, através de uma amiga, marcou um encontro com o acusado, no Shopping do Gama, para efetuar a compra do notebook, momento em que a vítima compareceu ao local, reconheceu o objeto, e o acusado foi preso.
> O réu foi citado e apresentou defesa, na qual requereu sua absolvição.
> O juiz da 1ª Vara Criminal do Gama o condenou pela prática do crime de receptação, descrito no art. 180, caput, do Código Penal, e fixou sua pena em 1 ano de reclusão e multa. Por estarem presentes os requisitos legais, o magistrado substituiu a pena privativa de liberdade por uma restritiva de direitos (TJDF, 2017, grifou-se).

O crime é visto diariamente nas redes de anúncios em redes virtuais. Trata-se das vendas de objetos subtraídos.

3.3 CRIMES DE DANO: VIOLAÇÃO DE SISTEMAS, ATAQUES A BANCO DE DADOS, TERRORISMO.

O intuito do agente que pratica crimes de violação de sistemas e ataque a bancos de dados, é exclusivamente causar dano a fim de inutilizar o bem de outrem ou utilizar em benefício próprio.

Nesse sentido podemos citar para exemplificar, ataques a bancos de dados ou violação de sistemas os ataques DDoS[9], que são ataques que tem como objetivo parar sistemas ou servidores de empresas, bancos e até mesmo órgãos públicos. Um dos mais recentes exemplos que se pode citar é o fato de uma possível *ciberguerra* estar ocorrendo entre a Coréia do Norte e os Estados Unidos. Neste sentido, para explanar o fato colaciona-se uma nota em que os Estados Unidos ameaçam sistemas Norte Coreanos com ataques DDoS.

> Os ataques DDoS lançados pelos EUA se encerraram fazem poucos dias — ou horas. No começo do ano, a Casa Branca comentou o

[9] DDoS é um ataque utilizado por Hackers para, simultaneamente acessarem determinada máquina. Uma vez iniciado o ataque resulta na queda total do sistema.

> seguinte sobre o Comando de Combate Unificado: "Demonstra nossa determinação contra *ciberameaças* e vai nos ajudar a tranquilizar aliados e parceiros, além de deter adversários". O relato não indica quando os EUA lançaram o ataque DDoS contra a Coreia do Norte, porém, acredita-se que os ataques se encerram entre os últimos dias de setembro e os primeiros deste mês, outubro. Um ataque DDoS realizado por uma potência como os Estados Unidos pode desde deixar um departamento ou agência no escuro por algum tempo, sem poder de monitoração, como até mutilar qualquer capacidade de ciberataque ou retaliação do adversário por um tempo (TECMUNDO, 2017, grifou-se).

Os ataques DDoS são poderosíssimos e podem parar setores que possuem a mais alta segurança tecnológica.

Vale ressaltar que o terrorismo se enquadra nos crimes de dano através de ataques a banco de dados. Em se tratando do século em que vivemos, o terrorismo não mais é apenas um ato físico, onde ocorrem mortes por destruição de bombas ou ataques, o conceito de terrorismo passou a ocupar um lugar virtual, pois máquinas de hospitais, computadorizadas, podem ser desligadas por *cibercriminosos*. Redes de energia elétrica podem ser desligadas através de ataques cibernéticos. Sistemas governamentais que envolvem agentes policiais podem perder seu banco de dados através de ataques promovidos pela internet. Nesse sentido pontua Fabiani Borges que:

> Os atos de terrorismo são aqueles praticados com o fim de ameaçar, amedrontar, e, até mesmo, lesar a vida ou patrimônio de outrem, em nome da defesa ou para a consecução de um ideal, normalmente fruto de intolerância política, religiosa ou social (BORGES, 2015).

No que tange a segurança da rede, pode-se afirmar que o mundo virtual facilita o acesso a dados confidenciais, o que possibilita uma probabilidade maior de ataques terroristas.

Neste sentido, corrobora Mayara Gabrielli Gardini que:

> O espaço cibernético facilitou o trabalho dos grupos terroristas. Neste sentido, é muito mais fácil alcançar seus objetivos com a ajuda de um espaço que permite o anonimato, mudanças rápidas, apresenta um baixo custo de entrada e é de fácil acesso, do que ter que alcançá-los em espaços que contenham leis, fronteiras e exércitos no caminho (GARDINI, 2014, p. 19).

Com a crescente evolução da inteligência artificial e computadorizada os atos terroristas também estão em constante desenvolvimento, saindo do espaço físico para o espaço virtual a fim de facilitar seus atos contra inimigos.

3.4 CRIMES SEXUAIS: PEDOFILIA E PORNOGRAFIA INFANTIL.

Dos crimes cometidos pela internet, a pornografia infantil tem apresentado um crescimento espantoso. Trata-se de um crime onde há divulgação de fotos de crianças e adolescentes na rede cibernética a fim de divulgação ou comércio.

De acordo com Fernando Capez:

> A modernidade trouxe novas possibilidades de cometimento de crimes sexuais contra menores, a exemplo da disseminação de pornografia infantil na internet. A Organização Não Governamental (ONG) Safernet, especializada em monitorar denúncias sobre crimes de direitos humanos em ambientes virtuais, recebeu, apenas em 2014, mais de 50 mil denúncias de pornografia infantil em mais de 22 mil páginas *online.* O número representa 27% do total de denúncias recebidas pela ONG naquele ano (CAPEZ, 2016).

O crime sexual contra a criança e o adolescente têm aumentado a cada dia ante a dificuldade de investigação do criminoso. Segundo Neto, Santos e Gimenes, “[...] neste novo cenário, o autor do crime não mostra seu rosto, oculta sua identidade e deixa apenas vestígios eletrônicos para serem rastreados [...]” (NETO, SANTOS & GIMENES, 2015, p. 52).

Diante disso o crime passa a ser um problema delicado a se enfrentar nas investigações policiais.

O ECA, Estatuto da Criança e do Adolescente, prevê no artigo 241 e seguintes, penas para quem praticar comércio, produzir materiais como fotografias infantis, induzir a criança ou o adolescente a material com teor pornográfico, aliciar, constranger ou cometer qualquer ato libidinoso contra a criança e/ou adolescente (BRASIL, 2017e).

João Miguel Almeida da Silva discorre que

> [...] O tipo legal de pornografia de menores passou a englobar a conduta daquele que produzir, distribuir, importar, exportar, exibir, ceder, adquirir ou detiver material pornográfico com representação realista de menor (SILVA, 2016, p. 22).

Segundo Barreto e Brasil

> Quanto a pornografia infanto-juvenil na internet, o Estatuto da Criança e do Adolescente é bem específico, em seus artigos 240 a 241-E. É válido ressaltar que, mesmo quando as imagens são trocadas ou disponibilizadas gratuitamente, como em grupos do WhatsApp, há crime (Art. 241-A), cuja a pena é de até seis anos de reclusão (BARRETO & BRASIL, 2016, p. 192)

Com o atual desenvolvimento da tecnologia, as crianças estão cada vez mais adeptas ao mundo virtual. Além da pornografia infantil temos a pedofilia como um crime cada vez mais constante na esfera virtual.

Vale ressaltar que o aparecimento dos crimes desse porte tem aumentado ante o sistema de punição estar cada vez mais rígido, as descobertas são mais constantes. O Marco Civil da internet tem uma grande colaboração no que tange as investigações dos crimes de pedofilia da internet, o que será abordado e explanado mais à frente.

A pedofilia já é uma pratica existente desde a Grécia antiga, há países onde o ato sexual de menores com adultos é visto como normal. Marco Aurélio de Almeida aduz que na sociedade da antiga Grécia a prática sexual de pessoa mais velha com pessoa mais nova era considerada normal. Esta prática ocorria para troca de favores e na maioria das vezes era cometida por homens para relacionar-se com pessoas do mesmo sexo (ALMEIDA, 2005, p. 3).

Para a caracterização da Pedofilia via internet é necessário que o agente mantenha contato com a vítima por sistema informático a fim de induzi-la a um envolvimento sexual. Leia-se que não há o crime de estupro nesse contexto, a vítima é induzida a prática pelo agente. Na grande maioria dos casos a pedofilia cibernética é cometida por homens que buscam satisfazer seus desejos sexuais em crianças e adolescentes.

3.5 INDUZIMENTO, INSTIGAÇÃO E AUXILIO AO SUICÍDIO

> Art. 122- Induzir ou instigar alguém a suicidar-se ou prestar-lhe auxílio para que o faça.

> Pena-reclusão, de 2(dois) anos a 6 (seis) anos, se o suicídio se consuma; ou reclusão de 1(um) a 3 (três) anos, se da tentativa de suicídio resulta lesão corporal de natureza grave (BRASIL, 2017d).

A legislação Brasileira atual não tipifica o suicídio em si como um crime, contudo, há tipificação do delito no caso de um terceiro induzir ou instigar, ou até mesmo ajudar alguém a suicidar-se.

Neto, Santos e Gimenes, corroboram a respeito a diferenciação de induzir, instigar ou dar auxílio ao suicídio.

> Induzir, que é dar a ideia a quem não a possui, inspirar, incutir; instigar, ou seja, fomentar, fortalecer a ideia que já existia; auxiliar, constituindo no apoio material ao ato suicida, fornecer os meios necessários, dar as instruções sobre o modo de se utilizar os meios para o suicídio. Caso o autor pratique uma das condutas ou todas elas, não implica a duplicidade de delitos, tratando-se de um crime de ação múltipla e conteúdo variado (NETO, SANTOS & GIMENES, 2012, p. 40).

O induzimento, instigação ou auxilio ao suicídio são considerados pelo Código Penal como crime contra a vida e podem ocorrer através da internet por um agente que estimule a prática do suicídio. A exemplo atual, cita-se o *jogo da baleia azul,* que provocou autolesões e mortes em crianças e adolescentes.

3.6 OS PERFIS FALSOS

Fake[10] é a palavra proveniente do inglês que significa falso. As redes sociais mais acessadas da atualidade estão carregadas de perfis falsos. Há duas linhas que seguem os criadores destes perfis: a) para homenagear ídolos através das redes sociais, os famosos fã clubes; e b) para promover ódio, realizar condutas ilícitas e praticar crimes.

Todos os crimes citados anteriormente neste trabalho possuem uma probabilidade de serem praticados por meio de perfis falsos, visto que o autor de cada delito não deseja ter sua identidade revelada e com base nisso, cria perfis falsos para pratica de ilícitos.

[10] FAKE ou FALSO que no caso em tela se remete a PERFIL FALSO, são aqueles criados em redes sociais sem que identificar a verdadeira identidade do indivíduo possuidor do perfil.

O Código Penal Brasileiro não traz explicitamente uma sanção para agentes que utilizam-se de perfis falsos para a prática de crime, contudo, através de alguns dispositivos concernentes na legislação penal o uso de perfil falso presume-se identidade falsa, ou falsidade ideológica.

Neste sentido, com a colaboração de Crespo e Santos:

> São bastante comuns na Internet os crimes de falsa identidade e falsidade ideológica. No primeiro deles alguém se passa por outrem, utilizando dados e até mesmo senhas, em proveito próprio ou alheio, ou para causar dano. As credenciais de acesso a uma rede social, por exemplo, quando usadas por outra pessoa que não o seu titular, com o fim de obter vantagem ou causar dano, pode ser subsumida ao crime do art. 307 do Código Penal (falsa identidade). No segundo caso, há inserção de dados falsos ou omissão de algo que deveria constar, em documentos públicos ou particulares, com intenção de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante. Esses documentos podem ser formulários constantes de páginas da Internet ou mesmo das redes sociais. Nada mais é, portanto, do que mentir em um documento, ou alterar seu conteúdo, para modificar o direito de alguém (criando, modificando ou extinguindo um direito ou uma obrigação) para obter algum tipo de vantagem, ou para modificar a verdade sobre um fato relevante (CRESPO & SANTOS, 2015).

Outrossim, segundo nota publicada por Alessandra Horto no diário online *O Dia*, "Se passar por outra pessoa na internet é crime de Falsidade Ideológica e o usuário pode pegar até cinco anos de reclusão, mesmo que não haja o intuito de prejudicar quem teve o nome utilizado” (HORTO, 2014).

Neto, Santos e Gimenes lecionam que no novo cenário de criminalidade virtual o autor não mostra seu rosto, oculta sua identidade, mas deixa vestígios eletrônicos para serem rastreados (NETO, SANTOS & GIMENES, 2012, p. 52).

Neste sentido, aquele que utiliza-se da ferramenta das redes sociais para promover dano a alguém sem utilizar-se de sua real identidade comete os crimes previstos nos artigos 299 e 307 do Código Penal.

3.7 A RESPONSABILIDADE CIVIL DOS PROVEDORES DE ACESSO E CONEXÃO EM DANOS CAUSADOS POR TERCEIROS

Se faz necessário diferenciar provedor de conexão à internet e provedor de aplicação à internet. O primeiro é aquele que distribui sinal para que o

usuário possa se conectar à rede, os provedores de banda larga ou via rádio por exemplo. O segundo é o provedor que dá o acesso às aplicações da rede, que são os sites específicos como *Google, Facebook, Twitter,* dentre outros.

Neste sentido, segundo Frederico Ceroy:

> Provedor de Acesso ou Provedor de Conexão é a pessoa jurídica fornecedora de serviços que consistem em possibilitar o acesso de seus consumidores à internet. Para sua caracterização, basta que ele possibilite a conexão dos terminais[4] de seus clientes à internet. Em nosso país os mais conhecidos são: *Net Virtua, Brasil Telecom, GVT* e operadoras de telefonia celular como *TIM, Claro* e *Vivo*, estas últimas que fornecem o serviço 3G e 4G (CEROY, 2014).

Conforme ensinamentos do autor, o provedor de aplicações é aquele que "fornece um conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet, não importando se os objetivos são econômicos" (CEROY, 2014).

Assim, quanto ao provedor de acesso e conexão temos aqueles que disponibilizam sinal de internet via – rádio, cabo ou fibra a seus clientes e, quanto aos provedores de aplicações, são aqueles que possuem um sítio onde há o armazenamento de informações que disponibilizam aos usuários, ferramentas para acesso e usufruto das aplicações da internet.

Maria Helena Diniz contribui no sentido de que a Responsabilidade Civil é

> [...] a aplicação de medidas que obriguem alguém a reparar dano moral ou patrimonial causado a terceiros e razão de ato próprio imputado, de pessoa por quem ele responde, ou de fato de coisa ou animal sob sua guarda ou, ainda, de simples imposição legal (DINIZ, 2009, p. 34).

Assim, a responsabilidade civil se da ao dever de reparar um dano causado a alguém. Antes da promulgação do Marco Civil, os tribunais entendiam que a responsabilidade civil por dano causado por terceiro, cabia ao provedor de acesso ou aplicação responder solidariamente em caso de descumprimento extrajudicial

Nesse sentido, leciona Marcelo Furllani Lopes

> [...] a jurisprudência do Superior Tribunal de Justiça vinha se consolidando no sentido de que o provedor seria responsabilizado

> solidariamente caso descumprisse mera notificação extrajudicial que requeresse a retirada do conteúdo (LOPES, 2016).

No entanto a legislação trouxe mudanças discorrendo em seus artigos 18 e 19 a respeito do tema. Vejamos:

> **Art. 18.** O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.
> **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, 2014b).

As normas referentes a responsabilidade civil dos provedores foram ajustadas estabelecendo que ao provedor de acesso e conexão não seria aplicado responsabilidade civil nos atos e danos causados por terceiros. Contudo, aos provedores de aplicação recaria a sanção através de responsabilização civil de atos cometidos por terceiros em casos de omissão ou desobediência de uma ordem judicial a um provedor de aplicações.

Neste sentido explana Barreto e Brasil que

> Ao ser comunicado sobre uma decisão judicial de indisponibilização de conteúdo, o provedor de internet deverá retirar o material ilícito no prazo máximo estipulado, sob pena de responder pela omissão praticada. Após a desabilitação do conteúdo, o provedor de aplicação comunicará a outra parte os motivos e as informações que levaram aquela providencia, a fim de possibilitar o contraditório e a ampla defesa, caso não seja determinado na ordem judicial (Barreto, Brasil, 2016, p.123).

Outrossim o artigo 21, é taxativo em relação ao compartilhamento de materiais que sobrepujem nudez ou apelo sexual.

> Art. 21 O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo (BRASIL, 2017b).

Inobstante, diante da gravidade dos casos de nudez e apelo sexual, caso haja divulgação do conteúdo e desobediência do provedor na retirada do mesmo, caberá responsabilidade subsidiária ao provedor de aplicação por não retirar o conteúdo de circulação na rede.

A responsabilidade civil dos provedores de internet por danos gerados por terceiros pode ser elencada na forma da lei, nos artigos supracitados, nos casos dos provedores de aplicações que ignorem determinação judicial referente aos conteúdos que devem ser retirados da rede. Igualmente, responderá e sofrerá sanção, os provedores de acesso e conexão que não obtiveram após a determinação judicial, os dados de acesso e aplicação a internet, assunto que será abordado posteriormente.

4. A INVESTIGAÇÃO DOS CRIMES COMETIDOS PELA INTERNET NO ÂMBITO DO DIREITO PENAL BRASILEIRO JUNTO AO MARCO CIVIL DA INTERNET

Os *ciberdelitos*, ou crimes cometidos pela internet estão relacionados ao modo do comportamento humano frente a uma máquina capaz de vislumbrar o universo digital em segundos.

Muito se tem discutido a respeito da temática do *ciberdelito* e da escassez de legislação apropriada para a resolução dos casos. Por certo há de se comentar que não basta apenas que se imponham medidas a fim de reduzir os riscos pela internet, mas, arrisca-se dizer, que há uma necessidade da implementação de políticas públicas que viabilizem educar o comportamento da vítima e do infrator no âmbito da internet.

Os crimes cometidos via rede digital estão divididos no comportamento humano (pre)conceituoso, que comete ilícitos ofendendo honra, raça, religião e opção sexual, no comportamento humano com a intenção de subtrair algo de outrem e, no comportamento humano a fim de cometer atos libidinosos contra menores, homens e mulheres.

Para complementar a temática da investigação criminal bem como a resolução dos casos, se faz necessário aprofundar acerca da competência jurisdicional dos crimes cometidos pela internet. Outrossim, mostra-se

importante relacionar os meios existentes de elementos que evidenciem a autoria delitiva do *cibercriminoso.*

4.1 DA COMPETÊNCIA

É de fundamental importância uma análise aos aspectos do crime cometido pela internet, onde ocorre, qual o tempo, o momento que se consuma o ato e qual o enlace do Marco Civil da Internet com a Legislação Penal Brasileira.

A internet é um campo vasto onde as pessoas interagem entre si em segundos, a agilidade do sistema colabora para que atos ilícitos sejam cometidos em diversos locais do país e do mundo, dificultando assim o modo de identificação do delito.

O Código Penal Brasileiro adotou algumas teorias no que concerne o tempo e o local do crime, Para Neto, Santos e Gimenes, a primeira fora adotada a teoria da atividade onde considera o tempo do crime o momento da ação ou omissão do agente, ou seja, no momento da prática da conduta prevista na normal penal incriminadora e, na segunda, da Ubiquidade onde considera-se o crime tanto o local em que ele foi cometido quanto o local onde ocorreu o resultado (NETO, SANTOS & GIMENES, 2012, p. 92).

Para adentrarmos na esfera de competência jurisdicional dos crimes cometidos pela internet é necessário que se faça a definição do que adota a doutrina no que tange o tempo e ao local do crime. Nota-se que a falta de legislação especifica com relação aos *ciberdelitos* impulsiona a aplicação do previsto no Código Penal Brasileiro no que se refere ás teorias da atividade e da ubiquidade.

Outrossim, é importante discorrer a respeito da territorialidade e dos atos cometidos pela internet. Neste sentido, temos os crimes que foram cometidos em território nacional, que se conceituam naqueles crimes, infrações ou delitos que ocorrem através de dispositivo conectado à internet, hospedado em servidores no território nacional. Nestes cabe à aplicação da legislação brasileira.

Da mesma forma ocorre com os crimes iniciados no Brasil e que tenha sido consumado no exterior, como o crime de injuria racial por exemplo, o ato pode ter sido iniciado no Brasil, mas divulgado em outro país. Neste caso, aplicar-se-á a legislação brasileira.

Para exemplificar, Neto, Santos e Gimenes discorrem que “desde que no Brasil tenha sido praticado atos de execução, no todo ou em parte, ou aqui se tenha produzido o resultado do comportamento ilícito, é de se aplicar a legislação pátria”. (NETO, SANTOS & GIMENES, 2012, p. 92).

É válido mencionar que as normas contidas no Marco Civil, juntamente com a aplicação do Código Penal nas suas teorias e sanções, devem ser respeitadas e submetidas às empresas internacionais. Em outras palavras, para exemplificar a obrigatoriedade, empresas como *Facebook, Instagram, WhatsApp,* dentre outras acessadas no Brasil, devem obedecer às normas e princípios da legislação vigente no que se refere aos crimes cometidos pela internet. Isso porque, como iremos adentrar mais à frente, facilitará a colaboração destas empresas com a investigação cibernética.

Muito se tem discutido a respeito do órgão competente para julgar os crimes cometidos pela internet. Isso ocorre porque o local onde inicia o crime nem sempre é o mesmo onde ele se consuma. Nos crimes de furto mediante a fraude, por exemplo, o ato inicia através de um computador que hospeda determinado IP naquela região, contudo o ato de furto ocorre em outro local, naquele onde há a invasão para que se obtenha os dados de terceiro. Nesse diapasão, Neto, Santos e Gimenes, elucidam o tema com objetividade, discorrendo que se pode denominar os atos cometidos pela internet como crimes plurilocais (NETO, SANTOS & GIMENES, 2012, p. 104). Que são aqueles onde em diversos locais ocorreram os atos do crime.

O Marco Civil não trouxe especificamente dispositivos que indicassem o órgão competente. Assim, se faz necessário recorrermos aos entendimentos dos tribunais a respeito.

Nesse sentido, o informativo do Superior Tribunal Federal de número 335 aduz que todo crime que atinja um bem tutelado pela União será de competência da Justiça Federal (MPPR, 2011).

O entendimento do STF se refere à pedofilia infantil e divulgação de imagens com conteúdo pornográfico infantil. Sendo que a proteção da Criança e do Adolescente é matéria do ECA, logo é tutelado pela União.

Outrossim, quando um crime é praticado através de um órgão federal, ou contra uma autarquia, sendo ele pela internet, também é de competência da Justiça Federal, pois está atingindo entes geridos pela União.

Igualmente, os crimes que excedam a esfera territorial, que ocorra a consumação fora do país, serão da mesma forma de competência da Justiça Federal. Os demais crimes que sejam cometidos dentro de território nacional nos limites dos estados e através de órgãos particulares, estes serão de competência da Justiça Estadual (NETO, SANTOS & GIMENES, 2012, p. 107-108).

Para explanar ainda mais a respeito da competência, colhe-se o entendimento do autor Lucas Souza, que discorre a seguir:

> No que tange aos crimes tentados e consumados aqui no Brasil, tem-se entendido nos tribunais superiores, que a competência será a da regra do artigo 70 do Código de Processo Penal, supra mencionado, sendo o foro competente, o local onde se consumou o fato. No caso da internet, seria o local onde se encontra o provedor, nos casos de crimes que ocorram dentro do próprio Estado e que não atinjam nenhum bem da União.
> Já nos crimes internacionais, que tenham dado início aqui no Brasil, mas que se prosperou para o exterior, como por exemplo, pornografia infantil que se iniciou aqui no Brasil mas está sendo visualizada na Holanda, a competência tornar-se-á da Justiça Federal, como elucidado no artigo 109, inciso IX da Constituição Federal o artigo 88 do Código de Processo Penal, haja vista que o crime ultrapassou a barreira nacional. Enquadram-se também nessa competência, os crimes que ocorrem dentro dos limites Estaduais, porém, atingem um bem jurídico tutelado pela União, como é o caso de crime de racismo praticado pela internet (SOUZA, 2017).

Ressalta-se a importância de distinção do órgão competente em matéria de crimes cometidos pela internet. Permeando a definição pode-se iniciar com os atos de investigação dos crimes digitais.

4.2 AS ALTERNATIVAS INVESTIGATIVAS QUE PODEM SER ADOTADAS PELAS AUTORIDADES NA RESOLUÇÃO DOS CRIMES COMETIDOS PELA INTERNET

Com o avanço tecnológico na era globalizada em que se vive é necessário ponderar a respeito do comportamento humano na internet. Atualmente muito se tem comentado a respeito do avanço tecnológico no mundo. É certo que boa parte das atividades humanas desenvolvidas atualmente necessitam da internet como meio de trabalho, pesquisa e até lazer.

A exemplo disso, pode-se citar o atual desenvolvimento em nossos tribunais, onde diversos mecanismos foram criados através de sistemas, que são acessados pela internet, para facilitar o acesso, bem como para a publicidade de determinados atos contidos nos processos por meio de sistema como o *e-SAJ e o e-PROC*.

Partindo do avanço tecnológico existente há uma necessidade de avançarmos também no âmbito investigativo do século atual, utilizando a internet como um gerador de evidências para facilitar o acesso aos dados para fins processuais.

Diante dessa necessidade, o Marco Civil trouxe a obrigatoriedade do armazenamento de dados de conexão no seu artigo 13, que dispõe:

> 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 (BRASIL, 2017b).

Também, trouxe elencado no artigo 15 à obrigatoriedade do armazenamento de dados de acesso.

> O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. (BRASIL, 2017b)

Barreto e Brasil lecionam que há uma diferenciação entre dados de conexão e os dados de acesso. Para exemplificar o tema, colaciona-se o entendimento dos autores:

> O primeiro é o conjunto de informações referentes a data e hora de inicio e termino de uma conexão a internet, sua duração e o endereço

> de IP utilizado pelo terminal para o envio e o recebimento de pacotes de dados. Já o segundo é definido como o conjunto de funcionalidades referentes a data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço de IP (BARRETO & BRASIL, 2016, p. 62).

Em outras palavras os dados de conexão servem basicamente para identificar o momento que o IP de identificação do usuário conectou a internet e qual o período em que ocorreu a sua permanência na rede. Já nos dados de acesso, é identificado o que o usuário acessou na rede, quais os sites, conteúdo visitados por ele.

4.2.1 A iniciativa da vítima

Diante da vulnerabilidade da segurança no meio digital, homens, mulheres, crianças e adolescentes sofrem constantemente ataques pela internet. Pode-se dizer que o ambiente virtual esconde o rosto delituoso, isso faz com que o crescimento dos *ciberdelitos* seja constante.

Spencer Toth Sydow colabora com o tema expondo que

> [...] a rede mundial de computadores mostra-se um ambiente propício constantemente para a execução de delitos informáticos, especialmente porque sua estrutura propicia a oportunidade, no sentido que a contemporaneidade por si só traz a vítima para o ambiente e a vulneraliza (SYDOW, 2015, p. 208).

Um dos elementos para a resolução dos crimes digitais é a iniciativa da vítima. A partir disso, pode-se iniciar a investigação dos atos cometidos pelo *cibercriminoso*. Nesse sentido, Sydow leciona que:

> [...] apesar da existência do fato perpetrado por alguém, ainda assim afasta-se do Estado o poder-dever de punir, porquanto demovida a antijuridicidade da conduta pela ação do titular do bem jurídico atingido que aceita a lesão, anuindo com seu consentimento (SYDOW, 2015, p. 236).

Quando se trata de crimes contra crianças e adolescentes, nos casos de pornografia infantil ou pedofilia, qualquer pessoa que tenha acesso ao conteúdo publicado pode realizar o registro do ocorrido desde que seja maior de 18 anos.

As denúncias de *cibercrimes* podem ser realizadas nas delegacias de polícia civil. Vale ressaltar que todos os estados do Brasil possuem delegacias especializadas em crimes virtuais que disponibilizam o acesso ao Boletim de Ocorrência *online*. Em Santa Catarina por exemplo, temos o site www.pc.sc.gov.br que possui a ferramenta de registro de boletim de ocorrência online.

Neste sentido extrai-se o conteúdo informativo do site:

> A Delegacia de Polícia Virtual é um serviço de registro de ocorrências disponibilizado ao cidadão via Internet, 24 horas, por dia e sete dias na semana. Desde março de 2002, a Polícia Civil de Santa Catarina disponibiliza este serviço de autoatendimento na qual é o próprio cidadão é quem efetua o registro. Seu objetivo é oferecer ao cidadão agilidade, conforto e confiabilidade no registro de ocorrências via internet, do conforto de seu ambiente doméstico ou profissional, sem a necessidade de deslocamento até uma Delegacia de Polícia. (PMSC, 2017)

Outra ferramenta de acesso a denúncias *online* é o site new.safernet.org.br que se trata de uma organização não-governamental e sem incentivos políticos, para que a as vítimas de crimes contra a internet possam realizar as denúncias de *cibercrimes*.

Todo crime denunciado em uma das ferramentas legais existentes são a porta do início das investigações dos crimes digitais. Todos os dados de ataques ou *ciberdelito*s estão disponibilizados no site www.cert.br, que extrai os dados em estatísticas para a informação ás autoridades e a população.

4.2.2 O armazenamento de IP

Internet Protocol é o nome dado à sigla IP, que se conceitua como números de protocolos lógicos onde definem a identidade de cada usuário na rede de internet e também de dispositivos que estejam conectados em redes por um provedor de conexão.

É importante frisar que além dos IP de usuários, temos IP de equipamentos como roteadores, computadores e câmeras de segurança.

Para Barreto e Brasil, “O endereço de IP é o código atribuído a um terminal (computador, por exemplo) de uma rede para permitir sua

identificação, definindo segundo parâmetros internacionais" (BARRETO & BRASIL, 2016, p. 12).

Para ilustrar, o IP equivale ao CPF de uma pessoa física, é uma forma de identificar usuários, provedores e equipamentos.

No que tange a identificação digital de um usuário na rede de internet, temos IP público e IP fixo. No primeiro, a cada início de conexão muda-se o número de protocolo lógico, ou seja, muda o número de IP identificador, este basicamente é o modelo de identificação utilizado por provedores de conexão e acesso à internet.

Neste sentido é disponibilizado ao provedor um bloco de IP com no mínimo 3 mil protocolos de IP para distribuição aos clientes. A cada conexão, um IP é logado no sistema do provedor identificando o usuário.

Já no segundo o IP fixo, do bloco de IP do provedor, poderão ser disponibilizados para usuários que necessitem de IP especifico para a configuração de determinado dispositivo ligado à internet. Ocorre com usuários que necessitem configurar sistema de segurança com câmera IP ou para jogos online.

Para aprofundar extrai-se o tema de Endereçamento IP, do Instituto Federal de Santa Catarina com sede na cidade de Camboriú.

> O endereço IP (v4) é um número de 32 bits com 4 conjuntos de 8 bits (4x8=32). A estes conjuntos de 4 bits dá-se o nome de octeto. Um exemplo de um endereço IP é: 192.168.1.10. Podemos dizer que um endereço IP tem duas partes: - a identificação da REDE - a identificação do *host* dentro dessa rede (*host* é um terminal, um nó da rede – um computador, impressora, *router, switch*...) (IFSC, 2017).

A identificação através do IP no acesso do usuário ficará registrada no provedor de conexão à internet e identificará o conteúdo utilizado por aquele IP no acesso ao provedor de aplicações da internet.

Trazendo a identificação dos usuários aos crimes digitais, o IP do provedor de conexão será identificado pela autoridade policial no site www.cgi.br, onde se buscará o endereço físico da matriz, seu ramo de atividade e se está homologada ou autorizada perante a Anatel para exercer suas atividades de comunicação.

Após esse primeiro passos serão requeridos ao provedor através de mandado judicial, a identificação em IP do bloco de seu AS o horário e os dados completos do usuário que utilizava este IP no momento do delito cibernético.

Estando no prazo legalmente estabelecido pelo Marco Civil, o provedor de conexão deverá, obrigatoriamente, fornecer os dados cadastrais à autoridade policial, bem como o provedor de aplicação deverá fornecer os dados do acesso do IP.

Ao passo que será requerido o protocolo de IP ao provedor de conexão para fins de identificação do usuário, será também requisitado ao provedor de aplicações os conteúdos abordados por aquele IP na navegação da rede, sendo necessário que se identifique exatamente o conteúdo e o tempo em que ficou conectado.

4.2.3 Os *Logs* de acesso e veracidade da evidência digital

O Marco Civil define em seu artigo 5º que a internet é um sistema constituído em conjunto de protocolos lógicos, estruturando em escala mundial para o uso público e irrestrito com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes. (BRASIL, 2017b).

A comunicação em massa é uma garantia da lei do Marco Civil da internet e da Constituição Federal, contudo, deve-se frisar que o uso irresponsável da rede pode acarretar dano e através do dano haverá uma sanção.

Muito se discutiu a respeito do armazenamento de *Logs* para fins de investigação. Barreto e Brasil (2016, p. 51). Os autores discorrem que é valido ressaltar que essa medida não foi adotada no Brasil e sim em reuniões do Grupo G8, onde criou-se a cooperação entre países, para iniciar uma rede que visasse o rápido armazenamento de dados ou evidencias eletrônicas para que se pudesse investigar os criminosos e suas localizações (BARRETO & BRASIL, 2016, p. 51).

Para que se identifique horário e o usuário a lei estabelece que o provedor de conexão e aplicação deva armazenar os *Logs* de acesso através do IP, como são conhecidos.

> *Log* é uma expressão empregada para descrever os rastros (histórico) em um sistema eletrônico. Os *Logs* são importantes meios de prova computacional, pois permitem a identificação de quem praticou certo ato em ambiente eletrônico, incluindo ilícitos de cunho civil e penal. O *Log* também é conhecido como *Log* de dados (MPSP, 2017).

O IP serve necessariamente para identificar um usuário na rede de internet. Contudo, os provedores de acesso devem ter rigorosamente os dados pessoais e técnicos de cada usuário através de coleta de dados pessoais para o armazenamento de *Log*. Vale ressaltar que a Anatel já determinava antes da promulgação do Marco Civil a guarda dos registros de acesso dos usuários, contudo, o período para o armazenamento destes dados que antes eram 2 (dois) anos passou a 1 (um) ano, podendo, através de determinação judicial, o tempo de armazenamento ser aumentado (BRASIL, 2017b).

O *Log* possibilita o armazenamento de dados do usuário bem como a guarda da “evidência digital”. Entretanto há um árduo trabalho da Polícia especializada e do Ministério Público para a resolução dos casos envolvendo evidencias digitais

Barreto e Brasil conceituam a vulnerabilidade da evidência digital, neste sentido:

> Caracteriza-se por ser volátil, anônima (em princípio), alterável e/ou modificável, bem como pode ser eliminada a qualquer instante. Arquivos temporários, *cookies*, horário de inicialização de um computador e *Logs* de acesso são exemplos de evidencias digitais (BARRETO & BRASIL, 2016, p. 29).

Apesar de ser garantido pela legislação a guarda dos *Logs* para armazenamento de informações, o delito cometido pela internet pode ser modificado ou alterado com facilidade.

Neste interim, Barreto e Brasil, mencionam que

> [...] cabe ao responsável pela investigação a identificação, coleta e análise da evidência de maneira correta. A integridade e a

> autenticidade da informação devem ser demonstradas através da cadeia de evidências (BARRETO & BRASIL, 2016, p. 30).

Com base nesse pressuposto, cabe a polícia e ao Ministério Público a investigação dos dados de armazenamento e, com a colaboração dos provedores de aplicação e de conexão, a verificação da integral autenticidade da informação.

Dois pontos devem ser analisados na investigação destes crimes: a) deve ser colhido às evidências dos dados originais extraídos pela internet e; b) deve verificar se a ordem da evidência não foi alterada (BARRETO & BRASIL, 2016, p. 30).

Assim, cabe identificar o fato original da página onde ocorreu o delito, e o que ocorreu após o ato, verificando se houve algo que indicasse a mudança do conteúdo.

Outrossim, para que sejam válidas, as evidências extraídas em investigações, é necessário que se adote algumas medidas:

> Ressalta-se, por oportuno, que a preservação perderá sua eficácia caso não haja protocolo de representação judicial no prazo de sessenta dias a contar da data do requerimento de preservação de evidencias ou haja indeferimento do pedido (BARRETO & BRASIL, 2016, p. 30).

Determinadas evidencias devem ser analisadas pelos investigadores dos crimes cibernéticos, dentre elas o prazo jurisdicional válido para o protocolo de coleta de evidências infracionais dos atos delituosos que é de 60 dias.

Segundo exemplificam Barreto e Brasil, algumas plataformas de sites de relacionamento estão aderindo a protocolos online de requerimento de evidência digital. Para tanto, é necessário solicitar ao site através de uma plataforma disponibilizada, o armazenamento dos dados e *Logs* do investigado. Após isso é concedido um prazo de 90 dias para a apresentação da Ordem Judicial (BARRETO & BRASIL, 2016, p. 33).

> A plataforma para auxilio as autoridades policiais ainda faz uma diferença entre registros de informações da conta e das que contenham o conteúdo de comunicação, Para o primeiro caso, necessita de uma ordem judicial o fornecimento de cabeçalho de mensagem e endereço de IP (*Logs* de acesso com início e fim de

> cada conexão, além de registros básicos de usuários, tais como: nome completo, endereço, conta de e-mail, telefone registrado em caso de verificação em uma segunda etapa, dentre outros dados uteis. Quando se tratar de conteúdo de comunicações, em vídeos, publicações no mural e informações de localização, a plataforma exige mandado de busca do telemático ou a interceptação telemática para fornecê-lo (BARRETO & BRASIL, 2016, p. 33).

Somente autoridades policiais munidas de ordem judicial podem obter acesso as evidências digitais, no caso de evidências armazenadas em plataformas de redes sociais, inicialmente são válidos os dados investigativos, para posteriormente apresentar a ordem judicial.

Outrossim, vale lembrar que todas as plataformas de redes de relacionamento em que há uso por brasileiros estão sujeitas aos prazos estabelecidos pelo Marco Civil da Internet, no que tange ao armazenamento de *Logs*. Em outras palavras, redes como *Facebook, Instagram e WhatsApp*, estão sujeitas aos prazos e normas da legislação brasileira.

Para que os dados de *Logs* sejam válidos como prova, é necessário que se cumpra os requisitos anteriormente mencionados. No que refere ás mensagens instantâneas, onde não há um armazenamento dos dados, como no *WhatsApp*, é valido como prova o *printscreen* da página onde ocorreu o delito. Contudo, deve-se ater-se a um elemento básico, o registro da conversa em ata notarial no cartório.

Neste sentido Barretos e Brasil lecionam que:

> A finalidade da Ata Notarial é determinar a existência de um fato que tenha relevância jurídica. É lavrado por um notário, dotado de fé pública, que não poderá emitir nenhum juízo de valor sobre o que está vendo, apenas deve narrar o que está observando, sem nenhuma alteração do conteúdo. Apesar de ser um instrumento ainda pouco conhecido, tem sido bastante utilizado na preservação de fatos ocorridos na internet (BARRETOS & BRASIL, 2016, p. 41).

Esta medida para validação em ata notarial é necessária, pois há uma facilidade em burlar ou omitir fatos ou artigos em *printscreen*. Para que seja aceita como válida, essa evidência necessita ser documentada por quem detenha fé pública.

A guarda de *Logs* notadamente é o meio de acesso mais eficaz para a investigação de *cibercrimes*. Para que seja eficaz como prova é necessário que a vítima tenha agilidade na denúncia, que a Polícia Civil seja ágil nas

investigações e que os provedores de conexão e aplicação colaborem no armazenamento de dados.

4.3 A IMPLEMENTAÇÃO DE PONTOS DE ACESSO À INTERNET GRATUITOS NO MUNICÍPIO DE CRICIÚMA.

Vivemos na era da informação. A modernidade avançou ao ponto de a inteligência artificial ser colocada em prática. Robôs atualmente estão sendo inseridos no mercado, substituindo a mão de obra de humanos.

A assertiva acima é apenas um ponto, bem avançado, da era digital, que facilitou a informação e o acesso a inteligências movidas por máquinas, dentre elas, o computador, que em épocas atrás, era apenas uma ferramenta que transportava dados via internet para fins militares.

No ano de 2014, a ONU manifestou-se acerca da possibilidade de inserção da internet como um direito humano básico. Ariana Chagas Gerzson Knoll em nota ao jornal digital Gazeta do Povo, trouxe o posicionamento da Organização das Nações Unidas, vejamos:

> O acesso à internet, assim como o acesso à água, à luz foi declarado direito humano básico pela ONU este ano. Fato que foi reforçado pelo relator dos Direitos Humanos da Organização das Nações Unidas (ONU), Frank la Rue, no dia 17 de julho de 2014, em San Salvador, El Salvador, durante a Sétima Reunião Regional Preparatória para o Fórum de Governança da Internet.
> Uma das reflexões em destaque nesta reunião foi sobre o papel da internet como apoio ao crescimento econômico local. A conclusão é de que nos locais onde é disponibilizado mais acesso à rede, maior é a possibilidade de alfabetização para as crianças, assim como o acesso ao ensino superior para os jovens, além de maior desenvolvimento econômico para as mulheres e suas famílias (KNOLL, 2014).

Por certo que a acessibilidade digital é um avanço em nossos tempos, onde facilita a sociedade dispor de comunicação onde quer que esteja.

É importante mencionar que a Constituição Federal do Brasil, garante em seus dispostos o direito à informação. Com a promulgação do Marco Civil foi garantido o direito à internet como um direito fundamental à cidadania.

É inegável que a agilidade da informação contida na internet é um grande avanço na era atual. Políticas públicas estão sendo implementadas em vários estados para garantir o direito à internet para o acesso de todos, inclusive, em julho de 2017, foi aprovado a PL 2021/2011 que dispõe da obrigatoriedade de órgãos públicos, autarquias e entes federados a disponibilizarem internet gratuita em pontos públicos (CÂMARA DOS DEPUTADOS, 2017a).

Neste interim, extrai-se dispositivos contidos no projeto que está em fase de conclusão, necessitando apenas do parecer dos órgãos de tecnologia do governo.

> Artigo 1º - Os órgãos da administração direta, e indireta, além das instituições custeadas com recursos públicos em âmbito federal, estadual e municipal, deverão disponibilizar canal de conexão sem fio à rede mundial de computadores com acesso universal e gratuito;
> Artigo 2º - O canal de conexão deverá funcionar vinte e quatro horas diárias e, caberá à administração pública tomar as medidas necessárias para o funcionamento da rede em ao entorno do prédio onde estiver instalado o órgão, mesmo nos horários nos quais não haja expediente;
> Artigo 3º - Os órgãos da administração pública deverão implantar o sistema de acesso à rede mundial de computadores em até cento e oitenta dias a contar da publicação da presente Lei;
> § 1º - Os órgãos deverão dotar o canal disponibilizado de filtros que impeçam o acesso à pornografia e conteúdo impróprio, bem como poderão dotar o sistema de dispositivo que detecte a possível existência de crimes como a pedofilia e a obtenção indevida de dados bancários, além de outros crimes que possam ser detectados pela rede;
> § 2º - Caso seja constatada a possível existência de crime, caberá ao responsável pela rede, que deverá ser nomeado pela autoridade responsável pela repartição, comunicar imediatamente a Polícia Federal;
> Artigo 4º **-** Os órgãos da administração pública ligados à segurança e soberania nacional, estadual e municipal ficam dispensados da obrigação prevista nos artigos antecedentes (CÂMARA DOS DEPUTADOS, 2017a, grifou-se).

Dispõe o projeto a obrigatoriedade da instalação de pontos de internet gratuitos oferecidos pelo governo. Contudo, há de se mencionar que o texto contido no artigo 3°, parágrafo 1°, restou modificado em sua última pauta, excluindo o filtro de segurança no acesso aos conteúdos impróprios, pois os dispositivos de acesso serão os de propriedade do cidadão, não podendo a administração pública direcionar o seu uso. Contudo, deverão os órgãos

públicos adotar as medidas necessárias a fim de garantir a segurança aos usuários (CÂMARA DOS DEPUTADOS, 2017b).

O filtro de segurança, antes assegurado no projeto de lei, tinha por finalidade filtrar os sites frequentados pelos usuários. Assim, quando o usuário viesse a usar a rede para cometer um ato ou para se sujeitar a um conteúdo improprio, o filtro de segurança negaria a conexão.

Apesar do andamento no Congresso da PL 2.021 de 2011, algumas Prefeituras já estão disponibilizando em diversas cidades do Brasil pontos de Wi-Fi gratuitos para a chamada inclusão digital a população. Rodoviárias, aeroportos, supermercados, lanchonetes, disponibilizam cada vez mais o acesso gratuito à internet em suas instalações.

Sobre o tema, colaciona-se o entendimento de Franklin Dias Coelho:

> A visão de inclusão digital como inserção das comunidades na sociedade do conhecimento deve se materializar pela disseminação e garantia do direito à informação como elemento constituinte do direito à cidade e deve ser assegurada pela implantação de redes que permitam o acesso universal da população às redes mundiais de informação (CGI, 2010, p. 193).

No ano de 2015, a Câmara dos Vereadores de Criciúma teve como pauta um projeto de lei de autoria do vereador Vanderlei Zilli que determinava o acesso via Wi-Fi gratuito a população. A PL de número 21/2015 determinava “a disponibilização de sinal de internet sem fio (Wi-Fi) nas repartições da administração pública municipal direta e indireta e das autarquias, para acesso universal e gratuito à população do município de Criciúma” (CÂMARA DOS VEREADORES, 2015).

Dentre os dispostos na PL 21/2015, extrai-se os artigos 4º e 5º que previam a segurança da rede de internet fiscalizada pela administração pública.

> Art. 4º O canal de conexão deverá funcionar em horário determinado pelo órgão e caberá à administração pública tomar as medidas necessárias, podendo realizar parcerias para o funcionamento da rede no entorno do prédio onde estiver instalado o órgão.
> Art. 5º Os órgãos deverão dotar o canal disponibilizado de filtros que impeçam o acesso a pornografia e conteúdo impróprio, bem como poderão dotar o sistema de dispositivo que detecte a possível existência de crimes como a pedofilia e a obtenção indevida de dados bancários, além de outros crimes que possam ser detectados pela rede (CÂMARA DOS VEREADORES, 2015).

O projeto foi arquivado, pois em análise jurídica, se mostrou inconstitucional por invadir a competência do poder Executivo e por causar despesa (CÂMARA DOS VEREADORES, 2015)

Posteriormente no ano de 2016, o PROCON em parceria com a Prefeitura Municipal de Criciúma anunciou um projeto de implementação de pontos de Wi-Fi gratuitos à população criciumense, projeto este colocado em prática ainda no exercício do governo de 2016. “O projeto teve início em dezembro de 2015 através de uma parceria entre a Administração Municipal e a Câmara de Dirigentes Lojistas” (CIDADE DIGITAL, 2016).

O primeiro ponto de Wi-Fi gratuito foi disponibilizado em dezembro de 2015, na região central de Criciúma, posteriormente outros 6 (seis) bairros foram contemplados com a medida. No ano de 2016 outros 11 pontos de internet foram disponibilizados, dentre eles, nos terminais urbanos de ônibus (CRICIÚMA, 2016).

A ideia inicial da disponibilização de internet gratuita era assegurar a conectividade, bem como assegurar a segurança no acesso aos pontos públicos.

Neste interim colaciona-se trecho da nota emitida pela Prefeitura de Criciúma.

> Para que o cidadão possa utilizar o serviço, o usuário terá que realizar um cadastro com CPF, número de telefone e senha. Cada pessoa poderá utilizar o serviço por aproximadamente 1h 30 min diários, sendo que a cada 30 minutos haverá queda de sinal, fazendo com que seja necessário a reconexão por parte do usuário. A internet gratuita nas imediações da Praça Nereu Ramos atende a um pedido do Conselho Municipal de Cultura, feito no ano de 2012 (CRICIÚMA, 2015).

Inicialmente previa-se a criação de um cadastro ao usuário para poder conectar-se a internet. Atualmente os pontos estão sendo utilizados sem que seja necessário o cadastro inicial. Ou seja, a pessoa se conecta na rede pública sem cadastrar-se e dispõe do uso da internet por tempo indeterminado.

Diante de falta de cadastro no acesso à internet em pontos públicos, a conexão apresenta-se vulnerável, pois diversos fatores atingem a segurança da navegação, podendo ser interceptada por terceiros a fim de cometerem crimes e subtrair informações.

Outro fator que poderá ocorrer diante da vulnerabilidade é o acesso malicioso de usuários a fim de, através daquela conexão, cometerem algum ilícito previsto na legislação.

4.4 A NECESSIDADE DE ADEQUAÇÃO DE PONTOS DE WI-FI EM LOCAIS PÚBLICOS

Muito se tem comentado a respeito da conectividade em redes públicas, sinais de longa distância capazes de conectarem milhares de pessoas, facilita o acesso à internet.

Frankling Dias Coelho colabora ao dizer que:

> A questão do acesso à internet, que esbarrava na barreira tecnológica, vem sendo quebrada pela tecnologia de transmissão sem fios. Com sistemas que fazem uso de satélites e transmissão sem fio para longas distâncias, rompe-se o mito de que os sistemas locais de comunicação digital deveriam se restringir ao âmbito de operação das grandes empresas de telecomunicações. Começam a surgir sistemas locais de comunicação digital, experiências hoje realizadas em comunidades e municípios (CGI, 2010).

Atualmente, restaurantes, supermercados, livrarias, hotéis, têm um ponto de acesso à internet gratuito a seus clientes, porém são poucos que asseguram a acessibilidade segura ao público. Para confirmar essa afirmativa extrai-se o comentário do Ministério Público de São Paulo em seu manual de investigação cibernética.

> É muito comum encontrar cybercafés e *lan-houses* instalados nas cidades brasileiras. A maioria não mantém nenhum registro de usuários, o que praticamente impede a investigação de eventuais crimes por eles cometidos, já que não é possível identificá-los. Em algumas cidades e Estados há leis que obrigam esses estabelecimentos a manter um cadastro de seus usuários; é preciso admitir, porém, que o grau de eficácia dessas normas é muito pequeno. Outro problema sério que deverá ser enfrentado nos próximos anos é o uso crescente de sistemas de transmissão sem fio (Wireless ou Wi-Fi). A tecnologia permite a conexão entre equipamentos de forma simples e fácil, pois os dados são transmitidos através de ondas eletromagnéticas. A maioria dos notebooks comercializados nos últimos meses já vem com a facilidade. Apesar das muitas vantagens do sistema (mobilidade, flexibilidade, custo reduzido, instalação simples...), há duas desvantagens que facilitam a prática de crimes: a) a vulnerabilidade a acessos não autorizados; e b) a dificuldade de identificação do

> computador que acessou a rede, através desse sistema: com efeito, qualquer pessoa que estiver na área de abrangência das ondas emitidas pelo ponto de acesso poderá praticar, anonimamente, toda a sorte de delitos. Considerando que as redes sem fio já estão funcionando em aeroportos, faculdades e cafés nas grandes cidades brasileiras, será preciso encontrar rapidamente formas de tornar o sistema mais seguro (MPSP, 2006).

O Comitê Gestor de Internet leciona a respeito de segurança na internet, neste sentido colaciona-se o entendimento:

> Os provedores de acesso da Internet (comerciais, acadêmicos, governamentais, entidades de classe, organizações não governamentais, etc.) são os responsáveis pelo acesso final dos usuários na rede. Cabe a eles prover acesso dentro de condições mínimas de segurança, confiabilidade e privacidade, bem como providenciar meios que torne possível a identificação de práticas ilícitas ocorridas através da rede. Muitas vezes, em virtude de falhas, as contas dos usuários finais são utilizadas por terceiros implicando com isso em prejuízos e riscos desnecessários (CGI, 2017).

Com base nessa análise, entende-se que os órgãos públicos como a Prefeitura de Criciúma, têm o dever de cumprir com o que dispõe o Marco Civil da Internet, assegurando a privacidade e a segurança dos usuários que conectam à rede de internet. Nesse sentido, deve o município prever o cadastro do usuário para a guarda de *Log* na identificação da navegação.

Quando se trata de um provedor de internet, pessoa jurídica, devidamente licenciada pela ANATEL para prestação de serviços SCM, é necessário que este tenha sempre atualizado o cadastro de seus clientes, isso inclui, documentos pessoais, endereço físico e eletrônico e telefones de contato.

Igualmente, para que se possibilite a identificação do usuário na rede, é disponibilizado no acesso do usuário um protocolo de IP, que armazenará os acessos de cada usuário.

Partindo desse pressuposto, quando se tem uma rede Wi-Fi pública, disponibilizando acesso à internet sem cadastro, a vulnerabilidade da rede é ainda maior, pois caso ocorra qualquer delito, crime pela internet, não se há uma identificação do usuário que cometeu o ato ilícito.

Outrossim, muito se tem estudado a respeito da vulnerabilidade da rede Wi-Fi que recentemente foi descoberta uma falha na segurança.

> We discovered serious weaknesses in WPA2, a protocol that secures all modern protected Wi-Fi networks. An attacker within range of a victim can exploit these weaknesses using key reinstallation attacks (KRACKs). Concretely, attackers can use this novel attack technique to read information that was previously assumed to be safely encrypted. This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, and so on. The attack works against all modern protected Wi-Fi networks. Depending on the network configuration, it is also possible to inject and manipulate data. For example, an attacker might be able to inject ransomware or other malware into websites[11] (KRACKATTACKS, 2017).

O sistema de Wi-Fi que transporta o sinal de internet aos clientes possui uma grave falha que torna a navegação vulnerável e com isso possibilita que o dispositivo seja infectado por virus para obter informações e ocasionar qualquer um dos crimes comentados anteriormente.

Neste sentido, o grupo PSafe ,discorreu a respeito do uso e sua vulnerabilidade , explanando que invadir a segurança de um Wi-Fi público não é muito dificil, pois até o *Google* ensina com tutoriais a invadirem redes. (PSAFE, 2015)

E ainda, segundo o grupo PSafe:

> Um fato que pode agravar a questão é que as pessoas estão mais preocupadas com desempenho e velocidade do acesso à internet do que com questões de segurança.
> 49,75% dos usuários *Android* utilizam redes de Wi-Fi públicas. Destes, 86,03% assumem conversar via conexão de internet grátis, 67,23% se preocupam com a velocidade de conexão, 62,05% consideram Wi-Fi público problemático mesmo com senha e 49,14% terão problemas de segurança em relação ao Wi-Fi público, contra apenas 5% que estão cientes dos problemas de segurança para quem utiliza Wi-Fi público (PSAFE, 2015)

Em se tratando dessa vulnerabilidade, no ano de 2013, foi verificado que no aeroporto de Congonhas em São Paulo, havia pontos de Wi-Fi públicos vulneráveis a ataques cibernéticos. A rede *AirTight Networks*, especialista em

[11] Descobrimos graves pontos fracos no WPA2, um protocolo que assegura todas as redes Wi-Fi protegidas modernas. Um invasor ao alcance de uma vítima pode explorar essas fraquezas usando ataques de reinstalação de chaves (KRACKs). Concretamente, os atacantes podem usar esta nova técnica de ataque para ler informações anteriormente assumidas como criptografadas com segurança. Isso pode ser abusado para roubar informações confidenciais, como números de cartão de crédito, senhas, mensagens de bate-papo, e-mails, fotos e assim por diante. O ataque funciona contra todas as redes Wi-Fi protegidas modernas. Dependendo da configuração da rede, também é possível injetar e manipular dados. Por exemplo, um invasor pode ser capaz de injetar ransomware ou outro malware em sites. (Tradução nossa)

segurança no acesso à internet, identificou através de varreduras, riscos potenciais de ataques em pontos de acesso via internet no aeroporto de Congonhas (CONVERGÊNCIA DIGITAL, 2013)

> Além dos 86 access points que não estavam protegidos por nenhum tipo de senha, foram localizados dez pontos com apenas senhas do tipo 'WEP', consideradas fracas. Enquanto isto, três dispositivos encontrados na rede realizavam operações impróprias, com a falsificação de identidades de usuários de rede móvel (SSIDs) (CONVERGÊNCIA DIGITAL, 2013).

A acessibilidade segura garante o bom uso da internet, porém, sem a segurança os usuários são vulneráveis a vários tipos de crimes. O Marco Civil se preocupou com a guarda de *Log* para solucionar problemas decorrentes de falta de segurança, contudo, não há, em legislação, dispositivos que prevê a precaução relacionada à segurança nas redes de Wi-Fi.

4.5 A OBSCURIDADE DO MARCO CIVIL NO QUE TANGE AOS ACESSOS EM LOCAIS PÚBLICOS.

O Marco Civil, em sua aprovação foi enaltecido por deter um conteúdo normativo que, inicialmente, regularia as ações via internet.

Inobstante, trouxe à lei aspectos jurídicos que regulassem a relação de consumo regida pelo Código do Consumidor e estabeleceu em seus dispositivos atos que protegessem a privacidade dos usuários.

Contudo, no que se refere a segurança do usuário na internet, a lei mostrou-se vazia e sem um conteúdo que possibilitasse sua proteção.

Por certo que o Marco Civil prevê modos que possibilitem investigação dos crimes já cometidos. Entretanto, não há na lei modos de assistência ao usuário, principalmente quando se trata de acesso a internet em locais públicos.

Vale lembrar que o Marco Civil prevê sanção de multa para provedores de acesso e conexão que não detenham o armazenamento de IP, no prazo previsto em lei, pois são estes os responsáveis jurídicos, autônomos que possuem o acesso aos *Logs* de cada usuário que se conecta a seu *backbone* seja para conexão ou aplicação a internet.

A lei não prevê a responsabilização de entes que disponibilizem o acesso à internet por meio de rede sem fio. O problema não é a disponibilização de acesso e sim o direcionamento que cada aparelho de wireless irá fazer com cada usuário que utiliza uma rede (com apenas um IP). Em outras palavras, o compartilhamento de acesso à internet por Wi-Fi não registra IP de usuários individualmente. O IP utilizado será o cadastrado no provedor de conexão à internet.

Para exemplificar, extrai-se o entendimento do especialista Tarcísio Teixeira:

> Independentemente do número de internautas que estejam acessando a internet pelo roteador Wi-Fi de um usuário, para o provedor de acesso será considerada uma única conexão identificada pelo mesmo IP. Assim, a identificação no provedor será unicamente a do número do IP atribuído àquele roteador. Por isso, compartilhar o acesso à web por Wi-Fi nada mais é do que fazer o compartilhamento do IP atribuído pelo provedor de acesso (TEIXEIRA, 2015a).

Nesse sentido, órgãos públicos, restaurantes ou qualquer estabelecimento comercial ou não, que disponibilizem o acesso à internet via Wi-Fi, utilizam-se de IP único, que direcionam o acesso individual à rede cadastrada, devem tomar como precaução que a configuração do roteador seja restrita a dados de usuários, cadastro prévio, com identificação completa.

> Mister, porém, se faz ponderar algumas medidas que os estabelecimentos podem utilizar para identificar seus respectivos usuários, tais como autenticação e aceitação formal de termos de uso antes da liberação da internet, preenchendo dados como nome completo, número da cadastro de pessoa física, registro de identidade e endereço eletrônico, para que, caso haja um cometimento de ilícito possa, aquele que forneceu a internet, identificar o transgressor por dados extras ao número de IP individual (FIUZA, NETO & JUNIOR, 2015, p. 348)

A obscuridade da legislação se faz presente no que tange a proteção do usuário antes do ilícito. Nota-se que a lei implica em indisponibilidade de *Logs* de armazenamento pelos provedores de acesso e conexão, porém não se atém ao compartilhamento de Wi-Fi em pontos públicos. Nesse interim, em termos de investigação cibernética, nada vale o armazenamento de IP do provedor de acesso e conexão se ocorrer o compartilhamento de IP via distribuição Wi-Fi.

Não obstante, não haverá possibilidade de investigação e não se poderá determinar que o órgão que compartilha Wi-Fi seja sujeito à multa ou as normas do Marco Civil, visto que este não se trata de um provedor de acesso à internet e sim um usuário que disponibiliza seu acesso público. Tampouco poderá requerer que este vigie o usuário que utiliza Wi-Fi, pois estaria ele invadindo sua privacidade.

Nas palavras de Tarcísio Teixeira:

> Caso fosse atribuída responsabilidade a quem compartilha Wi-Fi pelos atos daqueles que se utilizam do acesso sem fio para praticar algum ilícito, a este deveria ser dado o direito de vigiar o conteúdo do que está sendo acessado, postado, enviado, recebido, etc. pelo usuário. Isso seria inconcebível na relação fornecedor-cliente, exemplificativamente, além da violação da privacidade (TEIXEIRA, 2015b).

Assim, em se tratando da legislação que atualmente trata das relações na internet, temos uma ineficiência na proteção do usuário no que tange aos pontos de distribuição via Wi-Fi público, devido a vulnerabilidade da segurança no acesso à internet, e a ineficácia da investigação em locais públicos que não possibilitam o armazenamento de *Log* dos usuários na rede.

5 CONCLUSÃO

O Marco Civil da Internet é uma lei que determina as ações de cada usuário na rede de internet. A lei determina direitos e impõe deveres aos usuários e a quem disponibiliza o acesso e a aplicação da internet.

Inicialmente, foi referenciado a respeito do surgimento da rede de mundial de internet. Seu aspecto, em primeiro momento foi para fins militares que nortearam pesquisas tecnológicas durante a guerra fria. Outrossim, algumas universidades iniciaram suas pesquisas utilizando a rede de internet como experimento para a transmissão de pacote de dados, o que deu inicio a rede mundial de comunicação.

Destarte que a rede de internet facilita relações de trabalho, consumo e pessoais. Contudo, de acordo com o tema abordado, a rede de internet possui uma vulnerabilidade no que tange a segurança dos usuários nos espaços virtuais. Nesse sentido, discorreu-se no trabalho a respeito de crimes *cybernéticos* que são divididos em próprios e impróprios, sendo conceituados como atos formais, ilícitos dolosos, onde o intuito é causar dano a alguém através da rede de internet.

Os *cybercirminosos* geralmente utilizam-se da rede, pois é difícil a identificação do criminoso no mundo virtual. Diante disso, Países estão implementando politicas investigativas que possibilitam a resolução de crimes cometidos pela internet.

No Brasil o surgimento do Marco Civil delimitou a guarda de *Logs* de acesso à internet e *Logs* de aplicações a internet. O intuito dessa medida adotada pelo código é, em caso de algum crime cometido pela internet, identificar o usuário que cometer o *cybercrime*.

O desenvolvimento do presente estudo possibilitou aprofundar sobre todos os crimes cometidos pela internet, bem como os projetos de leis e as leis que antecederam o Marco Civil da Internet. Igualmente, foi analisada a competência de cada crime cometido pela internet, à territorialidade, o *modus operandi* e também o resultado de cada ação e/ou omissão de ilícitos na internet.

Em análise mais técnica, foi discorrido a respeito das características de ataques cibernéticos cometidos contra computadores, redes ou servidores,

ataques que são utilizados por governos e também por terroristas a fim de moverem o caos *cybernético* e pararem entes federados, servidores e afins.

Foi necessário adentrar na presente pesquisa nos métodos técnicos de identificação de um usuário na internet. Sendo que ele é conectado a um IP que o direciona a todas as conexões que desejar. E este IP armazena toda identificação daquele usuário. O grande questionamento foi a respeito da legislação da internet no Brasil que, a grosso modo, ainda é vista como incompleta e vazia, pois não possibilita uma segurança adequada nos relacionamentos e na proteção do usuário na rede. Por certo, o Marco Civil da Internet determina que os provedores de acesso e conexão detenham os acessos de clientes pelo prazo determinado legalmente, porém, apesar disso, a lei fica obscura no que tange ao compartilhamento de sinal Wi-Fi em pontos públicos, o que favorece a vulnerabilidade da rede de internet e acarreta graves riscos ao usuário.

O Município do Criciúma tem disponibilizado a populações locais de acesso gratuito a internet. No inicio dos projetos de compartilhamento a ideia era de disponibilizar antes do acesso um prévio cadastro para o usuário ser identificado na rede. Entretanto, isso não ocorre atualmente. Os pontos de Wi-Fi disponibilizados no município não possuem limites de acesso nem tampouco cadastro de usuário, o que acarreta uma problema a ser resolvido pelo governo, visto a vulnerabilidade que estes pontos de acesso passam a obter.

Quando ocorre uma conexão em redes publicas, sem a devida identificação, não há como rastrear as atividades de cada usuário. Para exemplificar, em uma conexão IP, há todos os protocolos de navegação, conexão e acesso. Quando há o compartilhamento deste IP via Wi-Fi, que é o que ocorre em pontos públicos, não se pode identificar o usuário caso não haja um cadastro prévio deste.

Conclui-se que são necessárias medidas de inserção no Município de Criciúma. Por certo a inclusão digital oferecida pelo Município é relevante. Entretanto a indisponibilidade de cadastro de usuário oferece risco a quem utiliza a internet nos pontos públicos. Neste sentido, é imprescindível que haja uma adequação do Município nos pontos de *Wi-Fi*, disponibilizando em seus roteadores de acesso cadastros completo de usuários e limites de banda.

Outrossim, além dessas medidas, seria necessário que os entes federados disponibilizassem um filtro de segurança na rede de internet, permitindo que a cada conexão suspeita ou indevida haja um bloqueio prévio.

Faz se necessário, além disso, a implementação de politicas que informem os riscos no uso da internet nos pontos públicos aos usuários, permitindo o conhecimento, preservando a segurança e causando a repressão dos crimes *cybernéticos*.

REFERÊNCIAS

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à luz do Marco Civil da Internet.** Rio de Janeiro: Brasport, 2016. 222 p.

BORGES, Fabiani. **Terrorismo Cibernético e a Proteção de Dados Pessoais.** 2015. Disponível em: <https://fabianiborges.jusbrasil.com.br/artigos/218335957/terrorismo-cibernetico-e-a-protecao-de-dados-pessoais>. Acesso em: 08 nov. 2017.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal: Centro Gráfico, 2017a.

_____. **Pl 151/00**. Dispõe sobre o acesso a informações da Internet, e dá outras providências. Brasília, DF, Disponível em: <http://www.camara.gov.br/sileg/integras/190128.pdf>. Acesso em: 09 nov. 2017b.

_____. Dispõe sobre o acesso a informações da Internet, e dá outras providências. **Pl 151/00**. Brasília, DF, Disponível em: <http://www.camara.gov.br/sileg/integras/190128.pdf>. Acesso em: 09 nov. 2017c

_____. **Código Penal Brasileiro.** 18. ed. São Paulo, SP: Revista dos Tribunais, 2017d.

_____. **Estatuto da Criança e do Adolescente**. 15 ed. São Paulo: Saraiva, 2017e.

BRASIL. **Informativo 335 de 2014**. 2014b Disponível em: <http://www.criminal.mppr.mp.br/modules/conteudo/conteudo.php?conteudo=1530>. Acesso em: 08 nov. 2017.

_____. **Lei 12.965 de 23 de Abril de 2014.** 2014a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 08 nov. 2017.

CÂMARA DOS DEPUTADOS. Brasil. Projeto de Lei nº 2021, de 2011. Determina a disponibilização, pelos órgãos da administração pública, de canal sem fio para acesso universal e gratuito à rede mundial de computadores pela população. **Pl**. Brasilia, DF, 2011. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=515577>. Acesso em: 08 nov. 2017.

_____. Lei nº 12737/12, de 30 de dezembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.. **Lei**. Brasilia, DF, 30 dez. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 09 nov. 2017a.

_____. Brasil. Projeto de Lei nº 84/99, de 24 de fevereiro de 1999. **PL 84/99**. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>. Acesso em: 09 nov. 2017b.

CÂMARA DOS VEREADORES. CRICIÚMA. Projeto de Lei nº 21, de 24 de agosto de 2015. Determina a disponibilização de sinal de internet sem fio (wi-fi) nas repartições da administração pública municipal direta e indireta e das autarquias, para acesso universal e gratuito à população do município de Criciúma e dá outras providências. **Pl**. Disponível em: <http://www.camaracriciuma.sc.gov.br/documento/projeto-pl-no-21-2015-22699>. Acesso em: 08 nov. 2017.

CAPEZ, Fernando. **Decisões do STJ fortalecem o combate à violência sexual contra crianças.** 2016. Disponível em: <http://www.fernandocapez.com.br/decisoes-do-stj-fortalecem-o-combate-a-violencia-sexual-contra-criancas/>. Acesso em: 08 nov. 2017.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A TRAJETÓRIA DA INTERNET NO BRASIL:** DO SURGIMENTO DAS REDES DE COMPUTADORES À INSTITUIÇÃO DOS MECANISMOS DE GOVERNANÇA. 2006. 259 f. Dissertação (Mestrado) - Curso de Engenharia,

Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006. Disponível em: <http://www.nethistory.info/Resources/Internet-BR-Dissertacao-Mestrado-MSavio-v1.2.pdf>. Acesso em: 08 nov. 2017.

CEROY, Frederico Meinberg. **Os conceitos de provedores no Marco Civil da Internet.** 2014. Disponível em: <https://jus.com.br/artigos/31938/os-conceitos-de-provedores-no-marco-civil-da-internet>. Acesso em: 08 nov. 2017.

CERT.BR: Estatísticas. 2017. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 08 nov. 2017.

CGI. Comitê Gestor Internet (Org.). **Recomendações para o Desenvolvimento e Operação da Internet no Brasil.** Disponível em: <https://www.cgi.br/pagina/recomendacoes-para-o-desenvolvimento-e-operacao-da-internet-no-brasil/202>. Acesso em: 08 nov. 2017

CONVERGÊNCIA DIGITAL. WI-FI: varredura revela alta vulnerabilidade no aeroporto de Congonhas. 2013. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=34089>. Acesso em: 08 nov. 2017.

CRESPO, Marcelo Xavier de Freitas; SANTOS, Coriolano Aurélio de Almeida Camargo. **Perfis falsos nas redes sociais e o projeto de lei 7.758/14.** 2015. Disponível em: <http://www.migalhas.com.br/dePeso/16,MI213736,81042-Perfis+falsos+nas+redes+sociais+e+o+projeto+de+lei+775814>. Acesso em: 08 nov. 2017.

CRICIUMA. **Internet Gratuita na Praça Nereu Ramos.** 2016. Disponível em: www.gov.br/procon/noticia.php?internet-gratuita-na-praca-nereu-ramos/10938>. Acesso em: 08 nov. 2017.

CRICIÚMA. **Procon de Criciúma vai disponibilizar internet gratuita em mais seis bairros.** Projeto Teve Início em Dezembro de 2015 Através de Uma Parceria Entre Administração Municipal e A Câmara de Dirigentes Lojistas, 08 nov. 2015. Disponível em: <http://redecidadedigital.com.br/noticias.php?id=1329&data=Procon de

Criciúma vai disponibilizar internet gratuita em mais sete bairros>. Acesso em: 08 nov. 2017.

DIÁRIO OFICIAL DA UNIÃO. BRASIL. 3º Turma Criminal do Tribunal de Justiça. Apelação nº 0001291-61.2017.807.0004. RAIMUNDO KLINSMAN GOMES DE LIMA. **MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS**. Relator: Des. WALDIR LEÔNCIO LOPES JÚNIOR. Brasília, DF, 03 de novembro de 2016. Brasilia,. Disponível em: <http://cache-internet.tjdft.jus.br/cgi-bin/tjcgi1?NXTPGM=plhtml06&SELECAO=1&ORIGEM=INTER&CDNUPROC=20170410013327APR>. Acesso em: 08 jan. 2017.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro.** 17. ed. SÃo Paulo: Saraiva, 2003. 7 v.

FIUZA, César Augusto de Castro; NETO, Orlando Celso da Silva; JUNIOR, Otavio Luiz. DIREITO CIVIL CONTEMPORÂNEO II. In: XXIV CONGRESSO NACIONAL DO CONPEDI, 24, 2015, Belo Horizonte. **Anais.** Florianopolis: Conpendi, 2015. p. 332 - 354. Disponível em: <https://www.conpedi.org.br/publicacoes/66fsl345/oy1ux21y/8QYtBEA7KXH4PT5A.pdf>. Acesso em: 08 nov. 2017.

GARDINI, Mayara Gabrielli. **Terrorismo no ciberespaço: o poder cibernético como ferramenta de atuação de organizações terroristas.** Belo Horizonte: Fronteira, 2014. Disponível em: <http://periodicos.pucminas.br/index.php/fronteira/article/viewFile/10461/10543>. Acesso em: 08 nov. 2017.

HORTO, Alessandra. **Perfil falso na internet dá 5 anos de prisão:** Crime de Falsidade Ideológica é praticado por quem cria páginas de terceiros na internet. 2014. Disponível em: <http://odia.ig.com.br/noticia/economia/2014-07-08/perfil-falso-na-internet-da-5-anos-de-prisao.html>. Acesso em: 08 nov. 2017.

IFSC. SANTA CATARINA. (Org.). **ENDEREÇAMENTO DE IP.** Disponível em: <http://www.ifc-camboriu.edu.br/~nildo/redes/TCP_IP/IP_Endereçamento.pdf>. Acesso em: 08 nov. 2017

INTERPOL. **Supporting member countries following global cyber-attack.** 2017. Disponível em: <https://www.interpol.int/Crime-areas/Cybercrime/The-threats>. Acesso em: 08 nov. 2017.

KNOLL, Ariana Chagas Gerzson. **ONU declara acesso à internet como direito humano básico. E a escola com isso?** 2014. Disponível em: <http://www.gazetadopovo.com.br/blogs/educacao-e-midia/onu-declara-acesso-a-internet-como-direito-humano-basico-e-a-escola-com-isso/>. Acesso em: 08 nov. 2017.

KRACKATTACKS. **Reinstallation Attacks Breaking WPA2 by forcing nonce reuse**. Disponível em: <https://www.krackattacks.com/>. Acesso em: 08 nov. 2017.

LEONARDI, Marcel Dias. **Responsabilidade Civil dos Provedores de Internet.** São Paulo: Juarez de Oliveira, 2005.

LOPES, Marcelo Frullani. **STJ relativiza artigo do Marco Civil da Internet em decisão.** 2016. Disponível em: <https://www.conjur.com.br/2016-set-02/marcelo-frullani-stj-relativiza-marco-civil-internet-decisao>. Acesso em: 08 nov. 2017.

MSSP. **CRIMES CIBERNÉTICOS: MANUAL PRÁTICO DE INVESTIGAÇÃO.** São Paulo: Procuradoria da República no Estado de São Paulo, 2006. Disponível em: <http://tmp.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInformática-versaofinal.pdf>. Acesso em: 08 nov. 2017.

NETO, João Araújo Monteiro. **ASPECTOS CONSTITUCIONAIS E LEGAIS DO CRIME ELETRÔNICO.** 2008. 192 f. Dissertação (Mestrado) - Curso de Programa de PÓs-graduaÇÃo em Direito Constitucional, Universidade de Fortaleza, Fortaleza, 2008. Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp055676.pdf>. Acesso em: 08 dez. 2017.

NETO, Mario Furlaneto; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. **Crimes na Internet e o Inquérito Policial Eletrônico.** São Paulo: Edipro, 2012. 190 p.

PAYÃO, Felipe. **Ciberguerra: EUA atacam a Coreia do Norte com DDoS.** 2017. Disponível em: <https://www.tecmundo.com.br/seguranca/122616-ciberguerra-eua-atacam-coreia-norte-ddos.htm>. Acesso em: 10 nov. 2017.

PMSC. SANTA CATARINA. POLICIA CIVIL. . **Boletins de Ocorrencia.** 2015. Disponível em: <http://www.delegaciaeletronica.sc.gov.br/inicio.aspx>. Acesso em: 08 nov. 2017.

CIDADE DIGITAL, **PROCON de Criciúma vai disponibilizar internet gratuita em mais seis bairros.** 2016. Disponível em: <http://redecidadedigital.com.br/noticias.php?id=1329&data=Procon de Criciúma vai disponibilizar internet gratuita em mais sete bairros>. Acesso em: 10 nov. 2017

PSAFE. O**s 3 maiores riscos para quem utiliza wi-fi público: Veja quais são os 3 maiores riscos para quem acessa wi-fi público sem proteção**. 2015. Disponível em: <http://www.psafe.com/blog/os-3-maiores-riscos-para-quem-utiliza-wi-fi-publico/>. Acesso em: 08 nov. 2017.

RIBEIRO, Luiz. **Os avanços tecnológicos da internet.** 2010. Disponível em: <http://www.administradores.com.br/artigos/tecnologia/os-avancos-tecnologicos-da-internet/49331/>. Acesso em: 08 nov. 2017.

SARAIVA, Antonio Heli Manzoni. **ASPECTOS GERAIS DOS CRIMES DIGITAIS E A REGULAMENTAÇÃO NO ORDENAMENTO JURIDICO BRASILEIRO.** 2010. 58 f. TCC (Graduação) - Curso de Direito, Universidade Federal da Paraíba, Campina Grande, 2010. Disponível em: <http://dspace.bc.uepb.edu.br/jspui/bitstream/123456789/6885/1/PDF- Antonio Heli Malzoni Saraiva.pdf>. Acesso em: 09 nov. 2017.

SILVA, João Miguel Almeida da. **Cibercrime: O Crime de Pornografia Infantil na Internet.** 2016. 57 f. Dissertação (Mestrado) - Curso de Ciência Juridico

Forense, Universidade de Coimbra, Coimbra, 2016. Disponível em: <https://estudogeral.sib.uc.pt/bitstream/10316/34801/1/Cibercrime_o Crime de Pornografia Infantil na Internet.pdf>. Acesso em: 08 nov. 2017.

SILVA, Leonardo Werner. Internet foi criada em 1969 com o nome de "Arpanet" nos EUA. **Folha Online.** SÃo Paulo, p. 1-1. 12 ago. 2001. Disponível em: <http://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml>. Acesso em: 08 nov. 2017.

SOBRE O SIGNIFICADO DE PEDOFILIA. SÃo Paulo: Lexml, 2005. Disponível em: <http://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:artigo.revista:2005;1000732162>. Acesso em: 10 nov. 2017.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS. In: 1° SEMINÁRIO CIBERCRIME E COOPERAÇÃO PENAL INTERNACIONAL, ORGANIZADO PELO CCJ DA UFPB, 1., 2009, João Pessoa. **Anais... .** João Pessoa: Ufpb, 2009. p. 01 - 15. Disponível em: <http://www.charlieoscartango.com.br/Images/A convencao de Budapeste e as leis brasileiras.pdf>. Acesso em: 09 out. 2017.

SOUZA, Lucas. **Competência para processar e julgar crimes virtuais.** 2017. Disponível em: <https://lucasaps91.jusbrasil.com.br/artigos/417311418/competencia-para-processar-e-julgar-crimes-virtuais>. Acesso em: 08 nov. 2017.

SYDOW, Spencer Toth. **CRIMES INFORMÁTICOS E SUAS VÍTIMAS.** 2. ed. SÃo Paulo: Saraiva, 2015. 360 p. De acordo com a lei n 12.965, de 2014-Marco Civil da Internet.

TEIXEIRA, Tarcisio. DIREITO DIGITAL: Wi-fi: riscos e aspectos jurídicos. **Carta Forense.** Vila Olimpia, p. 1-1. 07 fev. 2015. Disponível em: <http://www.cartaforense.com.br/conteudo/artigos/wi-fi-riscos-e-aspectos-juridicos/15506>. Acesso em: 08 nov. 2017.

_____. **Wi-Fi - riscos e limites da responsabilidade pelo compartilhamento.** São Paulo: Revista dos Tribunais, v. 961, nov. 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.961.02.PDF>. Acesso em: 08 nov. 2017.

TJDF. BRASIL. Tribunal de Justiça de São Paulo. Apelação nº 0001647-62.2015.8.26.0177. Rita de Cassia Guimaraes Tassi. Angélia Teixeira de Carvalho Cravo Roxo. Relator: James Siano. São Paulo, SP, 05 de agosto de 2017. **Diário Oficial da União**. BrasÍlia, . Disponível em: <https://esaj.tjsp.jus.br/cposg/show.do?processo.foro=990&processo;.codigo=RI004285N0000>. Acesso em: 08 nov. 2017a.

_____. Brasil. **Mulher é condenada a 6 anos de reclusão por crime de extorsão pela Internet**: Notícias. Notícias. 2011. Disponível em: <https://www2.tjdft.jus.br/noticias/noticia.asp?codigo=16393>. Acesso em: 08 nov. 2017b.

VIEIRA, Jair Lot. **CRIMES NA INTERNET INTERPRETADOS PELOS TRIBUNAIS.** Bauru: Edipro, 2009. 342 p.