UNIVERSIDADE REGIONAL INTEGRADA DO ALTO URUGUAI E DAS MISSÕES

URI CAMPUS DE ERECHIM

DEPARTAMENTO DE CIÊNCIAS SOCIAIS APLICADAS

CURSO DE DIREITO

CRIMES CIBERNÉTICOS: (IM)POSSIBILIDADES DE COERÇÃO

CHALIDAN ADONAI CALLEGARI TORMEN

ERECHIM

2018

CHALIDAN ADONAI CALLEGARI TORMEN

CRIMES CIBERNÉTICOS: (IM)POSSIBILIDADES DE COERÇÃO

Monografia apresentada à banca examinadora do Curso de Direito da Universidade Regional Integrada do Alto Uruguai e das Missões – URI – Campus de Erechim, como exigência parcial para obtenção do grau de bacharel em direito, sob a orientação do Professor Me. Luciano Alves dos Santos.

ERECHIM

2018

CHALIDAN ADONAI CALLEGARI TORMEN

CRIMES CIBERNÉTICOS: (IM)POSSIBILIDADES DE COERÇÃO

Monografia apresentada à Universidade Regional Integrada – URI Campus de Erechim como requisito parcial para a obtenção do título de bacharel em direito.

Aprovada em ____ de _____ de 2018.

BANCA EXAMINADORA

_____

_____

_____

Dedico este trabalho aos meus pais Darci e Matilde, com imenso carinho, pelo exemplo de vida que me deram na formação de meu caráter.

Obrigado por tudo e amo vocês incondicialmente.

AGRADECIMENTOS

Agradeço ao Professor Me. Luciano Alves dos Santos pela atenção e presteza na orientação deste trabalho.

RESUMO

No mundo globalizado que se vive a crescente evolução tecnológica fez com que as distâncias do mundo fossem reduzidas drasticamente, esse fato se deu, pelo motivo do uso de equipamentos eletrônicos, que são conectados a uma rede, chamada internet, a qual essa rede interliga vários internautas ao mesmo tempo, sendo eles de qualquer região do mundo, ocorre que em tudo que é criado para beneficio de avanço, pode ser utilizado para fazer o mal também, pessoas de má-fé, se utilizam desse meio para praticarem delitos de diversas modalidades, e todo o delito que é praticado por intermédio dessa “rede” são classificados como os crimes cibernéticos. Então o presente trabalho objetivou estudar a respeito dos casos que já aconteceram, bem como das leis que amparam tal problemática, tendo em vista as possibilidades ou impossibilidades que existem para coibir ou evitar os crimes que são praticados pela internet, dando ênfase à quais medidas de proteção que podem ser tomadas para evitar os crimes, bem como quais as ações poderão ser aplicadas no caso de sofrer um crime nesse sentido.

Palavras-chave: Crime Cibernético, coibir, medidas de proteção.

SUMÁRIO

1. INTRODUÇÃO

A internet foi o início de um grande avanço dentro do contexto do mundo globalizado, onde o fácil acesso e a rapidez em busca de informação foi um dos principais fundamentos, pois basta entrar em um site e escrever o que procura para obter as informações de forma rápida.

Tendo em vista que cada dia que se passa, mais pessoas utilizam-se da internet como meio de informação, para lazer, estudos, e venda e compra de objetos, etc. O meio está se tornando rotineiro na maioria dos países do mundo, como Wilson Dizard já dizia nos anos 2000: “A internet é um sistema de redes de computadores interconectadas de proporções mundiais, atingindo mais de 150 países e reunindo cerca de 300 milhões de computadores”. (DIZARD, 2000).

Apesar dessas facilidades e benefícios que são oferecidos em rede, esse cenário também deixa o usuário a mercê de crimes, tendo em vista que cada vez mais, criminosos se valem desse meio para praticar os mais variados tipos de crimes.

Com o advento da internet em diversos lares e lugares, os crimes que já são tipificados pelo Código Penal passaram a ser praticados pelo meio virtual, sendo que o criminoso fica “escondido através da rede”, dificultando a localização da autoria dos crimes.

Desse modo, surgiram novas modalidades de crimes que passaram a ser praticados nesse meio, surgiu-se então os denominados Crimes Cibernéticos, que apesar de fazerem parte da realidade mundial e também brasileira, carece muito de legislação específica no ordenamento jurídico brasileiro.

Diante disso, o presente trabalho de pesquisa busca inicialmente falar sobre o surgimento da internet, conceito de internet, partindo daí esclarecer o conceito dos crimes cibernéticos, delimitando os crimes em próprios e impróprios, as competências dos crimes cibernéticos. No segundo capítulo abordará as legislações que competem para os crimes cibernéticos, analisando também a evolução histórica dos sistemas de rede e informática, e encerrando o trabalho, e no último capítulo com estudo do ordenamento jurídico buscando quais os instrumentos jurídicos cabíveis para coibir ou evitar os crimes cibernéticos.

A metodologia que foi utilizada para criação desse trabalho cientifico foi a técnica de pesquisa bibliográfica.

2. SURGIMENTO DA INTERNET

O surgimento da internet se deu em meados do século XIX, em 1969, nos Estados Unidos, em plena Guerra Fria, onde os EUA utilizavam a rede como uma ferramenta de comunicação militar alternativa, caso algum pais inimigo ataca-se os meios convencionais de telecomunicações.

Antigamente a rede era chamada de "*Arpanet*[1]", (Advanced Research Projects Agency Network) sendo criada pelo Departamento de Defesa dos Estados Unidos, que desenvolveram uma rede sem nenhum controle central, inicialmente ligada a quatro computadores, que logo após se foi expandido a mais computadores, pertencentes a universidades, centros de pesquisas com fins militares e indústrias bélicas.

Segundo informações retiradas do Artigo "Tecnologias de informação e comunicação" publicado em 2010 por Liliane Silva:

> A ARPANET funcionava através de um sistema conhecido como chaveamento de pacotes, que é um sistema de transmissão de dados em rede de computadores no qual as informações são divididas em pequenos pacotes, que por sua vez contém trecho dos dados, o endereço do destinatário e informações que permitiam a remontagem da mensagem original. O ataque inimigo nunca aconteceu, mas o que o Departamento de Defesa dos Estados Unidos não sabia era que dava início ao maior fenômeno midiático do século 20', único meio de comunicação que em apenas 4 anos conseguiria atingir cerca de 50 milhões de pessoas.(SILVA, 2010)

No início dos anos 1980, foi desenvolvido o TCP/IP (Transmission Control Protocol/Internet Protocol) que possibilitou a conexão de diversas redes, aumentando drasticamente a abrangência da rede. Em 1990, a ARPAnet foi transformada em NSFnet (National Science Foundation's Network), se ligando a outras redes existentes, abrangindo redes inclusive fora dos Estados Unidos, passando a interconectar centros de pesquisa e universidades em todo mundo.

Conforme estudos foi identificado que em 1995 devido ao grande numero de usuários a internet foi transferida para uma administração não governamental:

> Em 1995, devido ao grande aumento de usuários no início da década de 90 a internet foi transferida para a administração de instituições não-governamentais, que se encarregam, entre outras coisas,

[1] **ARPANET** – rede, criada em 1969 pelo Departamento de Defesa dos Estados Unidos, que depois se tornou a Internet. (CAPRON, 2010)

> estabelecer padrões de infraestrutura, registrar domínios, etc. Exemplos dessas instituições são a Internet Society, situada nos Estados Unidos, mas atuando no mundo inteiro, e o Comitê Gestor da Internet que atua restritamente no Brasil. (MONTEIRO, 2001)

No Brasil, as primeiras iniciativas de disponibilizar internet ao público geral foi em 1995, que teve como atuação fundamental o Ministério da Comunicação e o Ministério de Ciência e Tecnologia no sentido de implantar a infraestrutura necessária e definir os parâmetros para operar em empresas privadas provedoras de acesso aos usuários.

Segundo dados do Instituto de pesquisa Nielsen na revista Veja:

> A internet no Brasil experimentou um crescimento espantoso, notadamente entre os anos de 1996 e 1997, quando o número de usuários aumentou 1000% (mil por cento), passando de 170 mil em janeiro de 1996 para 1,3 milhão em dezembro de 1997. Em janeiro de 2000, eram estimados 4,5 milhões de "internautas". Atualmente, cerca de 10 milhões de brasileiros podem acessar a Rede de suas residências. Se consideradas as pessoas que têm acesso apenas nos seus locais de trabalho, esse número sobe para 15 milhões. (REVISTA VEJA, 2000).

Todo esse volume de crescimento se refere à evolução digital, sendo que antigamente se pensava que a "era digital" seria algo para o futuro, hoje em dia a realidade é uma só, tudo, se não quase tudo está em sintonia com os sistemas de rede, estamos vivendo em um ambiente que quase tudo é informatizado.

2.1. CONCEITO DE INTERNET

Internet em poucas palavras é um conjunto de redes mundial, que teve origem inglesa , onde "*inter*" vem de internacional, e "*net*" significa rede, ou seja rede de computadores mundial.

A internet é um meio pelo qual se permite o acesso a informações de todos os tipos, além de obter uma grande variedade de recursos e serviços, como compartilhamento de arquivos, e-mails, serviços de comunicação ao vivo, redes sociais, entre outros.

Em outras palavras, buscamos uma definição na doutrina de Luis Monteiro, que ele classificou Internet como:

> A internet (ou a "Rede" como também é conhecida) é um sistema de redes de computadores interconectadas de proporções mundiais, atingindo mais de 150 países e reunindo cerca de 300 milhões de

> computadores (DIZARD, 2000) e mais de 400 milhões de usuários. Computadores pessoais ou redes locais (em um escritório, por exemplo) se conectam a provedores de acesso, que se ligam a redes regionais que, por sua vez, se unem à redes nacionais e internacionais. A informação pode viajar através de todas essas redes até chegar ao seu destino. Aparelhos chamados “roteadores”, instalados em diversos pontos da Rede, se encarregam de determinar qual a rota mais adequada. (MONTEIRO, 2011).

Do conceito de internet partimos para, o conceito de crimes cibernéticos, devido esse meio tem uma grande crescente, sendo que os usuários ficam camuflados atrás de uma tela de um computador, perdendo um pouco de vergonha, vindo a praticar delitos através desse modo.

2.2. CONCEITO DE CRIMES CIBERNÉTICOS

São de suma importância esclarecer que não existe uma única nomenclatura sobre crimes cibernéticos, e sim várias, sendo que não há um consenso sobre a melhor denominação que relacionam os delitos com a tecnologia. Segundo Antônio Chaves, cibernética é a “ciência geral dos sistemas informantes e, em particular, dos sistemas de informação” (CHAVES, Antônio apud SILVA, Rita de Cássia Lopes. Direito Penal e Sistema Informático, p. 19). Sendo a ciência da comunicação e dos sistemas de informação, um termo mais amplo e apropriado, a denominação dos delitos tratados nesse projeto de pesquisa sobre crimes cibernéticos.

Através do conceito analítico finalista de crime, pode ser chegar a conclusão de que os crimes cibernéticos são todas as condutas típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática.

Fabrizio Rosa conceitua o crime cibernético, como sendo:

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O ‘Crime de Informática’ é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o ‘Crime de Informática’ pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos

> crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc. (ROSA, 2002, p. 53)

Já Sérgio Marcos Roque (2005, p. 25) conceitua crimes cibernéticos como sendo "toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material."

Portanto, crimes cibernéticos são todas as condutas típicas, antijurídicas e culpáveis contra ou praticadas com a utilização de instrumentos eletrônicos que podem entrar em rede, através da internet.

A autora contemporânea Patricia Peck Pinheiro em seu livro Direito Digital (2007), define com exemplos duas modalidades de crimes virtuais, que segue abaixo:

> Os crimes virtuais têm modalidades distintas, dependendo do bem jurídico tutelado. Nesse sentido, podemos dar como exemplo o crime de interceptação de dados, que tem como bem jurídico tutelado os dados, ou seja, o que se quer é proteger a transmissão de dados e coibir o uso dessas informações para fins delituosos, como, por exemplo, captura de informações para envio de "e-mail bombing[2]", e o "e-mail com vírus[3]", o "spam[4]". Esse tipo penal protege também a questão da inviolabilidade das correspondências eletrônicas. (PINHEIRO)

Existe uma classificação que divide os crimes cibernéticos em dois tipos: os Crimes Cibernéticos Próprios e os Crimes Cibernéticos Impróprios. Os quais a seguir adentraremos no assunto.

---

[2] **E-mail Bombing** – é o envio de e-mails imensos ou vários e-mails, por isso Bombing, que se refere como "explosão, ou bomba" em inglês. De qualquer forma pode vir a causar atraso na recepção e gasto adicional com conta de internet, por exemplo. Nesses casos seria aplicável o art. 163 do Código Penal (crime de dano).

[3] **E-mail com vírus** – é quando a pessoa recebe um email, e vem anexado um vírus, é muito comum nos dias de hoje, e-mails com tentativas de vírus através de propostas bancárias, ou solicitação de dados por e-mail. Nesse sentido a legislação prevê os artigos 151, § 1º, II e III, e 163 do Código Penal, com aplicação do artigo 65 da LCP, com pena de prisão simples de 15 dias a 2 meses, ou multa por perturbação da tranquilidade.

[4] **Spam** – Propaganda maciça na Internet, feita em geral com software especialmente projetado para enviar solicitações aos usuários por meio de e-mail. (CAPRON, 2010)

2.2.1 CRIMES CIBERNÉTICOS PRÓPRIOS

São aqueles que só podem ser praticados na informática, ou seja, a execução do crime e a consumação ocorrem nesse meio, trata-se de tipos novos em que o bem jurídico tutelado é a informática, são os crimes praticados contra os dados da vitima que utiliza o computador, ou o celular da mesma. Conforme explica a Marco Túlio Viana, em seu livro Fundamentos de direito Penal Informático; “São aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados).” (VIANA, 2003)

É estas condutas que são praticadas por “*hackers*[5]”, tanto a invasão de sistemas, modificar, alterar, inserir dados ou informações falsas, ou seja, casos que atinjam diretamente o softwares dos computadores, que geralmente invadem computadores através de *Pen drives*, *e-mails*, e em forma de arquivos que são baixados em sites não confiáveis que contém “*vírus*[6]”, a qual danifica diversos arquivos ou programas, chegando até em alguns casos ter de efetuar a formatação do computador em virtude do vírus.

2.2.2 CRIMES CIBERNÉTICOS IMPRÓPRIOS

Nos crimes cibernéticos impróprios são aqueles que são tipificados, no Código Penal, pois violam bens jurídicos comuns, ferem à dignidade da pessoa humana, entre outros crimes que são praticados através do meio informativo.

Com relação ao patrimônio, tem-se uma certa dificuldade em reconhecer os crimes cibernéticos impróprios, pois não se consegue tipificar a informação armazenada como um bem material, mas sim um bem imaterial, insuscetível de apreensão como objeto, por exemplo os crimes de transferência de valores em contas bancárias, no qual os criminosos utilizam-se dos sistemas informáticos apenas como *animus operandi*, ou seja, furtando dinheiro da conta da vítima através de um sistema interligado a internet.

---

[5] **Hacker** – no sentido original da palavra, um hacker é alguém que passa longas horas programando computadores para executar tarefas avançadas. No sentido mais comum, o termo passou a denominar a pessoa que tenta violar ou atacar sistemas. Outros termos comuns são violador, cracker e intruso. (BERNSTEIN et al., 1997)

[6] **Vírus** – trecho de um programa de computador que se reproduz embutindo-se em outros programas. Quando esses programas são executados, o vírus é ativado e pode se espalhar ainda mais. (BERNSTEIN et al., 1997)

Conforme, Rita de Cássia Lopes da Silva explica:

> ... a informação neste caso, por se tratar de patrimônio, refere-se a bem material, apenas grafado por meio de bits, suscetível, portanto, de subtração. Assim, ações como alteração de dados referentes ao patrimônio, como a supressão de quantia de uma conta bancária, pertencem à esfera dos crimes contra o patrimônio. (SILVA, 2003)

Definindo os crimes próprios, bem como crimes impróprios, falar-se-á sobre a competência dos crimes cibernéticos.

2.2.3 COMPETÊNCIA DOS CRIMES CIBERNÉTICOS

Como a Internet não é um local físico é uma rede, cada dispositivo conectado à ela possui um endereço lógico, esse endereço é conhecido como IP, “Internet Protocol[7]”.

Devido a esse fato a pessoa que utiliza a internet, fica na obscuridade do dispositivo, através de um IP; se o dispositivo que foi utilizado para entrar na internet é um celular por exemplo, fica mais fácil de localizar a autoria do fato, pois o proprietário ou quem detém a posse do mesmo fica responsável pelos atos que são feitos na internet, de outro modo se o dispositivo é um computador de uma “Lan House[8]” por exemplo, fica mais difícil de localizar o praticante dos atos, pois o computador tem um IP mas o usuário não necessariamente será o mesmo, pois o local é público, sendo assim qualquer pessoa pode conectar em rede.

A Internet não possuí fronteiras, então qualquer conteúdo pode ser acessado de qualquer lugar do mundo. Qualquer país por exemplo, pode proibir o acesso delimitado de um assunto na rede, mas só para os usuários do território que abranger o país.

Marco Antônio de Barros, exemplificando com um crime contra a honra de uma pessoa, através do uso da Internet, delimita que:

> Se um crime contra a honra de uma pessoa foi perpetrado em um estado da federação ou em outro país, sua transmissão virtual

[7] **IP**, (Internet Protocol) é um protocolo de comunicação usado entre todas as máquinas em rede para encaminhamento dos dados. Tanto no Modelo TCP/IP, quanto no Modelo OSI, o importante protocolo da internet IP está na camada intitulada camada de rede. (CAPRON, 2010)

[8] **Lan House** - é um estabelecimento comercial onde, à semelhança de um cyber café, onde os usuários podem utilizar um computador com acesso à Internet ou a uma rede local, com a principal finalidade, acesso à informação de forma rápida pela rede e/ou entretenimento através dos jogos em rede.

> propagará efeitos para todo o mundo. Pode ser que a vítima se encontre em outra unidade da federação ou país, e ali venha a tomar conhecimento do crime. (BARROS)

Nesse sentido, seguindo a logica de Marco Antônio de Barros, temos um conflito de competência entre o foro do local de onde partiu a ofensa, do domicílio do ofendido e do infrator, e ainda do local onde o ofendido toma ciência da ofensa.

Os artigos 5º e 6º do Código Penal (BRASIL, 1940), versão sobre a territorialidade dos crimes e sobre o local do fato. Conforme segue abaixo:

> Territorialidade
>
> Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.
>
> § 1º - Para os efeitos penais, consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar.
>
> § 2º - É também aplicável a lei brasileira aos crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aquelas em pouso no território nacional ou em vôo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil.
>
> Lugar do crime
>
> Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado. (BRASIL)

O que, para Celso Valin, “a aplicação dos artigos 5º e 6º do Código Penal brasileiro deixa dúvida quanto a solução do problema. Entretanto, não é admissível que o infrator fique impune”.

Já o Código de Processo Penal deduz no artigo 69 a competência jurisdicional, que diz:

> Art. 69. Determinará a competência jurisdicional:
>
> I - o lugar da infração:
> II - o domicílio ou residência do réu;
> III - a natureza da infração;
> IV - a distribuição;
> V - a conexão ou continência;
> VI - a prevenção;
> VII - a prerrogativa de função.

O grande problema de tudo isso, é que nos crimes cibernéticos, os atos executórios da infração ocorrem em lugares diferentes, ficando mais difícil de fixar a competência.

Quando o crime é cometido fora do território nacional a solução seria aplicar o artigo 7º do Código Penal, conforme segue o entendimento de Gabriel C. Zaccarias de Inelas no seu livro Crimes na Internet.

> Quando o infrator comete o delito fora do território nacional e o dano ocorre dentro do território nacional, a solução se encontra no art. 7º do Estatuto Repressivo, "que determina a sujeição a lei brasileira, embora cometido no estrangeiro, de alguns ilícitos penais, dentro de critérios de nacionalidade, representação e justiça penal universal, dentre outros. (INELAS, 2009)

Sendo assim a competência para julgar os crimes cibernéticos, em regra, seria da Justiça Comum Estadual. Porém o Ministério Público Federal no seu Manual Prático de Investigação de São Paulo, prevê que:

> Nos termos do artigo 109, inciso IV, da Constituição Brasileira, compete aos juízes federais processar e julgar os crimes cometidos em detrimento de bens, serviços ou interesses da União, suas entidades autárquicas ou empresas públicas. Assim, é competência da Justiça Federal julgar os crimes eletrônicos praticados contra os entes da Administração Federal indicados nesse inciso. Podemos citar, a título exemplificativo, o estelionato eletrônico, o dano ou a falsificação de dados constantes em sistemas informatizados mantidos por órgão ou entes da administração pública federal. (MINISTÉRIO PÚBLICO FEDERAL, 2006)

Todo crime eletrônico praticado contra ente ou entidade federativa deverá ser julgada pela Justiça Federal. Por exemplo um crime muito comum é o estelionato eletrônico, que geralmente é praticado contra a Receita Federal, em declarações de imposto de renda ideologicamente falsas.

Dentro desse viés ainda temos a hipótese do inciso V do artigo 109 da Constituição Federal, que diz:

> V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente. (BRASIL, 1988)

Que determina que os crimes que tem assunto de tratados ou convenções internacionais, quando ocorrem em lugar estrangeiro tem-se como competência a Justiça Federal.

2.2.4 INVESTIGAÇÃO E AUTORIA DOS CRIMES CIBERNÉTICOS

Na parte de investigação dos crimes cibernéticos, temos como plano normativo, o artigo 1º da Lei de Organização da Investigação Criminal, (Lei nº 49/2008) que vale a ressalva que a sua última versão tem como Lei nº 57/2015; no que tange as seguintes informações:

> A investigação criminal compreende o conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito do processo. (BRASIL, 2015)

A investigação fica a cargo do Ministério Público e/ou pelas Policias Judiciárias dependendo a ocasião do crime.

Nos crimes cibernéticos, a perícia é a melhor das fontes para se identificar a materialidade e a autoria do crime. Geralmente a perícia é realizada na fase policial, devido a necessidade de serem feitas de imediato ou o mais breve possível após o acontecimento do crime.

Em questão do perito especializado em casos de crimes cibernéticos, devem ficar em constante atualizações devido a rapidez com que os aplicativos, e meios para acesso a internet são atualizados. Inclusive nesses termos, não só os peritos devem acompanhar tais atualizações, o Direito em sí deveria acompanhar, bem como os operadores do direito, as entidades de classe, e os meios acadêmicos.

Na parte de autoria do crime cibernéticos, um dos grandes problema a ser enfrentado é a dificuldade de localizar o autor do fato, devido a que os criminosos se esconderem (atrás de um dispositivo, sendo computador, tablet, ou celulares por exemplo), outro fator que aumenta a dificuldade é que o autor do fato geralmente utiliza-se de perfil falso para cometer os crimes, dificilmente o autor vai utilizar dados verdadeiros.

Deste modo já que os usuários dificilmente são identificados através de fotos ou documentos, a autoria fica vinculada através de um IP do dispositivo utilizado para o crime.

Guilherme Schmidt, em projeto publicado no site de artigos, JusBrasil, explicou a grande importância dos provedores de internet colaborarem contra os crimes, deste modo afirmou nesses termos que segue:

> Aí está a importância da cooperação dos provedores de acesso nesse tipo de investigação. Como visto acima, o provedor é o computador que providencia acesso à rede e é responsável por fornecer aos clientes um número de IP para que este se conecte. Portanto, após se conseguir o número de IP utilizado na realização de uma conduta criminosa, é necessário requisitar ao provedor de acesso informações sobre o usuário daquele IP. (SCHMIDT, 2014)

Tão grande a cooperação desses provedores na investigação do crime, quanto a questão da quebra do sigilo dos dados de conexão do usuários, em outras palavras a quebra do sigilo nas conversas, ou meios que podem conter dados para investigação criminal.

> A quebra do sigilo dos dados de conexão de usuário, trata-se somente da disponibilização por parte das empresas, em um primeiro momento, de qual teria sido o IP utilizado e o horário (incluindo informações de fuso horário) de determinada ação criminosa realizada em um serviço de Internet, como redes sociais, contas de e-mail, programas de mensagens instantâneas, dentre outros e em um segundo momento das informações do usuário que efetivamente utilizou aquele IP de determinado provedor, ou seja, qual teria sido, supostamente, o endereço físico no "mundo real" em que o computador ou outro equipamento informático com acesso à Internet estaria instalado no momento da conduta criminosa. (SCHMIDT, 2014)

No Brasil tivemos casos em que a Justiça mandou bloquear o WhatsApp[9], devido ao aplicativo não cumprir determinações judiciais de investigação criminal.

Conforme dados retirados do site do Wikipédia, houve 5 casos desses bloqueios do WhatsApp, conforme segue:

> Em fevereiro de 2015, o juiz Luiz Moura Correia, da Justiça do Piauí, determinou a suspensão temporária do WhatsApp em todo o Brasil. Essa decisão foi tomada depois que o aplicativo se recusou a dar informações sobre um inquérito policial que investigava um crime de pedofilia ocorrido em Teresina, capital piauiense. Contudo, a decisão logo foi derrubada pelos desembargadores Raimundo Nonato da Costa Alencar e José Ribamar Oliveira. (WIKIPÉDIA, 2017)

[9] **WhatsApp** - é um aplicativo de mensagens instantâneas e chamadas de voz ou de vídeos para "smartphones" (telefones que tem acesso à internet). O usuário também tem a opção de mandar mensagens de texto, enviar imagens, vídeos e documentos em formato PDF, além de fazer ligações de voz ou vídeochamadas grátis por meio de uma conexão com a internet.

O segundo caso foi em Dezembro de 2017, o que ocorreu a seguinte informação:

> Em 16 de dezembro de 2015, uma nova ordem judicial determinou o bloqueio do aplicativo por um período de 48 horas. O autor da ação não foi identificado. No entanto, as operadoras estimam que se trate de uma investigação policial. O bloqueio está relacionado a uma possível quebra de sigilo de dados. No Jornal da Cultura do dia 16 de dezembro, o filósofo Luis Felipe Pondé criticou a proibição do WhatsApp ocorrida naquele mês, dizendo que se tratava de uma palhaçada e mais um indicativo de que o Brasil seria um país na idade da pedra, indagando-se então se a juíza Sandra Regina Nostre Marques, quem deferiu o pedido de bloqueio, não teria noção de que o WhatsApp é uma ferramenta econômica. Roberto Delmanto Junior, por sua vez, disse que é algo inacreditável uma juíza de primeira instância afetar todo o Brasil, especulando logo em seguida se seria o caso de alguém que sofreria de "*juizite*". (WIKIPÉDIA, 2017)

O terceiro caso, aconteceu em maio de 2016, que segue:

> Um terceiro bloqueio judicial do aplicativo aconteceu às 14h do dia 2 de maio de 2016 (uma segunda-feira). De acordo com a *Folha de S.Paulo*, a decisão, de 26 de abril, de bloqueio do WhatsApp por 72 horas foi do juiz Marcel Montalvão, da comarca de Lagarto (Sergipe) que definiu o bloqueio depois que o WhatsApp se negou a cumprir determinação de quebra de sigilo de dados trocados entre investigados criminais relacionadas a uma quadrilha interestadual de drogas investigada pela Polícia Federal.
> No dia 3 de maio, o WhatsApp conseguiu obter uma decisão favorável da Justiça de Sergipe e o serviço foi desbloqueado, e por volta das 17h o serviço foi gradativamente estabelecido no país. O desembargador do Tribunal de Justiça de Sergipe, Ricardo Múcio Santana de Abreu Lima, aceitou o pedido de reconsideração dos advogados do WhatsApp. Durante o bloqueio, o aplicativo de mensagens Telegram foi o mais sugerido pelos usuários de redes sociais como alternativa ao WhatsApp, segundo um monitoramento da TNS. (WIKIPÉDIA, 2017)

O quarto e último caso ocorrido no Brasil, aconteceu em julho do ano de 2016, conforme relato abaixo:

> Um novo bloqueio foi solicitado pela juíza Daniela Barbosa Assumpção de Souza, da comarca de Duque de Caxias (RJ) em 19 de julho de 2016. O pedido da juíza é para que o WhatsApp intercepte mensagens de envolvidos em crimes na região. Como após três notificações o Facebook não atendeu aos pedidos, a juíza pediu o bloqueio. A justiça espera que o Facebook faça com que o WhatsApp desvie mensagens antes da criptografia ou então desenvolva tecnologia para quebrar a criptografia. A multa para o Facebook pelo não cumprimento é de 50 mil por dia.
> O bloqueio foi cancelado, no mesmo dia, por liminar concedida por Ricardo Lewandowski, ministro do STF, ao Partido Popular Socialista (PPS). Por volta das 18 horas, muitos utilizadores já relatavam estarem conseguindo utilizar o serviço normalmente.

> Na noite seguinte, pelo *Jornal da Gazeta, Edição das 10*, o comentarista de política José Nêumanne Pinto teceu duras críticas a Lewandowski e a Zuckerberg. "O Ministro desmoralizou a juíza e aceitou que uma empresa americana também desmoralizasse a justiça brasileira, da qual ele é o principal representante". (WIKIPÉDIA, 2017)

De outro modo temos também a interceptação de dados telemáticos, que dizem respeito aos acessos de dados através da autoridade policial, de forma investigativa.

Que segundo o artigo de Schmidt, ele faz uma equiparação com a interceptação telefônica, conforme segue:

> Se equipara, em todas as questões legais, à intercepção telefônica, devendo, portando, ser realizada em sede de Inquérito Policial, sendo, necessária, portanto, a provocação do Poder Judiciário e Ministério Público, por meio de Representação, a fim de obtermos a autorização judicial, nos moldes da legislação vigente, em especial a Lei 9.296/96, a Lei de Interceptações Telefônicas. (SCHMIDT, 2014)

Outro dado relevante que foi encontrado nesse artigo, foi a notícia que o Ministério Público Federal, em 2008, fez um Termo de Ajustamento para que a empresa Google, guardasse os dados dos utilitários dos serviços cibernéticos por prazo de 6 meses, e quando solicitados que fossem entregues de imediatos as requisições da policia brasileira, mediante autorização judicial.

Sendo assim, concluindo o segundo capítulo, falar-se-á sobre a parte legislativa do trabalho.

3. LEGISLAÇÕES COMPETENTE PARA OS CRIMES CIBERNÉTICOS

Nesse capitulo procurarei buscar as legislações bem como regulamentações que podem ser aplicadas nos crimes cibernéticos, e vale muito a pena referir que a Constituição Federal no seu artigo 5º, XXXIX, deduz que: “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”, nesses termos é de total convencimento que se não haver tipificação penal sobre crimes cibernéticos, não será cominado como crime, começando com a Legislação que abrange os Crimes Cibernéticos, Lei 12.737/12.

3.1. LEI CAROLINA DIECKMANN – LEI Nº 12.737/12

Não tem como falar em crimes cibernéticos sem tocar o nome da atriz Carolina Dieckmann, pois em 03 de dezembro de 2012 publicada pelo Diário Oficial de União, sancionada pela Presidente da República, Dilma Rousseff, a Lei 12.737/12, lei está que veio dispor a tipificação criminal para os crimes cibernéticos.

Apelidada de Lei Carolina Dieckmann, ganhando essa nomenclatura pelo fato de que a atriz teve seu computador invadido por hackers, no qual foram subtraídos fotos intimas que foram divulgadas pelas redes sociais através da internet.

Sendo que está lei foi composta de 2 (dois) artigos no qual foram incluídos no Código Penal de 1940, segue abaixo os artigos:

> **Invasão de dispositivo informático**
>
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

No artigo 154 – A, trata-se de quando o criminoso invade um dispositivo, utilizando-se de um meio fraudulento para romper os mecanismos de segurança e praticar os delitos. Trazendo nos parágrafos 1, 2 e 3, que atenua a pena quando a invasão resulta prejuízo econômico, ou que contenha informações sigilosas, ou comunicações eletrônica privada. Outrossim a pena é aumentada há 2 terços se o conteúdo for comercializado ou transmitido a terceiros.

Quando o crime for ocorrido contra Presidente da República, governadores e prefeitos, bem como autoridades públicas, a pena é aumentada de 1 terço à 50% nas atenuantes da dosimetria da pena.

> Ação penal
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.
>
> Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:
>
> Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.

Já no artigo 154 – B, trata-se do funcionalismo da Ação Penal, que somente é procedida perante representação, tendo a exceção quando o crime for contra administração pública direta ou indireta, independente dos poderes do Estado.

> Art. 266.
>
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
>
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR)
> Falsificação de documento particular.

Já o artigo 266 estabelece regulamentação sobre quem pratica o crime impedindo ou dificultando informações de utilidade pública, e de quem usa dos dados para falsificação de documentos.

Outro artigo que foi contemplado no Código Penal, através da Lei Carolina Dieckmann, é o Artigo 298 com uma singela redação, trata da falsificação de cartões, que é um crime bem utilizado contemporaneamente. Que segue:

> Art. 298.
>
> Falsificação de cartão
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (NR)
>
> Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

No que diz respeito a Lei 12.737/12, o Sr. Advogado Eudes Quintino de Oliveira Junior, Mestre em Direito, ex-promotor de justiça do Estado de São Paulo, delimitou em um artigo publicado no site Jusbrasil, a seguinte prerrogativa:

> Extrai-se do texto legal a finalidade de incriminar a conduta do agente que invade, driblando os mecanismos de segurança, e obtém, adultera ou destrói a privacidade digital alheia, bem como a instalação de vulnerabilidades para obtenção de vantagem ilícita. Observa-se, contudo, a necessidade da existência de um mecanismo de segurança no sistema do aparelho, uma vez que a lei condiciona a ocorrência do crime com a violação indevida deste. Assim, a invasão do dispositivo informático que se der sem a violação do mecanismo de segurança pela inexistência deste será conduta atípica. Por tal razão torna-se cada vez mais importante proteger os aparelhos com antivírus, firewall, senhas e outras defesas digitais. (JUNIOR, 2012)

Eudes Quintino trouxe em seus dizeres que além da tipificação criminal sobre o crime cibernético, o usuário ainda sim, tem de se proteger cada vez mais com mecanismos de segurança, como antivírus e senhas.

Acrescentou também a demora da criação da Lei de Crimes Cibernéticos, tendo em vista que as pessoas depositam muitos dados na rede internética, e

necessitava criar barreiras para os crimes que podem vir a ser praticados em virtudes destes.

> A lei ora apresentada veio com certa demora. A sociedade reclamou a tutela penal da intimidade cibernética durante muito tempo. E com razão. Muitas outras intimidades foram protegidas, tais como a inviolabilidade de domicílio, o sigilo epistolar, o sigilo das correspondências e das comunicações, sigilos das comunicações telefônicas, sigilo bancário e outros. E no mundo digitalizado há a mesma necessidade de se erguer muros protetores. (JUNIOR, 2012)

Partindo desse pressuposto, encontrou-se o “Marco Civil da Internet”, que foi a criação da Lei N° 12.965/14.

3.2. MARCO CIVIL DA INTERNET, LEI Nº 12.965/14

O Marco Civil da internet foi criado pelo Poder Executivo no inicio do ano de 2014, mais precisamente em 23 de abril de 2014, onde em uma Conferência Internacional, conhecida como NETMundial[10], realizada em São Paulo, que reuniu 90 países do mundo inteiro.

O grande objetivo da Lei 12.965/2014 é garantir à defesa dos consumidores que usam a internet para adquirir produtos ou serviços, pois regula a comercialização das empresas que utilizam da internet como meio de comércio, assegurando a livre iniciativa, bem como a livre concorrência. Regendo também os serviços que são prestados pelas multinacionais provedoras de Internet, criando um fornecimento com garantia de funcionalidade e segurança para os usuários.

Essa lei para o Brasil estabeleceu princípios, garantias, direitos e deveres para o uso da internet, que segue nos artigos abaixo, conforme redação da lei:

> Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.
>
> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
>
> I - o reconhecimento da escala mundial da rede;

[10] **NETMundial** – é um encontro Multissetorial Global Sobre o Futuro da Governança da Internet, que acontece em São Paulo. E tem como objetivo a elaboração de princípios de governança sobre a Internet e a proposta de um roteiro para a evolução futura desse ecossistema, a qual vem recebendo muitas críticas devido ao controle do poder estar enraizado somente nos Estados Unidos.

> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
>
> III - a pluralidade e a diversidade;
>
> IV - a abertura e a colaboração;
>
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VI - a finalidade social da rede.

O artigo segundo dessa legislação se deu, para disciplinar o uso de internet no Brasil, trazendo como fundamento principal à liberdade de expressão.

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II - proteção da privacidade;
>
> III - proteção dos dados pessoais, na forma da lei;
>
> IV - preservação e garantia da neutralidade de rede;
>
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
>
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
>
> VII - preservação da natureza participativa da rede;
>
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
>
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

O artigo terceiro veio no viés intencional do artigo segundo, trazendo consigo alguns princípios, como proteção da privacidade, proteção de dados pessoais, preservação de rede, com padrões internacionais, e responsabilização dos agentes em conformidade com a lei.

> Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:
>
> I - do direito de acesso à internet a todos;

> II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;
>
> III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
>
> IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

O artigo quarto teve com objetivo a promoção do direito à acesso de internet para todos, prezando também o acesso à informação ampliando, e fomentando as novas tecnologias, fazendo com que as pessoas aderissem a novos estilos de pesquisa.

> Art. 5º Para os efeitos desta Lei, considera-se:
>
> I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;
>
> II - terminal: o computador ou qualquer dispositivo que se conecte à internet;
>
> III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;
>
> IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;
>
> V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
>
> VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
>
> VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
>
> VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

O artigo quinto veio para determinar os efeitos da Lei, estabelecendo fundamentos sobre internet, terminal, endereço de protocolo, conexão e registros de aplicações de internet. Já o artigo sexto delimitou que a legislação além de utilizar-se

de seus fundamentos, princípios e objetivos previstos, pode se fazer uso de costumes e importância dos particulares. Abrangendo o contexto legislativo.

> Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

Deste sim, conforme vimos no decorrer desse estudo, o Marco Civil da Internet surgiu para regular as ações tomadas na internet estipulando os direitos e deveres de quem à utiliza. Tendo em vista que a internet é a maior fonte de informações de hoje em dia, que com o Marco Civil buscou-se regulamentar os tráfegos de dados e minimizar os problemas que ocorrem na rede.

3.3. O CÓDIGO DE DEFESA DO CONSUMIDOR E SUA APLICABILIDADE PARA OS CRIMES VIRTUAIS

Devido à internet ser um dos meios mais fáceis para celebrar contratos, hoje em dia, milhares de contratos por essa via, é plausível que a maioria dos contratos obedece os princípios de publicidade, vinculação, veracidade, e não abusividade, entre outros.

Nesse sentido tendo em vista que o ordenamento jurídico brasileiro não tem legislação específica sobre os delitos nos contratos virtuais, o Código Civil e o Código do Consumidor tentam sanar esses conflitos através do principio da analogia.

3.4 O ESTATUTO DA CRIANÇA E DO ADOLESCENTE SOBRE OS CRIMES CIBERNÉTICOS

O ECA, (Estatuto da Criança e do Adolescente), criado em 1990, como é uma lei considerada antiga, está não previa crimes com menores ligados à internet, deste sim, devido ao grande número de crianças e adolescentes ativos na rede, começaram a acontecer vários delitos, devido a imprudência de pais ou mesmo dos próprios menores usuários, mesmo assim a nova lei deu mais ênfase no crime de pedofilia infantil, transmissões de imagens que afrontam a dignidade da crianças ou adolescente, exposição de menores, e pornografia infantil.

Deste fato, a Lei 8.069/90 encontrava-se defasada, tendo em vista que o direito deve acompanhar a era da informatização, então em 25 de novembro de 2008, entrou em vigor a Lei 11.829, chamada Lei da Pornografia Infantil, que modificou o artigo 241 da Lei 8.069/90, e tipificou o crime de pedofilia pela internet, alterando a letra da legislação.

No artigo 241-A, que segue:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (BRASIL, 2008)

O que mais nos assusta são os dados sobre os crimes sexuais contra crianças e adolescentes, que vem acontecendo no Brasil, conforme dados retirados do site de noticias em 2015:

> No ano de 2014, o governo federal recebeu, por meio do disque 100, mais de 180 mil denúncias de violência contra crianças e adolescentes. Desse total, 26 mil tratavam de abuso sexual, o que representa uma média de 70 denúncias por dia. São Paulo lidera os casos, com 14,5%, seguido da Bahia, com 8,74%, e do Rio de Janeiro, com 8,34%. (R7 notícias, 2015)

A maior preocupação, é que os entes públicos fazem sua parte na medida do possível, porém a população ainda se sente acoada quando se trata desses assuntos, pois se sabe que muitos casos são acometidos dentro de casa , e muitas vezes a genitora da criança não denuncia e tenta defender o abusador, por se tratar de união estável ou afins.

3.5. A CONVENÇÃO DE BUDAPESTE

Se tratando um pouco no âmbito internacional, outros países ao contrário do Brasil tem mais legislação competente sobre crimes cibernéticos, um grande exemplo que podemos retirar é a Convenção de Budapeste.

A convenção de Budapeste, ou nomenclada como A Convenção Sobre Cibercrime, foi criada em 2001, entrando em vigor em 01 de julho de 2004 e é um tratado internacional que abrange o direito penal e o direito processual penal, para

definir de forma mais harmônica os crimes cibernéticos e as formas de persecução, em qual o Brasil não é signatário.

Essa convenção trata basicamente sobre as violações de direito autoral, fraudes relacionadas com o acesso da internet pelo computador, pornografia infantil e violações de segurança de rede.

Segundo seu Preâmbulo, a Convenção prioriza “uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional” reconhecendo “a necessidade de uma cooperação entre os Estados e a indústria privada”.

Infelizmente, como a convenção teve origem por integrantes do Conselho Europeu, o Brasil não foi convidado para participar, por este motivo não somos signatários desse tratado. A título de curiosidade os Estados Unidos da América foi o único país que não pertence a territorialidade da Europa que assinou (ratificou) o tratado em 2006.

Deste sim, falar-se-á do próximo e último capítulo, na qual tratarei a problemática do trabalho de pesquisa.

4. COMO EVITAR ALGUNS TIPOS DE CRIMES CIBERNÉTICOS

Nesse capítulo falar-se-á sobre como evitar ou se prevenir de alguns tipos criminais, que são praticados através da internet.

Nos dias atuais, pode-se dizer que a criminalidade na internet avança a cada dia que passa, pois tem pessoas que praticam crimes, e nem se quer se dão por conta, em questão de informação, um artigo publicado no site da Tecmundo, dispõe que:

> No mundo, dois em cada três usuários já foram vítimas de crimes virtuais, que atingem 556 milhões de pessoas todos os anos. Só no Brasil, o prejuízo anual é o maior de todos, estimado em R$ 16 bilhões. Os dados são de 2012, da empresa de segurança virtual Symantec. De acordo com o relatório de 2014 da Kaspersky Lab, outra companhia de segurança na Internet, o Brasil é o segundo país onde mais acontecem fraudes bancárias. (TECMUNDO, 2016)

Isso mostra que os crimes cibernéticos estão cada vez mais frequentes, sofisticados, e mais difíceis de combater.

Este artigo também delencou quais são os 7 (sete) crimes que são mais praticados em rede; classificando os crimes como roubo de identidade e senha: que são utilizadas para efetuar compras online ou transações financeiras de forma indevida.

A falsa identidade em segundo lugar, é um dos crimes mais comuns em redes sociais, é quando uma pessoa omite, mente sobre suas características para tirar proveito de outrem.

Calúnia ou difamação que é a divulgação de informações falsas sobre alguém, que podem por ventura prejudicar a vítima do crime.

Estelionato é quando um criminoso engana a vítima querendo tirar vantagem sobre ela.

Pirataria, cópias ou reprodução de livros, músicas, imagens e softwares de empresas sem a devida autorização do proprietário.

Discriminação é toda divulgação de informações com caráter preconceituoso sobre a cor de pele, sexo, orientação sexual, religião e nacionalidade das pessoas.

Pedofilia já qualificado no capítulo anterior, sob normatização do Estatuto da Criança e do Adolescente, pedofilia é o abuso sexual infantil, que geralmente são possibilitados através de sites ou rede sociais.

Ficando a difamação como primeira colocada nos casos de crimes virtuais no Brasil, segundo o advogado Jair Jaroleto, especialista e Direito Penal e crimes na internet, que diz: “Isso porque as pessoas esquecem que escrever nas redes sociais é similar a escrever em um outdoor”.(JAROLETO, 2011 apud RIBEIRO, 2012)

Apesar de todos estes desafios, algumas soluções estão sendo tomadas, como por exemplo alguns aplicativos estão investindo em proteção no seu sistema, o Facebook quando você postar algo ofensivo, automaticamente o sistema exclui a publicação. Vale ressaltar também que estão sendo criadas novas legislações para combater com mais vigor os crimes, o treinamento para capacitação mínima do pessoal que trabalha com investigação desses tipos penais também é de suma importância, a cooperação policial de todas as instancias, inclusive a polícia internacional, entre outras soluções que são necessárias para acompanhar o desenvolvimento dos crimes na internet.

A legislação que se tem em vigência, ainda é insuficiente para coibir os crimes, as penas são brandas, e a investigação é pouca, chegando as vezes em ter a comprovação do delito, mas sem a localização do criminoso, então as informações que mais são repassadas para os usuários que utilizam da internet, é a precaução, evitar e prevenir os crimes.

Tendo em vista a forma mais recomendada para se proteger de crimes cibernéticos é o uso de programas antivírus no computador, smartphones, tablets, ou qualquer outro dispositivo que venha a ter acesso a internet. Mesmo assim não é o suficiente para ficar 100% seguro, em função disso buscou-se informações diretamente de um site de provedor de antivírus, chamado Norton Symantec Corporation, que trouxe para nós 12 dicas de como se prevenir contra ataques cibernéticos.

Uma das dicas mais fundamentais da Norton é manter seu computador atualizado com os patches[11] e atualizações mais recentes de antivírus. Conforme texto retirado do site da Norton.

> Uma das melhores formas de manter seu computador livre de agressores é aplicando patches e outras correções de software assim que eles se tornam disponíveis. Ao atualizar seu computador

[11] **Patch** – Um patch é um arquivo que contém apenas as mudanças feitas pela atualização e, justamente por isso, é sempre muito pequeno se comparado ao arquivo original. Ele é obtido comparando a versão anterior com a nova (com a ajuda de algum programa naturalmente). Ao ser aplicado, o patch modifica o programa,"transformando-o" na versão corrigida. (MONIROTO, 2016)

> regularmente, você impede que os agressores tirem proveito das falhas do software (vulnerabilidades) que, do contrário, seriam usadas para entrar no seu sistema. (NORTON, 2016).

Mesmo com a atualização do seu computador, você não fica protegido contra todos os ataques cibernéticos, apenas torna o acesso ao seu sistema um pouco mais difícil para os hackers, uma vez que com a versão atualizada o provedor do antivírus vai bloqueando ataques automatizados em rede, fazendo com que o criminoso procure um computador mais vulnerável para ter acesso.

Versões de dispositivos mais recentes, podem ser configuradas para fazer download[12] automaticamente dos softwares, assim você não precisa se lembrar de verificar a disponibilidade do software mais recente.

Outra dica importante que o sistema Norton traz é a configuração de aplicativos da internet, que segue:

> A configuração de aplicativos da Internet, como o navegador da Web e o programa de e-mail, é uma das áreas que merece mais atenção. Por exemplo, algumas configurações no seu navegador da Web (como o Internet Explorer ou Firefox) determinarão o que acontece quando você acessa sites na Internet. As configurações de segurança mais rigorosas proporcionarão maior controle sobre o que acontece on-line, mas podem também causar frustração em algumas pessoas, com um volume exagerado de perguntas do tipo "Isso pode não ser muito seguro, deseja realmente seguir em frente?" ou a incapacidade de fazer o que desejam.
>
> A seleção do nível apropriado de segurança e privacidade depende de cada usuário do computador. Muitas vezes, as configurações de privacidade e segurança podem ser definidas adequadamente sem nenhum conhecimento especial. Basta usar o recurso "Ajuda" do seu software ou ler as informações contidas no site do fornecedor. Caso não se sinta à vontade para definir essas configurações sozinho, consulte alguém conhecido em quem você confie para obter assistência ou entre em contato diretamente com o fornecedor. (NORTON, 2017).

Essa parte de configurar a segurança da página é muito importante devido a sites com arquivos corrompidos, ou até mesmo com vírus, geralmente os computadores vem configurados com segurança mínima, devido à sites como por exemplo site bancários tem pop-ups[13], pois abrem uma página especifica para

---

[12] **Download** – significa transferir **"**baixar". Em um ambiente de rede, receber arquivos de dados de outro computador, provavelmente de um computador maior ou de um computador host. (CAPRON, 2010)

[13] **Pop-ups** – é uma janela que abre no navegador ao visitar uma página de internet, na qual, geralmente é expressa alguma propaganda ou informações a respeito do conteúdo que está sendo procurado.

transações diretas no site do banco, com a utilização de senhas. E se tratando de senhas, a escolha de senhas é a próxima dica que o site traz.

A próxima dica é a escolha de senhas complexas, pois hoje em dia as senhas são muito usadas na internet, usamos senhas em quase tudo, pois usar senha para entrar no e-mail, fazer transações bancárias, acessar sites compra e venda, rede sociais, etc. Segue as dicas conforme diz o site:

> A seleção de uma senha que não possa ser facilmente descoberta é o primeiro passo para a manutenção de senhas seguras e longe de mãos erradas. Senhas complexas têm pelo menos oito caracteres e incluem uma ,combinação de letras, números e símbolos (por exemplo, "#", "$", "%", "!" e "?"). Evite usar estas informações como senhas: seu nome de login, qualquer informação baseada em informações pessoais (como seu sobrenome) e palavras que possam ser encontradas no dicionário. Tente selecionar senhas complexas e únicas para proteger atividades como transações bancárias on-line.
> Guarde suas senhas em um local seguro e tente não usar a mesma senha para todos os serviços que você utiliza on-line.
> Altere suas senhas regularmente, no mínimo a cada 90 dias. Isso pode limitar o dano causado por alguém que já tenha obtido acesso à sua conta. Se você notar algo suspeito com uma de suas contas on-line, uma das primeiras coisas a fazer será alterar a sua senha. (NORTON, 2017)

A manutenção de senhas é fundamental, coisa que nós não fizemos com frequência, outra medida é proteger os dispositivos com antivírus, ou melhor softwares de segurança, a qual é a próxima dica:

Uma das medidas de proteção que o site da Norton nos dá é a instalação de softwares de segurança em seu dispositivo, e deduz que são necessários vários tipos de softwares de segurança para obter uma segurança on-line básica.

> Um software de segurança deve apresentar recursos essenciais como programas antivírus e firewall. Um firewall é normalmente a primeira linha de defesa do seu computador. Ele controla quem e o que se comunica com o seu computador on-line. Você pode considerar o seu firewall como um "policial" que vigia todos os dados que tentam entrar e sair do seu computador pela Internet, permitindo comunicações que têm a garantia de serem seguras e impedindo que o tráfego "ruim", como ataques, entrem em seu computador.
> A segunda linha de defesa é o seu software antivírus. Ele monitora todas as atividades on-line, como mensagens de e-mail e navegação na Web, além de protegê-lo contra vírus, Cavalos de Tróia e outros tipos de programas maliciosos. As versões mais recentes de programas antivírus, como o Norton AntiVirus 2006, protegem também contra spyware e programas potencialmente indesejados, como adware. Um software de segurança que lhe permite controlar software indesejado e o protege contra ameaças on-line é essencial para manter a sua segurança na Internet. Seu software antivírus e anti-spyware devem ser configurados para serem atualizados automaticamente, e devem fazê-lo toda vez que você se conecta à

> Internet.
>
> Pacotes de segurança, como o Norton Internet Security, que combinam firewall, antivírus e anti-spyware com outros recursos (como anti-spam e controles para pais), tornaram-se muito populares, pois oferecem tudo o que um software de segurança precisa para a proteção on-line em um único pacote. Muitas pessoas consideram o uso de um pacote de segurança uma alternativa atraente para a instalação e configuração de vários tipos de software de segurança, além de ajudar a mantê-los todos atualizados. (NORTON, 2017)

Antes de se partir para a próxima dica, a Norton Internet Security, é um dispositivo pago, o que vale que os utilitários de rede, geralmente não pagam o pacote completo, e utilizam-se de tutoriais gratuitos para com softwares de segurança. Desta forma o computador fica protegido na faixa de 1 ano, expirada a validade desse período gratuito, as pessoas não renovam os pacotes.

Deste modo a próxima dica, indica o usuário a proteger suas informações pessoais, o que consiste em evitar de compartilhar dados pessoais, como seu nome completo, endereço residencial, telefones, e documentações, para com vantagens de serviços online. No site da Norton Security encontramos algumas recomendações nesse sentido, compartilhar informações de forma segura, conforme segue:

> Fique atento a mensagens de e-mail falsas. Indicadores de uma mensagem fraudulenta são erros de ortografia e gramática, frases que não soam bem, endereços de sites com extensões estranhas ou que são formados somente por números (pois normalmente teriam palavras) e qualquer outro detalhe que pareça pouco comum. Além disso, as mensagens de phishing quase sempre solicitam que você aja rapidamente para manter sua conta aberta ou atualizar sua segurança, ou solicitam com urgência que você forneça informações imediatamente, caso contrário uma tragédia acontecerá. Não morda a isca.
>
> Não responda a mensagens de e-mail que solicitam informações pessoais. Empresas genuínas não usarão mensagens de e-mail para solicitar suas informações pessoais. Quando em dúvida, entre em contato com a empresa por telefone ou digite o endereço do site da empresa no seu navegador. Não clique nos links dessas mensagens, pois eles podem direcioná-lo a sites fraudulentos e maliciosos.
>
> Mantenha-se longe de sites fraudulentos usados para roubar informações pessoais. Ao visitar um site, digite o URL diretamente no seu navegador, em vez de seguir um link contido em um e-mail ou mensagem instantânea. Impostores quase sempre falsificam esses links para torná-los convincentes. Um site de compras, banco ou qualquer outro site em que informações confidenciais precisam ser trocadas devem apresentar a letra "S" após as letras "http" (como em https://www.seubanco.com e não http://www.seubanco.com). O "s" representa "segurança" e deve aparecer quando você estiver em uma área que solicite o seu login ou o fornecimento de outros dados confidenciais. Outro sinal de uma conexão segura é o pequeno ícone do cadeado na parte inferior do seu navegador (normalmente no canto inferior direito).

> Preste atenção às políticas de privacidade nos sites e softwares. É importante que você entenda como uma empresa coletará e usará suas informações pessoais antes de compartilhá-las com ela.
> Proteja seu endereço de e-mail. Os propagadores de spams e phishing muitas vezes enviam milhões de mensagens para endereços de e-mail que podem ou não existir, na esperança de encontrar uma vítima potencial. Responder a essas mensagens ou até mesmo fazer o download de imagens garante que você seja adicionado às listas deles para que as mesmas mensagens sejam enviadas no futuro. Tenha cuidado também ao divulgar seu endereço de e-mail em grupos de notícias, blogs ou comunidades on-line. (NORTON SECURITY, 2017)

A última dica e não menos importante se refere aos extratos bancários e extratos de cartão de crédito regularmente, pois os hacker estão por toda a parte, inclusive quando se fala de agências bancárias, conforme relato em aula do Professor Mestre Luciano Alves dos Santos, afirmou que “esses criminosos hackeiam várias contas do banco e retiram R$ 0,01 centavo de cada conta, no final da um montante monstruoso, que os clientes nem vão atrás devido a quantia”, fazendo que os bancos deixem passar despercebidos, mas os impactos são enormes de furtos através dos crimes cibernéticos à agencias de bancos.

E segundo a dica do site Norton Security, reduz drasticamente se for efetuada nos conformes:

> O impacto de um roubo de identidade e crimes on-line pode ser reduzido significativamente se eles forem detectados logo após o roubo dos dados ou quando ocorrer a primeira tentativa de uso das informações. Uma das maneiras mais fáceis de descobrir se alguma coisa está errada é procurando transações incomuns nos extratos mensais fornecidos pelo seu banco ou operadora de cartão de crédito.
>
> Além disso, vários bancos e serviços utilizam sistemas de prevenção contra fraudes que chamam a atenção para compras fora do comum (por exemplo, se você mora no Texas e de repente começa a comprar refrigeradores em Budapeste). Para confirmar essas compras fora do comum, eles poderão entrar em contato com você para que você possa confirmá-las pessoalmente. Não ignore essas chamadas. Elas indicam que alguma coisa errada pode estar acontecendo e você deve considerar alguma das atividades mencionadas na seção sobre como reagir, caso se torne uma vítima. (NORTON SECURITY, 2017)

Concluindo esse título, de como evitar alguns tipos de crimes cibernéticos, vamos fazer um breve adendo sobre quais os procedimentos a se tomar quando sofrer um crime cibernético.

4.1 QUAIS PROCEDIMENTOS TOMAR SE SOFREU CRIME CIBERNÉTICO?

Devido a falta de orientações, falta de conhecimento ou por medo, diversas pessoas que sofrem com crimes, não só cibernéticos, não denunciam os casos. Então buscar compreender o que é um crime cibernético seria de suma importância, para evitar ou tentar combater essa prática de delito.

Apesar de ser um assunto comum no dia-a-dia, parece que as pessoas não se dão por conta que os crimes estão acontecendo, e ninguém toma providência, é quem nem aquela máxima que diz: “isso nunca vai acontecer comigo”, mas sim, acaba acontecendo, e qualquer pessoa que utiliza está a mercê de sofrer um crime cibernético.

Então independente de tudo, o importante é denunciar, pois dessa forma podemos contribuir para que os crimes cibernéticos diminuem.

Buscando de um passo-a-passo, de como proceder se caso sofreu um crime cibernético, encontrou-se em artigos os seguintes argumentos, sob embassamento no artigo Como denunciar um crime cibernético, passo à passo, publicado no site Direitos Brasil, que segue:

> **Passo 1: Coleta de informações**
>
> O primeiro passo para denunciar um crime virtual consiste em reunir as informações e dados do crime. A vítima deve salvar tudo que pode auxiliar a provar o crime cometido, desde e-mails, fotos de telas (print screen), dados do criminoso, conversas em redes sociais, entre outros. Ou seja, nessa etapa é essencial armazenar todos os materiais e arquivos que comprovem o crime.
>
> **Passo 2: Registro**
>
> Após coletar todas as informações relacionadas ao crime, a vítima deve dirigir-se a um cartório e registrar esses arquivos em uma ata notarial. Essa ata é um instrumento público que registra os documentos e declara a veracidade deles, ou seja, confirma que os documentos são verdadeiros.
>
> **Passo 3: Boletim de Ocorrência**
>
> A última etapa também está relacionada a um registro, que deve ser realizado em delegacias de polícia. A vítima do crime deve dirigir-se a uma delegacia de polícia e registrar um boletim de ocorrência sobre o ocorrido. Algumas cidades no país possuem Delegacias Especializadas em Crimes Cibernéticos, mas esse registro pode ser feito em qualquer delegacia por todo o país.
>
> O boletim de ocorrência é um documento fundamental no processo de denunciar um crime virtual, pois permite que seja instaurado um

> inquérito policial para realizar a apuração do crime, ou seja, a investigação. (DIREITOS BRASIL, 2017).

Portanto seguindo esse rito de procedimentos, se a pessoa vier à sofrer com crimes cibernéticos, a primeira hipótese a fazer é coletar as provas, para tentar saber a veracidade e a autoria do fato, deste sim, o segundo passo é a vitima procurar um Cartório de Registros para efetuar uma Carta Notarial, a qual deverá ser autenticada por um agente público, dando assim fé publica no documento, e o terceiro e último passo é procurar uma Delegacia de Polícia para efetuar o Boletim de Ocorrência (B.O), pedindo a representação ao Ministério Público, para dar prosseguimento a Ação Penal Pública.

Bem como também é fundamental procurar um advogado, se possível especialista em crimes cibernéticos, para que tome as medidas cabíveis para buscar a reparação do delito.

5. CONCLUSÃO

No decorrer dos dias, o número de pessoas conectadas na internet aumenta, com isso a Internet que pode ser utilizada para fazer coisas boas, pode também ser utilizadas por pessoas de má-fé que se aproveitam desse meio para praticar delitos na rede, a partir de o momento que o crime é praticado através de um dispositivo por meio da internet, pode se dizer que está sendo praticado um cibercrime ou um crime cibernético como doutrinadores delencam em seus livros e artigos.

Por conseguinte desses fatos tem de haver uma resposta do Estado, para tentar coibir essa nova modalidade de crime, e para que o Estado exerça tal função o meio que utilizam é a formulação da tipificação penal, ao que pese que nos tempos de hoje, no meu ponto de vista e indo em conjunto com a doutrina majoritária, não é suficiente as leis que vigoram no Brasil, pois necessita-se de leis mais brandas, e mais exigentes, no caráter de coibir os praticadores desses delitos, enfim, iniciando de um pressuposto de educação, tanto de quem utiliza o meio, como de quem cria meios de proteção contra crimes cibernéticos.

Nesse sentido a criação da Lei 12.735/12, Lei Caroline Dickmann é sem dúvidas uma das medidas importantes a ser revistas, basta ser um pouco mais rigorosa e ampliada, pois veio ao encontro de uma tipificação penal muito lesada, que é o Código Penal, que foi criado em 1940. Não desmerecendo a Lei, pode-se dizer que já é um grande avanço para o Direito Penal.

Outro meio que está de certa forma minimizando os crimes, foi a criação do Marco Civil da Internet, Lei 12.965/14, que regulou as translações internacionais através de acordos, sem dúvida um grande aliado no combate as ações delitivas digitais. Pois essa norma vem para ajudar no procedimento de investigações criminais virtuais, sendo o Estado um pouco mais ativo em virtude dos princípios, direitos, deveres e garantias de quem utiliza a Internet.

Na questão internacional conforme foi tratado no projeto de pesquisa, o Brasil sempre está em desvantagem com os demais países, pois como o Brasil é definido como “país de terceiro mundo”, então, nos países delencados como primeiro mundo existe pactos, como a Convenção de Budapeste, a qual trata dos crimes cibernéticos de forma mais branda.

Essa convenção não teve a participação Brasileira, pois foi criada por países da Europa, e o único país da América que foi convidado a participar dessa convenção foi os Estados Unidos da América.

Conclui-se pela possibilidade de coerção dos crimes cibernéticos, como um dos fatores importantes a cooperação internacional dos países, pois os crimes como são conectados em rede, podem ser rapidamente espalhados no mundo inteiro em minutos, outra medida seria a capacitação de todos os órgãos competentes, como os poderes governamentais, incluindo também a força policial, que tem um papel fundamental na obtenção dos delitos e na capturação dos criminosos.

Outra medida fundamental para não cair em crimes cibernéticos, é a prevenção, na dúvida não abrir arquivos que se acham suspeitos, e quando estiver certeza de que um site, ou arquivo estiver com vírus, denunciar para que outras pessoas não sejam lesadas, se o crime for de cunho pessoal cito injuria, calúnia, exposição de imagens constrangedoras, ou até mesmo crimes sexuais, a única saída é buscar o judiciário para resolver as questões de forma justa.

Por fim, espera-se que esse estudo agregue valor em pesquisas sobre esse tema, e ainda, que o mundo do direito consiga de certa forma prevalecer sempre com a JUSTIÇA nesses crimes, sendo que o direito visa um Estado perfeito, mas não sei se vamos alcançar tal preceito com as políticas de hoje.

REFERÊNCIAS

ALBUQUERQUE, Sylvia. **Governo federal recebe cerca de 70 denuncias de abuso contra crianças por dia**, 2015. Disponível em: <https://noticias.r7.com/cidades/governo-federal-recebe-cerca-de-70-denuncias-de-abuso-contra-criancas-por-dia-18052015>. Acessado em 20/11/2017.

BERSTEIN, Terry. et al., **Segurança na Internet**, Rio de Janeiro: Campus, 1997.

BRASIL, **Código Penal**. Brasília, 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm> Acessado em: 20/10/2017.

BRASIL, **Constituição Federal**. Brasília, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm> Acessado em: 24/10/2017.

BRASIL, **Estatuto da Criança e do Adolescente**. Brasília, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8069.htm>. Acessado em: 20/11/2017.

BRASIL, **Lei Caroline Dieckmann**. Brasília, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acessado em: 24/10/2017.

BRASIL, **Lei de Organização da Investigação Criminal**. Brasília, ed. 4ª – 2015. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1021&tabela=leis&so_miolo=. Acessado em 09/11/2017.

BRASIL, **Lei de Pornografia Infantil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>. Acessado em 20/11/2017.

CAPRON, H. L, **Introdução à Informática**. 8ª ed. São Paulo : Pearson Prentice Hall, 2010.

CHAVES, Antônio apud SILVA, Rita de Cássia Lopes. **Direito Penal e Sistema Informático**. Disponível em: http://schmidtadvogados.com/v/artigo5. Acessado em: 02/06/2017.

DIREITOS, Brasil. **Como denunciar um crime virtual passo a passo**. 2017. Disponível em: <http://direitosbrasil.com/denunciar-um-crime-virtual-passo-passo/> Acessado em: 30/11/2017.

DIZARD, Wilson Jr., **A nova mídia: a comunicação de massa na era da informação**. Rio de Janeiro: Jorge Zahar Ed., 2000.

MINISTÉRIO PÚBLICO FEDERAL. **Crimes Cibernéticos. Manual Prático de Investigação**. 2006. ACESSADO EM 06/11/2017

MONTEIRO, Luís. **A INTERNET COMO MEIO DE COMUNICAÇÃO: POSSIBILIDADES E LIMITAÇÕES**. Campo Grande/MS: INTERCOM, XXIV Congresso Brasileiro da Comunicação, set. – 2001. Disponível em : <http://www.jack.eti.br/www/arquivos/documentos/trabalhos/fae/Trabalho_Redes_Adinarte_26032008.pdf.> Acessado em 19/10/2017.

MONORITO, Carlos E. **Dicionário de Termos Técnicos Informática**. 3ª ed. São Paulo/SP. 2016. Disponível em: <http://fasam.edu.br/wp-content/uploads/2016/06/Dicion%C3%A1rio-T%C3%A9cnico-de-Inform%C3%A1tica.pdf.> Acessado em 18/04/2018.

NORTON, Symatec. **Dicas para prevenção**. 2016. Disponível em: <https://br.norton.com/cybercrime-prevention> Acessado em 25/11/2017.

PAESANI, Liliana Minardi, coordenadora. **O Direito na Sociedade da Informação**, Atlas, 2006. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acessado em 30/10/2017.

PECK PINHEIRO, Patrícia. **Direito Digital**, 2. Ed. rev., atual. E ampl. – São Paulo : Saraiva, 2007.

RIBEIRO, Diego. **Previna-se contra os crimes virtuais**. 2012, Disponível em: <http://www.gazetadopovo.com.br/vida-e-cidadania/previna-se-contra-os-crimes-virtuais-2p8t5psurl5g5vfgx3fd7j0b2> acessado em 26/11/2017.

ROSA, Fabrizio. **Crimes de Informática**. Campinas: Bookseller, 2002. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acessado em: 31/05/2017.

ROQUE, Sérgio Marcos. **Criminalidade informática**: crimes e criminosos do computador. São Paulo: ADPESP Cultural, 2007. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acessado em: 31/05/2017.

SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**, 2003. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acessado em: 24/10/2017.

SILVA, Liliana. **Tecnologias de informação e comunicação**, 2010. Disponível em: <https://pt.slideshare.net/lilianesilva14/a-internet>. Acessado em 07/05/2018.

TECMUNDO. **Crime Virtual: o que é e como se proteger das ameaças**. 2016. Disponível em: <https://www.tecmundo.com.br/crime-virtual/97401-crime-virtual-proteger-ameacas.htm>. Acessado em: 26/11/2017.

VALIN, Celso. **O Direito na Sociedade da Informação**, Atlas, 2006. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acessado em 30/10/2017.

VIANA, Marco Túlio apud CARNEIRO, Adeneele Garcia. **Fundamentos de direito penal informático. Do acesso não autorizado a sistemas computacionais**. Rio de Janeiro: Forense, 2003. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acessado em: 24/10/2017.