UNIVERSIDADE FEDERAL DA PARAÍBA - UFPB

CENTRO DE CIÊNCIAS JURÍDICAS - CCJ

CURSO DE DIREITO

LUÍZA ALICE TORRES ÂNGELO

CRIMES CIBERNÉTICOS: AS LIMITAÇÕES DA RESPOSTA ESTATAL A CRIMINALIDADE INFORMÁTICA

SANTA RITA

2017

LUÍZA ALICE TORRES ÂNGELO

CRIMES CIBERNÉTICOS: AS LIMITAÇÕES DA RESPOSTA ESTATAL A CRIMINALIDADE INFORMÁTICA

Trabalho de conclusão de curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas da Universidade Federal da Paraíba, como exigência parcial da obtenção do título de Bacharel em Ciências Jurídicas.

Orientador: Prof. Me. José Neto Barreto Júnior

SANTA RITA

2017

Ângelo, Luíza Alice Torres.

A581c Crimes cibernéticos: as limitações da resposta estatal a criminalidade informática / Luíza Alice Torres Ângelo – Santa Rita, 2017.

70f.

Monografia (Graduação) – Universidade Federal da Paraíba. Departamento de Ciências Jurídicas, Santa Rita, 2017.

Orientador: Profº. Me. José Neto Barreto Júnior.

1. Crimes Cibernéticos. 2. Ordenamento Jurídico. 3. Tipificação Específica. 4. Regulamentação Legal. 5. Limites Penais. I. Barreto Júnior, José Neto. II. Título.

BSDCJ/UFPB *CDU – 346:004.738.5*

LUÍZA ALICE TORRES ÂNGELO

CRIMES CIBERNÉTICOS: AS LIMITAÇÕES DA RESPOSTA ESTATAL A CRIMINALIDADE INFORMÁTICA

Trabalho de conclusão de curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas da Universidade Federal da Paraíba, como exigência parcial da obtenção do título de Bacharel em Ciências Jurídicas.

Orientador: Prof. Me. José Neto Barreto Júnior

Banca Examinadora: Data da Aprovação_____

_____

Prof. Me. José Neto Barreto Júnior (Orientador)

_____

Prof. Dr. Giscard Farias Agra

_____

Prof. Me. Waldemar de Albuquerque Aranha Neto

AGRADECIMENTOS

Agradeço a Deus, o Dono do meu coração, por ter me dado o dom da vida, pelo Seu carinho constate e pelas inúmeras bênçãos que têm conferido a mim. O Seu amor me envolve incessantemente no meu dia-a-dia apesar dos meus defeitos. Agradeço a meus pais por estarem sempre ao meu lado e compartilharem comigo de mais um sonho, essa vitória é nossa. Aos meus irmãos pelo convívio, compreensão, amizade e apoio. Agradeço aos meus avós que não mediram esforços para que eu chegasse até esta etapa da minha vida. Agradeço as minhas tias, tios e primos pelo apoio e amor incondicional. Aos meus amigos por permanecerem ao meu lado, acreditarem em mim e me incentivarem. E por fim, agradeço a Comunidade Nossa Senhora Menina que é presença indispensável em minha vida, por me fazer feliz. E a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

RESUMO

O presente estudo visa pontuar o surgimento histórico da internet, a sua relação com a sociedade atual e o seu desenvolvimento, bem como o desencadeamento dos crimes cibernéticos e a pertinência legislativa do Brasil para combater essas ameaças. Estudar a Darkweb, o lado mais profundo da internet, ambiente criminoso de criptografia diferenciada que melhor resguarda o anonimato de seus usuários, pontuando o seu modo de acesso. Analisar os limites que o ordenamento jurídico enfrenta ao tratar dos crimes cibernéticos e quais são as possíveis medidas a serem tomadas para melhor coibir esses atos ilícitos. Compreender que o aumento do respaldo dos crimes cibernéticos no mundo real se torna cada vez mais evidente e a legislação atual não é suficientemente efetiva para inibir a atuação dos criminosos virtuais. Não é admissível a aplicação ou tipificação de um crime por analogia, pois feriria o princípio da taxatividade. Portanto, se torna difícil a atuação do Estado perante esse impasse, visto que não existe uma lei específica regulamentadora dos crimes cibernéticos. Desse modo, é necessária a adoção de medidas preventivas e repressivas por parte do Estado, juntamente com a criação de uma lei que regulamente a cibernética e dê as punições cabíveis aos atos ilícitos virtuais para melhor proteger a sociedade dessas ameaças digitais.

PALAVRAS CHAVES: Crimes Cibernéticos. Ordenamento Jurídico. Tipificação específica. Regulamentação Legal. Limites Penais.

ABSTRACT

The present study aims to punctuate the historical beginning of the internet, it's relations with today's society and it's development, as well as the triggering of cybercrimes and Brazil's legislative pertinence to fight these threats. To study the dark web, the deepest side of the internet, a criminal environment of differentiated cryptography that best keeps it's user's anonymity, outlining it's access mode. To analyze the limits that stand against the legal order, as it treats these cybercrimes, and which are the possible measures to be taken to best restrain these illicit acts. To comprehend that the increase of cybercrimes backing into the real world becomes everytime more evident and today's legislation is not effective enough to inhibit the acts of virtual criminals. The application or typification of crime by analogy is not admissible, because it interferes with the principle of specificity. Therefore, the State's actions before this impass becomes difficult, because of the absence of a specific cybercrimes regulatory law. This way, it is necessary to adopt preemptive and repressive measures by the State, together with the creation of a regulatory law for cybernetics, and also fixates punishment for virtual illicit acts, to better protect society from these digital threats.

KEYWORDS: cybercrimes. Legal order. Specific typification. Legal regulations. Penal limits.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1. INTRODUÇÃO

O presente estudo é desenvolvido através da pesquisa, leitura, interpretação e análise sistemática de materiais colhidos da internet, livros, artigos, documentos, imagens, mapas, leis, jurisprudências e sentenças para fundamentação teórica. O material recolhido para estudo foi sistematizado para formar um plano de leitura constituindo uma vertente específica na pesquisa jurídica para investigar a efetividade e eficácia da legislação brasileira quanto aos crimes virtuais.

No primeiro capítulo a pesquisa analisa a Agência de Projetos de Pesquisa Avançados (Advanced Research Projects Agency Network) originalmente criada pelo departamento de defesa dos Estados Unidos para facilitar a comunicação e envio de informações secretas a locais distantes. O crescimento do número de hosts, no qual o Departamento de Defesa optou por desenvolver um novo sistema que suportasse os novos parâmetros descentralizados dos nomes de domínio. E ressalta o desenvolvimento de uma base de dados, difundida na Rede Mundial de Computadores, ensejando na formação da internet atualmente utilizada pela população mundial.

Em um segundo momento, visa avaliar a legislação atualmente em vigor e sua forma de receber as necessidades da sociedade quanto à proteção virtual, analisa o sistema de resposta estatal quanto à regulamentação do novo foco de criminalidade que emergiu com o avanço da tecnologia aplicada a internet e todos os meios eletrônicos que se propaga, já que em virtude da grande evolução tecnológica a internet passou a ser usada pela sociedade no cotidiano, como uma necessidade, pois web serve de auxílio para as atividades diárias, sendo útil a vida das pessoas, já que disponibiliza um amplo leque de serviços, produtos e redes sociais para se socializar. A pesquisa pondera o surgimento dos crimes virtuais, que em virtude de a internet ter um fluxo elevado de trânsito de informações serviu de incentivo para alguns criminosos a se aproveitaram dessa gama de serviços que a web oferece para realizar condutas danosas ou reprováveis pela sociedade, virando meio de propagação e execução de crimes. Com isso, novos crimes vão surgindo, como também novos bens jurídicos para serem tutelados pelo Estado. Desta forma o presente trabalho ressalta o fato de o ordenamento jurídico não possuir leis específicas ou políticas sociais que regulamentem a internet. Desse modo, é demonstrado que o Estado possui várias limitações no que tange os crimes cibernéticos.

Por fim, o trabalho defende que é extremamente necessário que o ordenamento jurídico se pronuncie com relação às medidas a serem tomadas para coibir essa onda de incidentes criminosos na web. Ressalta que é preciso a criação de tipos penais para tais condutas delituosas já que não é permitido ao Direito Penal usar de analogia em virtude do princípio da taxatividade, como também que sejam adotadas por parte do Ministério Público medidas preventivas socioeducativas para a população. O trabalho objetiva investigar como se dá a proteção do Estado aos bens jurídicos violados virtualmente. A pesquisa visa contribuir com a expansão do conhecimento criminológico no que tange os crimes digitais para toda a sociedade. Também serve como um alerta para a população se precaver com as ameaças promovidas na web. Enfim, examina a internet, os crimes virtuais nela incidentes, pontua os limites que o direito penal enfrenta para regulamentação e proteção da sociedade e propõe maneiras de transpor essas barreiras jurídicas.

2. O SURGIMENTO DA ERA DIGITAL

As mudanças econômicas e também sociais que nasceram com o surgimento e a utilização dos computadores de uso privado são crescentes: o uso de celulares, por exemplo, atualmente possuem os mesmos comandos de um computador comum. Ambos, computadores e telefones móveis, são exemplos da popularização da Internet. A Sociedade teve a possibilidade de entrar na era digital por meio desses artifícios, através dos quais a tecnologia se desdobra em função da informação e os dois caminham juntos promovendo novas formas de trabalho, inovando conceitos, alterando condutas de comportamentos.

Nesse Sentido, um forte indicativo da imersão da sociedade na era digital é facilmente notado pela popularidade e acessibilidade dos aparelhos que acrescentam informática e mobilidade ao dia-a-dia, permitindo a concretização de atividades usuais com mais rapidez e conforto. Exemplo disso são os caixas eletrônicos, que permitem o autoatendimento por meio do reconhecimento da digital dos dedos ou até mesmo transferências bancárias que podem ser realizadas por meio de aplicativos baixados nos smartphones[1], tablets[2] e notebooks[3] (HATAKA, Sidney Akira, 2013, pág 2).

Pode-se considerar que é necessário o estabelecimento de controle, um limite para o uso da informática, já que todas as engrenagens envolvidas no processo cibernético operam de modo sistemático, por isso podem causar interferência no modo de agir da sociedade e fugir

[1] Conforme o Dicionário de significados "Smartphone é um telefone celular, e significa telefone inteligente, em português, e é um termo de origem inglesa. O smartphone é um celular com tecnologias avançadas, o que inclui programas executados um sistema operacional, equivalente aos computadores. Os smartphones possibilitam que qualquer pessoa possa desenvolver programas para eles, os chamados aplicativos, e existem dos mais variados tipos e para os mais variados objetivos. Um smartphone possui características de computadores, como *hardware* e *software*, pois são capazes de conectar redes de dados para acesso à internet, sincronizar dados como um computador, além da agenda de contatos." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: < https://www.significados.com.br/smartphone/> Acesso em: 5 de janeiro de 2017.

[2] Segundo o Dicionário de significados "*Tablet* é um tipo de computador portátil, de tamanho pequeno, fina espessura e com tela sensível ao toque (*touchscreen*). É um dispositivo prático com uso semelhante a um computador portátil convencional, no entanto, é mais destinado para fins de entretenimento que para uso profissional. Devido ao formato e à praticidade do uso da tela com os dedos, é muito usado para navegar na internet, para a leitura de livros, jornais e revistas, para visualização de fotos e vídeos, reprodução de músicas, jogos, etc." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: <https://www.significados.com.br/tablet/ > Acesso em: 5 de janeiro de 2017.

[3] Em conformidade com o Dicionário informal "Computador portátil, leve, projetado para ser transportado e utilizado em diferentes lugares com facilidade. Geralmente, contém tela de LCD (cristal líquido), teclado, mouse (geralmente um touchpad, área onde se desliza o dedo), unidade de disco rígido, portas para conectividade via rede local ou fax/modem, gravadores de CD/DVD." Dicionário Informal. 2017. Disponível em: < http://www.dicionarioinformal.com.br/notebook/> . Acesso em: 5 de janeiro de 2017.

do controle do Direito Penal, desencadeando uma onda de atos ilícitos, por isso devem impreterivelmente serem assessoradas e protegidas.

2.1 Identificação Numérica De Computadores

Compreender a forma de como são identificados os computadores no âmbito da Internet é essencial para o processo de investigação. Todos os computadores que acessam a Internet possuem uma forma de identificação única e singular chamada de endereço de IP, o IP é a sigla usada para Internet Protocol[4]. Tecnicamente, o endereço de Internet Protocol é formado por um número inteiro composto por 32 bits[5]. Os bits são decodificados em dois únicos valores; 0 e 1. Os computadores foram arquitetados para que fossem capazes de armazenar códigos múltiplos de bits, classificados como bytes. Os bytes possuem, no momento, oito bits, são chamados de octetos por serem uma sequência de oito bits agrupados, exemplo; 00110101. Portanto, o endereço de IP é decifrado pelo computador digitalmente em notação binária representada por zero e um.

É claramente inviável a adoção de códigos binários para o cotidiano dos seres humanos, recordar de endereços de IP toda vez que fosse necessário conectar um computador a Rede Mundial de computadores não traria praticidade. Os programas de computador efetuam a conversão da notação binária para a base decimal, promovendo a melhor compreensão dos números pelos humanos, exemplo; 00110101 equivale ao número 200. Obviamente, dessa forma, os números seriam de melhor memorização e compreensão, porém, esse ainda não constituiria o melhor meio de comportar um endereço referente a um computador. Deste modo, fez-se mais conveniente e prático a atribuição de nomes aos números, criando um sistema que estabelece a tradução do endereço de IP em nome e letras.[6]

---

[4] Em consonância com o Meu IP identificador de dispositivos "Protocolo de Internet. IP significa "Internet Protocol" e é um número que identifica um dispositivo em uma rede (um computador, impressora, roteador, etc.). Estes dispositivos são parte de uma rede e são identificados por um número de IP único na rede. O endereço IP é composto por 4 números (até 3 dígitos) e separados por "." (ponto). Os valores que podem assumir estes números variam entre 0 e 255, por exemplo, um endereço de IP pode ser 192.168.66.254 (quatro números entre 0 e 255 separados por pontos)." Meu IP. Identificador de dispositivo. 2017. Disponível em: < http://meuip.eu/ > Acesso em: 2 fev. 2017.

[5] De acordo com Guimarães e Cabral "**Bit** é a sigla para Binary Digit, que em português significa dígito binário, ou seja, é a menor unidade de informação que pode ser armazenada ou transmitida. É geralmente usada na computação e teoria da informação. Um **bit** pode assumir somente 2 valores, como 0 ou 1." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em <https://www.significados.com.br/bit-e-byte/ > Acesso em: 2 fev. 2017.

[6] Roteiro de atuação: crimes cibernéticos / 2. Câmara de coordenação e revisão. – 3.ed. rev. e ampl. – Brasília: MPF, 2016. Pág; 23.

2.2 Distribuição De IP

A distribuição de IPs deve ser impreterivelmente de forma organizada, pois é necessário que cada host[7] criado seja único para melhor localização por parte da rede mundial de computadores, ou seja, não pode existir mais de um host partilhando o mesmo endereço na rede. Por isso, adota-se um modelo de patamares. A instituição responsável pela distribuição e organização de IPs é a Internet Assigned Numbers Authority[8], localizada nos Estados Unidos, está no topo do patamar na locação de blocos de endereços de IPs.

2.3 Sistema De Nomes De Domínio (DNS)

A Advanced Research Projects Agency Network[9](ARPANET), ascendente da Internet, criada pelo departamento de defesa dos Estados unidos da América em 1970 comportava um número restrito de computadores conectados entre si. Nesta Rede, a cada host era atribuído um nome próprio e todos os computadores carregavam um registro que armazenava todos os nomes dos outros respectivos hosts conectados a esse ambiente virtual, ou seja, todos possuíam um nome de identificação de fácil reconhecimento.[10]

Caso fosse necessária a mudança do nome de algum host seria preciso repassar a informação ao computador central responsável a atribuição do novo nome. O computador central recolhia, em um período de tempo determinado, todas as alterações de nomes realizadas na rede sempre deixando a lista de hosts atualizada. A classificação era disponibilizada por meio de um arquivo de texto chamado de HOSTS.TXT[11].

---

[7] Em concordância com Viana "por definição, **host** é qualquer computador ou máquina conectado a uma rede, que conta com número de IP e nome definidos. Essas máquinas são responsáveis por oferecer recursos, informações e serviços aos usuários ou clientes. Por essa abrangência, a palavra pode ser utilizada como designação para diversos casos que envolvam uma máquina e uma rede, desde computadores pessoais à roteadores." VIANA, Gabriela. Revista eletrônica Techtudo. 2012. Disponível em: < http://www.techtudo.com.br/artigos/noticia/2012/02/o-que-e-um-host.html >. Acesso em 3 de fevereiro de 2017.

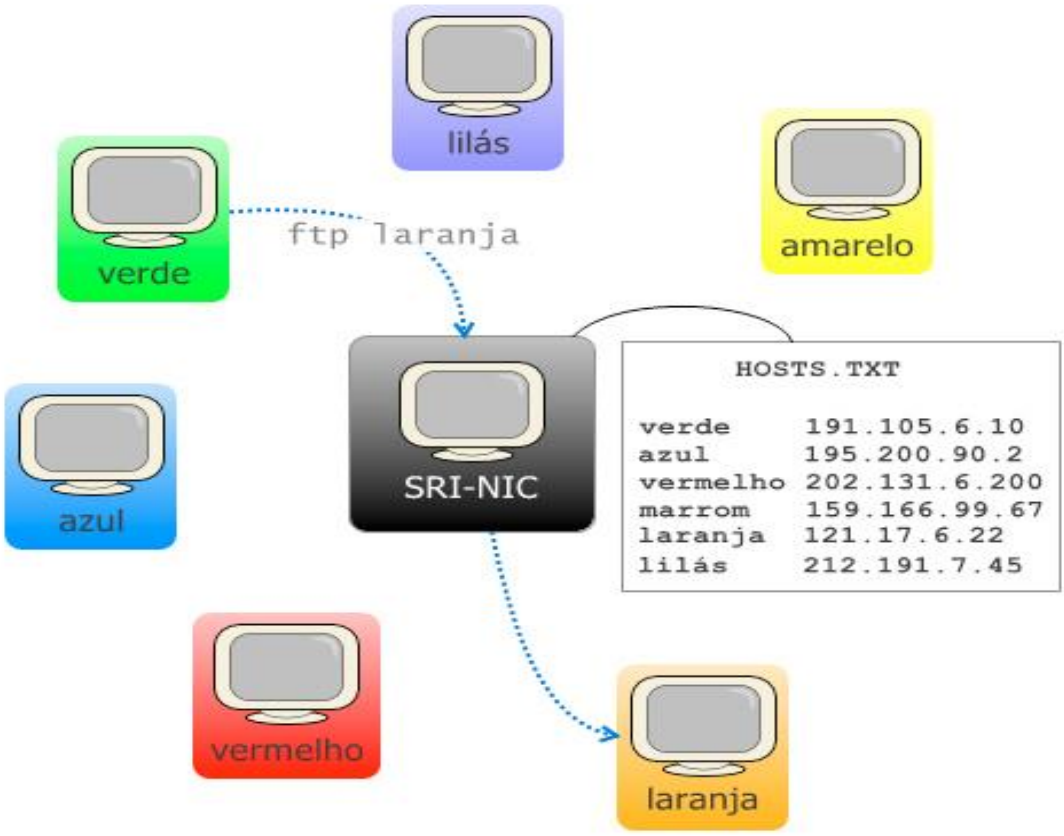
[8] Autoridade Atributiva de Números da Internet.

[9] Agência de Pesquisas em Projetos Avançados.

[10] Roteiro de atuação: crimes cibernéticos / 2. Câmara de coordenação e revisão. – 3.ed. rev. e ampl. – Brasília: MPF, 2016. Pág; 32.

[11] Consoante o Roteiro de Atuação "pode-se fazer analogia a uma agenda telefônica, que por sua vez relaciona nomes de pessoas com seus respectivos números. O arquivo HOSTS.TXT era uma agenda que relacionava nomes dos hosts com seus respectivos identificadores numéricos na rede." Roteiro de atuação: crimes cibernéticos / 2. Câmara de coordenação e revisão. – 3.ed. rev. e ampl. – Brasília: MPF, 2016, Pág;32.

Figura 1 Sistema de Nomes de Domínio, HOSTS.TXT da ARPANET



Fonte: Ministério Público Federal. **Roteiro de atuação – crimes cibernéticos.** Brasília – DF, 2016, pág. 33

Conforme a rede foi crescendo e o número de hosts aumentando a lista que catalogava todos os nomes findou sem utilidade, pois manter a lista atualizada segundo o método original que havia sido criada se tornou inviável para a ARPANET. O servidor que compartilhava o arquivo HOSTS.TXT não estava mais comportando o grande tráfego de informações, pois cresciam sem cessar os nomes e números dos novos hosts que adentravam a rede. O crescimento dos hosts ensejou em alguns conflitos frequentes, como o compartilhamento de nomes iguais a hosts distintos. Desta forma, os engenheiros do Departamento de Defesa optaram por desenvolver um novo sistema que suportasse os novos parâmetros descentralizados dos nomes de domínio, assim, poderiam fazer a manutenção da lista. Dado o exposto, o DNS, como é reconhecido atualmente, foi criado unicamente para a resolução da descentralização que adveio pelo aumento dos hosts.[12]

Tendo em vista os aspectos observados, o Sistema de Nome de Domínio trata-se de uma base de dados difundida na Rede Mundial de Computadores. Levando em consideração

[12] Roteiro de atuação: crimes cibernéticos / 2. Câmara de coordenação e revisão. – 3.ed. rev. e ampl. – Brasília: MPF, 2016. Pág; 33.

esses aspectos pode-se dizer que a Internet é na verdade o antigo sistema HOSTS.TXT do Departamento de Defesa Norte-Americano, que agora é acessível a população e espalhado em milhões de hosts pelo mundo. Essa disposição de hosts na rede de computadores é feita de forma descentralizada e possui uma hierarquia própria, por isso, a ARPANET não é mas a única responsável pelas atualizações supervenientes da distribuição de hosts. Em 1980 a ARPANET se dividiu em dois estabelecimentos, um deles herdou o mesmo nome do estabelecimento original e o outro foi batizado de Milnet, este ultimo findou sendo uma rede militar. A interligação desses dois órgãos é chamada de DARPA (Defense Advanced Research Projects Agency) (CASTRO, 2003, pág.2).

2.4 World Wide Web

Um dos elementos que fez com que a Internet se difundisse pelo mundo em grande escala foi a World Wide Web (WWW) que segundo Corrêa refere-se a:

> "Um conjunto de padrões e tecnologias que possibilitam a utilização da Internet por meio dos programas navegadores, que por sua vez tiram todas as vantagens desse conjunto de padrões e tecnologias pela utilização do hipertexto e suas relações com a multimídia, como som e imagem, proporcionando ao usuário maior facilidade na sua utilização, e também a obtenção de melhores resultados. " (CORRÊA, 2002, pág.11)

A WWW começou a ser desenvolvida em 1989, mas só entrou em vigor no ano seguinte que, conforme a ideia de Bernes-Lee, membro do laboratório de Física, em Genebra, recomendou a invenção de um sistema de redes conectadas que pudessem estabelecer a comunicação entre laboratórios, facilitando a interação entre os pesquisadores que estivessem em lugares distintos, a fim de facilitar as pesquisas desenvolvidas por eles. Em virtude disso, a World Wide Web foi o primeiro browser[13] a ser trabalhado para o desenvolvimento de fluxo de dados em rede.

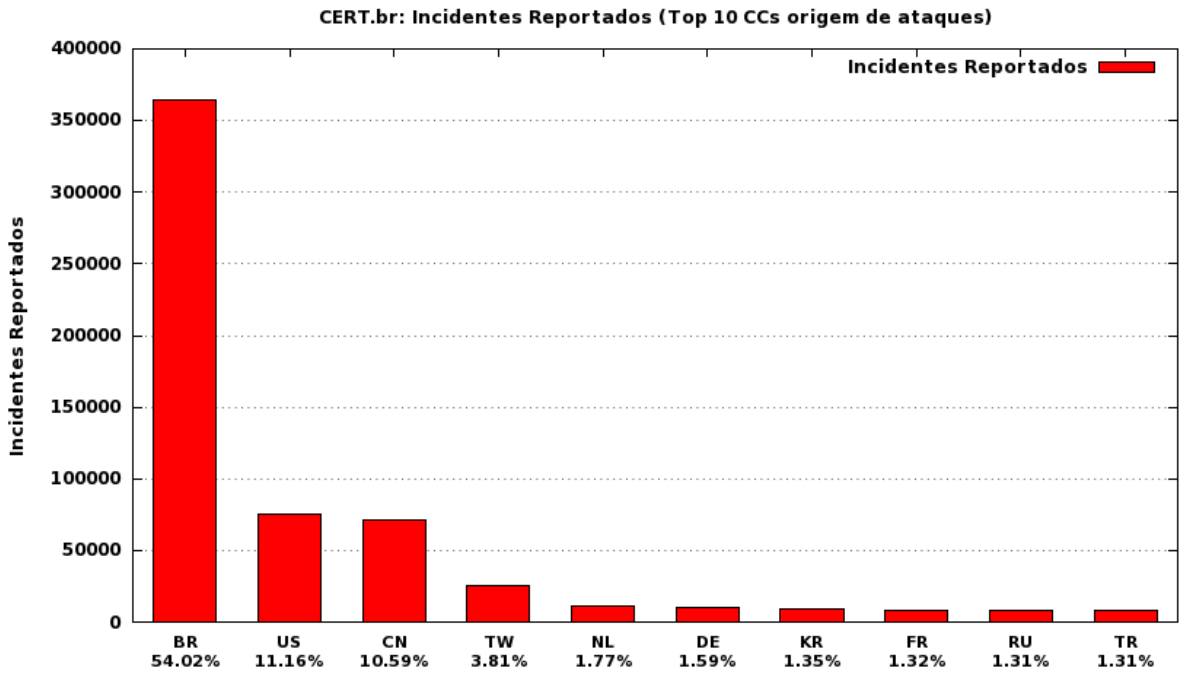
[13] Segundo Guimarães e Cabral "***Browser*** é um **programa** desenvolvido para permitir a **navegação pela web**, capaz de processar diversas linguagens, como HTML, ASP, PHP. Sua interface vai variar de acordo com a marca, onde quem escolhe é o usuário. Em inglês, o verbo *browse* pode significar procurar ou olhar casualmente para alguma coisa. Assim, o browser é um navegador, que permite que o utilizador encontre o que procura na internet. O *browser* ou *web browser* é responsável pela comunicação com os servidores, é ele que processa os dados recebidos pelos servidores da Internet e processa as respostas. Antigamente, os primeiros *browsers* tinham apenas texto, mas com o tempo foram aperfeiçoados, foram criados mecanismos para interagir com o usuário, com interfaces rápidas, coloridas e de fácil acesso." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: <. https://www.significados.com.br/browser/. > Acesso em: 5 de fevereiro de 2017

2.5 Ameaças Incidentes Na Web

Grande parte das ocorrências ligadas aos crimes faz uso dos meios eletrônicos para lograrem êxito, crimes como a injúria, calúnia, difamação, furto de dados, invasão de contas pessoais, fraudes eletrônicas, pirataria, pedofilia etc, todos eles podem ser cometidos através da informática, portanto são também classificados como cibernéticos. Existe a necessidade de vigilância sobre o tráfego desses dados de cunho criminoso por profissionais competentes, sobretudo no que tange condução da investigação e análise pericial (HATAKA, Sidney Akira, 2013, pág 3).

É indiscutível que além da internet ter um fluxo elevado de trânsito de informações pessoais ou públicas a mesma virou meio de propagação de crimes. Conforme os registos do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil os índices de incidentes reportados são disparadamente maiores do que quando comparados aos outros países.

Tabela 1- Incidentes Reportados ao CERT.br – janeiro a dezembro de 2015



Fonte: <https://www.cert.br/stats/incidentes/2015-jan-dec/top-atacantescc.html> - Acesso em: 15 de mar de 2017

Conforme exposto, com os assentamentos do CERT.BR pode-se notar a elevada taxa de incidentes que foram registradas no Brasil dentro do período de um ano. A tabela deflagra que a taxa brasileira é aproximadamente cinco vezes maior que as taxas dos Estados Unidos

da América e do Canadá. As ameaças cibernéticas multiplicam e espalham-se entre os computadores na medida em que se deslocam de um dispositivo a outro. Dependendo das ameaças que circulam a internet os danos causados ao hospedeiro infectado podem causar lesões ao software[14] ou ao hardware[15], diminuindo o desempenho funcional do computador. De acordo com CERT.BR as principais ameaças que incidem no país dentre um período de 10 anos são os worms, os scans e as fraudes, como observa-se na tabela abaixo:

Tabela 2 – Totais Mensais e Anual Classificados por Tipo de Ataque - Estatística de incidentes de janeiro a dezembro de 2005

Mês	Total	worm (%)		af (%)		dos (%)		invasão (%)		web (%)		**scan** (%)		fraude (%)	
jan	**4448**	1019	22	16	0	0	0	14	0	22	0	2694	60	683	15
fev	**3142**	1157	36	5	0	1	0	27	0	57	1	1433	45	462	14
mar	**4848**	1906	39	1	0	2	0	42	0	24	0	1805	37	1068	22
abr	**5253**	1432	27	17	0	0	0	20	0	25	0	1437	27	2322	44
mai	**6883**	2175	31	4	0	2	0	34	0	22	0	1489	21	3157	45
jun	**5406**	1510	27	0	0	5	0	17	0	55	1	1356	25	2463	45
jul	**5146**	1329	25	3	0	2	0	15	0	22	0	1045	20	2730	53
ago	**5718**	1144	20	7	0	5	0	45	0	41	0	1522	26	2954	51
set	**5361**	1075	20	2	0	2	0	87	1	64	1	1527	28	2604	48
out	**6316**	1220	19	4	0	13	0	66	1	62	0	2185	34	2766	43
nov	**7901**	1484	18	4	0	45	0	43	0	122	1	3022	38	3181	40
dez	**7578**	1881	24	2	0	19	0	38	0	54	0	2682	35	2902	38
Total	**68000**	17332	25	65	0	96	0	448	0	570	0	22197	32	27292	40

Fonte: <https://www.cert.br/stats/incidentes/2015-jan-dec/top-atacantescc.html> - Acesso em: 15 de mar de 2017

[14] Em conformidade com Guimarães e Cabral "Software é uma sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas. Também pode ser definido como os programas que comandam o funcionamento de um computador. Em um computador, o software é classificado como a parte lógica cuja função é fornecer instruções para o hardware. Existe também o conceito de software livre, que remete para um programa que dá liberdade ao utilizador, permitindo que ele o estude, modifique e compartilhe com outras pessoas. Para isso, é preciso que o utilizador possa aceder o código-fonte, para mudá-lo conforme as suas necessidades." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: < https://www.significados.com.br/software/> Acesso em: 10 de fevereiro de 2017.

[15] Entende Guimarães e Cabral "*Hardware* é a parte física de um computador, é formado pelos componentes eletrônicos, como por exemplo, circuitos de fios e luz, placas, utensílios, correntes, e qualquer outro material em estado físico, que seja necessário para fazer com o que computador funcione. O *hardware* é basicamente utilizado por computadores e elementos eletrônicos. Qualquer equipamento físico como chaves, fechaduras, correntes e peças do próprio computador, são chamados de *hardware*. O *hardware* não se limita apenas a computadores pessoais, também está disponível em automóveis, celulares, tablets e etc." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: < https://www.significados.com.br/hardware/>.Acesso em: 10 de fevereiro de 2017.

Tabela 3 – Totais Mensais e Anual Classificados por Tipo de Ataque - Estatística de incidentes de janeiro a dezembro de 2015

Mês	Total	worm (%)		dos (%)		invasão (%)		web (%)		**scan** (%)		**fraude** (%)		outros (%)	
jan	**67661**	2829	4	1367	2	409	0	6547	9	36445	53	18465	27	1599	2
fev	**66700**	2682	4	2056	3	289	0	8102	12	39267	58	12513	18	1791	2
mar	**52959**	2867	5	70	0	489	0	8822	16	32351	61	6338	11	2022	3
abr	**52991**	3046	5	34	0	150	0	6297	11	31215	58	10571	19	1678	3
mai	**58322**	3122	5	374	0	177	0	5399	9	23242	39	23890	40	2118	3
jun	**81244**	3423	4	1016	1	157	0	9219	11	29593	36	36327	44	1509	1
jul	**53075**	4141	7	2763	5	160	0	4716	8	32601	61	6561	12	2133	4
ago	**65486**	3683	5	3354	5	104	0	4447	6	33446	51	18701	28	1751	2
set	**59311**	4326	7	2511	4	119	0	3993	6	29759	50	16560	27	2043	3
out	**52226**	6301	12	1702	3	140	0	4315	8	32554	62	6089	11	1125	2
nov	**64203**	5912	9	9142	14	145	0	2297	3	38482	59	6595	10	1630	2
dez	**48027**	5390	11	971	2	118	0	1493	3	32268	67	6165	12	1622	3
Total	**722205**	47722	6	25360	3	2457	0	65647	9	391223	54	168775	23	21021	2

Fonte: <https://www.cert.br/stats/incidentes/2015-jan-dec/top-atacantescc.html> - Acesso em: 15 de mar de 2017

É notório o crescimento das ameaças cibernéticas na nação brasileira, em 2005 o índice total de crimes cometidos foram 68.000, já em 2015 a totalidade dos crimes durante o ano foram de 722.205, um crescimento alarmante. Os computadores domésticos, devido a sua popularização, acabaram por se tornarem os principais alvos dos crimes cibernéticos nos últimos anos por serem mais vulneráveis devido à falta de proteção, desta forma é possível ter acesso aos aparelhamentos das vítimas através de técnicas de invasão, gerando facilidade ao furto de dados, informações particulares, senhas de bancos, e também na derrubada de páginas da web.

Com base nesse panorama é evidentemente preciso o desenvolvimento da pesquisa sobre as técnicas usadas pelos criminosos cibernéticos que atuam por meios maliciosos, a fim de proporcionar ao Estado e aos usuários domésticos um conhecimento prévio, capaz de promover melhor proteção dos mesmos. Com isso, é necessário analisar as ameaças mais incidentes: o Malware e suas espécies; Vírus, Worm, Bot e Botnet, Spyware, Backdoor, Cavalo de Troia, Rootkit e o Scan.

2.5.1 Malware

Malware[16] são os códigos maliciosos utilizados para a prática de crimes, conforme o CERT, eles são programas feitos exclusivamente para executar procedimentos ilícitos em um computador. É avaliado com uma espécie maligna de código que tem por finalidade ter acesso ao dispositivo do usuário sem o seu conhecimento ou consentimento. Segundo Oliveira e Torres, pode-se contaminar o computador do usuário da seguinte forma:

> "As principais formas como os códigos maliciosos podem infectar ou comprometer um computador são: Pela exploração de vulnerabilidades existentes nos programas instalados, por auto execução de mídias removíveis infectadas, como exemplo pen-drives, pelo acesso a páginas Web, utilizando navegadores vulneráveis, por ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos, pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas" (OLIVEIRA E TORRES, Crimes Cibernéticos, Estudo de Caso: Técnica Maliciosa, pág. 2).

Igualmente, os Malwares comumente também acessam os dispositivos das vítimas por meio de demos de jogos, e-mail, download de músicas, assinaturas gratuitas e por intermédio de qualquer via que permita o usuário baixar arquivos da web. Uma das formas de reconhecer a infecção por malware é a lentidão excessiva da máquina do usuário. A forma de retirá-lo é por meio de ferramentas de remoção em softwares de antivírus. Outra forma de detectar a contaminação é submetendo a análise online de arquivos suspeitos através de sites[17] como virusscan.jotti.org que ajudam a encontrar esses códigos maliciosos.

Figura 2– Análise online de malware

Fonte: <http://virusscan.jotti.org> - Acesso em: 20 de mar de 2017

[16] O Avast concerne que "Malware é a abreviatura de "Software malicioso"." Avast software, AVG Technologies. 2016. Disponível em: <https://www.avast.com/pt-br/c-malware. >. Acesso em: 12 de fevereiro de 2017.

[17] Entende Guimarães e Cabral que "*Website* é uma palavra que resulta da justaposição das palavras inglesas *web* (rede) e *site* (sítio, lugar). No contexto das comunicações eletrônicas, *website* e *site* possuem o mesmo significado e são utilizadas para fazer referência a uma página ou a um agrupamento de páginas relacionadas entre si, acessíveis na internet através de um determinado endereço. No Português Europeu é também comum utilizar o termo sítio da internet ou sítio eletrônico." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: < https://www.significados.com.br/website/>.Acesso em: 13 de fevereiro de 2017.

Figura 3– Análise online de malware

Fonte: <http://virusscan.jotti.org> - Acesso em: 20 de mar de 2017

2.5.2 Vírus

O Vírus é uma espécie de programa de computador ou um pedaço de código que é baixado no dispositivo da vítima sem o seu consentimento. Essa espécie maliciosa de código é destrutiva, instituída para assumir o controle de sistemas frágeis. Possui a capacidade de se espalhar para vários dispositivos conectados a rede, portando-se também como um vírus de corpo humano criando cópias de si mesmo a fim de se proliferar na internet. De acordo com Oliveira e Torres os vírus se definem:

> "Um vírus de computador como sendo um software com capacidade de se duplicar, infectando outros programas, usualmente com alguma intenção maliciosa. Um vírus não pode executar-se sozinho, requer que o seu programa hospedeiro seja executado para ativar o vírus; Segundo Cert(2014), vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas ou arquivos. O vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o computador seja infectado é preciso que um programa já infectado seja executado." (OLIVEIRA E TORRES, Crimes Cibernéticos, Estudo de Caso: Técnica Maliciosa, pág. 3).

Vale ressaltar que os vírus mais comuns geralmente são adquiridos via e-mail através de arquivos que vem em anexo, eles acabam induzindo a vítima a abrir o arquivo e infectar o seu computador. Outra forma de contrair o vírus é simplesmente acessando alguma página na internet que, anonimamente, já possui o malefício embutido no seu sistema, de forma que o acesso comum à página seja suficiente para executar o código malicioso. Este tipo de vírus é formado em linguagem de script[18] e por isso foi batizado com o mesmo nome. Ainda assim,

[18] Concerne Guimarães e Cabral que "em Informática, *script* é um conjunto de instruções em código, ou seja, escritas em linguagem de computador. É uma linguagem de programação que executa diversas funções no interior de um programa de computador. As linguagens de *script* são ferramentas utilizadas para controle de um determinado programa ou aplicativo; para configuração ou instalação em sistemas operacionais; e ainda, em jogos para controlar as ações dos personagens. Algumas linguagens de programação geralmente usadas como *script* são: ActionScript, JavaScript, Lua, PHP, Python, ShellScript, Ruby, VBScript." GUIMARÃES, DIL-

eles podem estar escondidos em programas de uso comum e compartilhamento entre pessoas conectadas a web, como um jogo ou um PDF de um livro. A interação como malefício faz com que ele desempenhe sua função automaticamente. Nos anos 90, os vírus se propagavam por meio dos disquetes[19] que eram o recurso de armazenamento móvel no momento. Quando os disquetes caíram em desuso novas formas de armazenamento de mídias surgiram, como os pen-drives, por exemplo, que se tornaram formas de propagação de vírus.

2.5.3 Worm

A palavra worm significa "verme", trata-se de uma espécie de arquivo danoso, esse tipo de vírus habita dentro da memória ativa do computador e tem a habilidade de se replicar automaticamente sem que seja necessária a participação do usuário abrindo um arquivo contaminado ou executando-o para fomentar a sua replicação. Ele se instala no dispositivo devido ao estado de seus programas e da sua própria fragilidade, quanto mais vulnerável estiverem ou desatualizados, mais fácil se torna a sua contaminação. (WENDT, Emerson,2011, Págs. 31, 35 e 61).

Desta forma, pode-se entender que os worms são culpados por dizimarem os recursos do computador, reduzindo a sua performance em rede e podendo superlotar o espaço do disco rígido devido a sua própria proliferação quando cria copias dele mesmo. Os worms são transmissíveis através de anexos, links de sites ou quando se compartilha dados. Como eles consomem a memória do dispositivo, os servidores de redes ao qual está conectado o computador passam a ficar sem resposta aos comandos do usuário. (CERT.BR, 2015).

O processo de proliferação do worm se inicia primeiramente por meio da identificação dos dispositivos que almeja atingir, produzida da seguinte forma: é feita uma varredura na web por computadores infectados e identificam-se os computadores que estejam ativos através do contato que possuem entre si, por meio de listas criadas na internet e das informações contidas em cada computador possuidor do vírus. Feitas as identificações o worm passa a si copiar para que possa se propagar enviando seus clones da seguinte maneira: em anexos de e-mail, aplicativos sociais de trocas de mensagens em tempo real, explorando as áreas vulneráveis do computador hospedeiro e com o compartilhamento de pastas em redes P2P[20]. Desta

---

VA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: < https://www.significados.com.br/script/ >.Acesso em: 11 de fevereiro de 2017.

19 É um aparelho removível e era usado em computadores antigos como meio de armazenar arquivos.

[20] Conforme Ciriaco "P2P (do inglês *peer-to-peer*, que significa par-a-par) é um formato de rede de computadores em que a principal característica é descentralização das funções convencionais de rede, onde o computador de cada usuário conectado acaba por realizar funções de servidor e de cliente ao mesmo tempo.

forma seguem as ativações das cópias do worm logo quando recebidas ou quando ele vem através de uma mídia removível, no qual precisa que haja a sua inserção no computador para que possa ser executado. Em consequência disso, logo após a infecção do computador o processo se reinicia e o hospedeiro passa a ser o produtor dos incidentes. (CERT.BR, 2015).

2.5.4 Bot e Botnet

O Bot é uma espécie de programa que permite que o invasor possa controlar, através de seus mecanismos, remotamente o computador da vítima. Ele é similar ao worm quanto ao seu desempenho referente ao contágio, isto é, possui a capacidade de se propagar automaticamente se utilizando das fragilidades nos aplicativos e programas residentes no dispositivo, conforme observa Oliveira e Torres:

> "Bot é um malware que dispõe de mecanismos de comunicação com o invasor, que permitem que o computador da vítima seja controlado remotamente. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado." (OLIVEIRA E TORRES, Crimes Cibernéticos, Estudo de Caso: Técnica Maliciosa, pág. 3).

O invasor estabelece a comunicação com o computador contaminado por meio da web, canais de rede P2P ou IRC[21]. Quando regularizada a comunicação com o computador contaminado o invasor pode executar ações ou até mesmo ataques a outros dispositivos. Quando um computador é alvo de um bot ele passa a ser um zombie computer[22], é classificado com essa nomenclatura pelo fato de ser manipulado remotamente sem a ciência do usuário do computador, conforme observa Oliveira e Torres no seu estudo sobre crimes cibernéticos:

> "Um computador infectado por um bot costuma ser chamado de zumbi, pois pode ser controlado remotamente, sem o conhecimento do seu dono. Também pode ser chamado de spam zumbi quando o bot instalado o transforma em um servidor de e-mails e o utiliza para o envio de spam, assim contaminando outros computadores."

Seu principal objetivo é a transmissão de arquivos e seu surgimento possibilitou o compartilhamento em massa de músicas e filmes. Com a crescente utilização da rede P2P para este fim, cada vez mais surgem programas para este fim, porém nem sempre eles atendem às expectativas do usuário." CIRIACO, Douglas. Tecmundo. 2008. Disponível em: <https://www.tecmundo.com.br/torrent/192-o-que-e-p2p-.htm >. Acesso em: 18 de fevereiro de 2017.

[21] De acordo com Adami "O IRC **(***Internet Relay Chat***)** é um protocolo utilizado na Internet como troca de arquivos e de informações. Desenvolvido em 1988 pelo programador Jarkko Oikarinen, só foi utilizado de maneira formal em 1993. O objetivo da criação foi desenvolver um sistema compatível a TCP/IP e SSL, com capacidade e armazenamento de conversas entre muitos usuários simultaneamente. A primeira rede com IRC surgiu em Universidades da Finlândia e em 1993, o sistema foi utilizado para informar as notícias em tempo real pela internet. O modo de comunicação e canais do IRC é a conversação de um canal, no qual os usuários enviam mensagens ao servidor que as reenvia a todos do mesmo canal. Como o IRC é um protocolo de texto, pode ser utilizado através de um servidor como o netcat ou telnet." ADAMI, ANNA. Infoescola. 2017. Disponível em: < http://www.infoescola.com/internet/internet-relay-chat-irc/ >. Acesso em 18 de fevereiro de 2017.

[22] Computador Zumbi.

> (OLIVEIRA E TORRES, Crimes Cibernéticos, Estudo de Caso: Técnica Maliciosa, pág. 3).

O Botnet é uma forma melhorada do Bot, ele é formado por uma teia de computadores zumbis interconectada por um mesmo Bot, isso permite um maior ataque danoso na web, pois quanto mais aumentar o número de computadores infectados maior é o alcance de área para o invasor controlar, isso permite que os ataques sejam direcionados ou não a um fim comum, como por exemplo; o invasor pode promover o aluguel de uma teia Botnet para um grupo terrorista para executar um ataque com um fim específico.

> "Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots. As principais ações maliciosas que costumam ser executadas por intermédio de botnets são: ataques de negação de serviço, propagação de códigos maliciosos (inclusive do próprio bot), coleta de informações de um grande número de computadores, envio de spam e camuflagem da identidade do atacante." (OLIVEIRA E TORRES, Crimes Cibernéticos, Estudo de Caso: Técnica Maliciosa, pág. 4).

Em consequência disso, alguns dos ataques que podem ser executados no uso dos botnets, são: inexecução de um serviço, proliferação do vírus, colheita de informação de toda a teia de computadores envolvida, disseminação de spams[23] e a ocultação da identidade do autor por meio de proxies[24] nos computadores hospedeiros.

2.5.5 Backdoor

Backdoor significa porta dos fundos, ele possui essa nomenclatura porque permite que um invasor que já tenha corrompido o computador anteriormente volte a invadi-lo novamente.

---

[23] Consonante Guimarães e Cabral "Spam é um termo de origem inglesa cujo significado designa uma mensagem eletrônica recebida mas não solicitada pelo usuário. O conteúdo de um spam é normalmente uma mensagem publicitária que tem o objetivo de divulgar os serviços ou produtos de alguma empresa a uma grande massa de usuários de e-mail. Além das corriqueiras mensagens para fins comerciais, existem vários outros tipos de spam que invadem as caixas de mensagens dos usuários. Por exemplo, aquelas mensagens maliciosas que tentam induzir o usuário a informar os seus dados pessoais ou da sua conta bancária ou ainda, executar algum programa que contém vírus. Outros tipos de spam como boatos ou correntes, que estimulam ou forçam o usuário a reencaminhar para os seus contatos, têm geralmente o objetivo de expandir a base de dados de email do *spammer*. Em muitos casos, os usuários não têm o cuidado de ocultar os endereços de email quando reencaminham este tipo de mensagem." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: <https://www.significados.com.br/spam/ >. Acesso em: 14 de fevereiro de 2017.

[24] Em concordância com Oliveira "Proxy é o termo utilizado para definir os intermediários entre o usuário e seu servidor. Todos os dados que deseja acessar na internet são disponibilizados por um servidor. Logo, o servidor proxy atende seus pedidos e repassa os dados do usuário à frente. O cliente conecta-se a um servidor proxy, requisita algum serviço e cabe ao proxy enviar a solicitação do endereço local para o servidor, traduzindo e repassando o seu pedido para o seu PC. Essa solicitação pode ser algo como um arquivo, um site na web, ou qualquer outro recurso disponível em outro servidor. Esse endereço local da sua máquina não pode ser acessado por qualquer rede externa. O proxy conecta o seu computador a uma rede externa, como a internet. Representando a 'identidade do seu PC' no servidor de destino da sua solicitação." OLIVEIRA, Arize. Revista eletrônica techtudo. 2016. Disponível em: < http://www.techtudo.com.br/artigos/noticia/2011/05/o-que-e-proxy-descubra-o-significado-desse-termo.html>. Acesso em: 20 de fevereiro de 2017.

Observa-se que esse código malicioso pode se infiltrar nos computadores descobrindo as suas fragilidades nos programas já residentes e também através de outros malwares que tenham infectado o dispositivo anteriormente. Nesse sentido, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil concerne:

> "Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo. Após incluído, o backdoor é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado. A forma usual de inclusão de um backdoor consiste na disponibilização de um novo serviço ou na substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitem o acesso remoto." (CERT.BR,2015).

Logo após a sua inserção, o backdoor garante uma futura acessibilidade ao dispositivo eletrônico, sem que possam notar a sua presença, isso permite que ele possa manipular remotamente o hospedeiro sem precisar realizar uma outra invasão.

2.5.6 Cavalo de troia

É uma espécie de programa cuja função é a alteração dos aplicativos já existentes, sem a ciência do usuário, de forma a invadir os computadores. Geralmente se infiltram por meio de sites na web que oferecem propagandas, Gifs[25], backgrounds[26], galerias de fotos e jogos. Usualmente esses programas tratam-se de um arquivo exclusivo e, para executá-lo, é necessária a interação do usuário com os mesmos para que eles possam se instalar no computador. (CERT.BR,2015).

---

[25] Conforme Brito "GIF (*Graphics Interchange Format ou formato de intercâmbio de gráficos*) é um formato de imagem muito usado na Internet, e que foi lançado em 1987 pela CompuServe, para disponibilizar um formato de imagem com cores em substituição do formato RLE, que era apenas preto e branco. Um tipo particular de GIF bastante conhecido é o chamado GIF animado. Ele na verdade é composto de várias imagens do formato GIF, compactadas em um só arquivo. Essa variante é utilizada para compactar objetos em jogos eletrônicos, para usar como emoticon em mensageiros instantâneos e para enfeitar sites na Internet. Apesar do formato GIF atualmente ainda ser muito utilizado na web por conta de seu tamanho compacto, ele tem uma paleta limitada de cores - 256 no máximo -, impossibilitando o seu uso prático na compactação de fotografias. Por causa disso, o formato GIF é utilizado apenas para armazenar ícones e pequenas animações." BRITO, Edivaldo. Revista eletrônica Techtudo. Disponível em: http://www.techtudo.com.br/artigos/noticia/2012/04/o-que-e-gif.html. Acesso em: 21 de fevereiro de 2017.

[26] Guimarães e Cabral entendem "no contexto da informática a palavra *background* muitas vezes remete para o plano de fundo, ou seja o papel de parede, a imagem que aparece no fundo do ambiente de trabalho ou de um site, por exemplo. Essa imagem de fundo que pode ser usado em alguns sites como Tumblr, Twitter, etc. Muitas dessas imagens são conhecidas como *vector background*, imagens que são feitas com pontos, linhas, curvas, que são fundamentadas em fórmulas matemáticas e apresentadas em gráficos de computador." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: < https://www.significados.com.br/background/>.Acesso em: 16 de fevereiro de 2017.

2.5.7 Rootkit

O Rootkit é uma espécie de programa que esconde e permite que um invasor ou um código maléfico fiquem assegurados em um dispositivo eletrônico. Deste modo, este código malicioso permite a remoção de dados de arquivos, a instalação de outros malwares, oculta informações residentes no computador, realiza o mapeamento de fragilidades pertinentes a outros dispositivos através de varreduras na web e sequestra informações da localidade do dispositivo. A sua principal atribuição é manter o acesso ao computador corrompido. Conforme a cartilha de segurança para internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil entende-se que:

> "Rootkits inicialmente eram usados por atacantes que, após invadirem um computador, os instalavam para manter o acesso privilegiado, sem precisar recorrer novamente aos métodos utilizados na invasão, e para esconder suas atividades do responsável e/ou dos usuários do computador. Apesar de ainda serem bastante usados por atacantes, os rootkits atualmente têm sido também utilizados e incorporados por outros códigos maliciosos para ficarem ocultos e não serem detectados pelo usuário e nem por mecanismos de proteção." (CERT.BR, 2015).

O termo Root refere-se à conta do servidor administrador do sistema Unix, kit corresponde aos aglomerados de aplicativos e programas utilizados para manter-se como administrador mor da conta, por consequência disso o código malicioso foi batizado como Rootkit.

2.5.8 Comparação

Como pode-se observar todos os códigos possuem as suas peculiaridades e características singulares que os diferencia uns dos outros como tipo de instalação, proliferação, veículos de contágio, ações e entre outras particularidades. Desta forma, foi constituída por meio deste estudo uma tabela para melhor entendimento, comparação e distinção entre os vírus.

Tabela 4– Tabela comparativa de formas de obtenção de códigos maliciosos

Códigos Maliciosos						
	Vírus	*Worm*	*Bot*	*Trojan*	*Backdoor*	*Rootkit*
FORMAS DE CONTÁGIO						
Automaticamente da WEB		✓	✓			
Via e-mail	✓	✓	✓	✓		
Baixado da WEB	✓	✓	✓	✓		
Via compartilhamento de arquivos	✓	✓	✓	✓		
Mídias removíveis contaminadas	✓	✓	✓	✓		
Redes Sociais	✓	✓	✓	✓		
Mensagens instantâneas	✓	✓	✓	✓		
Por meio de um invasor		✓	✓	✓	✓	✓
Inserido por outro código malicioso		✓	✓	✓	✓	✓
FORMAS DE INSTALAÇÃO						
Executando arquivo contaminado	✓					
Executando o próprio código		✓	✓	✓		
Executando outro código					✓	✓
Através das fragilidades do dispositivo		✓	✓		✓	✓
PROPAGAÇÃO						
Se copia para se inserir em arquivos	✓					
Envia cópias para a web automaticamente		✓	✓			
Envia cópias para o e-mail automaticamente		✓	✓			
Não se copia				✓	✓	✓
AÇÕES COMUNS						
Alteração e remoção de arquivos	✓			✓		✓
Consome recursos		✓	✓			
Extrai informação			✓	✓		
Insere outros códigos		✓	✓	✓		✓
Viabiliza o retorno de códigos					✓	✓
Ataca na web		✓	✓			
Se mantém em sigilo	✓				✓	✓

Fonte: Elaborada pela própria autora.

Vale Ressaltar que as características e peculiaridades definidas nesses códigos maliciosos são cada vez mais difíceis de classificar devido ao surgimento de variantes que podem interligar atributos com os mesmos. Em virtude disso, a tabela formada por este estudo não é definitiva podendo mudar futuramente conforme forem surgindo novos atributos.

3. CRIME CIBERNÉTICO

Observa-se que a imagem do crime na seara do Direito Penal tem suas peculiaridades, quando fala-se sobre delito lembra-se de conduta criminosa e nexo causal do agente. Assim, para que seja concretizada a devida punição a um indivíduo é necessário que este fato praticado por ele trate-se de fato típico, antijurídico, culpável e punível previsto legalmente. No Código Penal o legislador optou por não definir especificamente o crime em si. Nota-se que na redação do primeiro artigo do referido código é feita apenas uma breve explanação "Art. 1º - Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal" (CÓDIGO PENAL, 1940).

Apesar disto, pode-se observar que no Decreto – Lei n. 3.914/41, lei de introdução ao Direito Penal, também não foi constituída uma definição de crime, estabelecendo unicamente a distinção entre o que são considerados crimes e o que seriam contravenções penais como narra o seu artigo 1°:

> "Considera-se crime a infração penal a que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente." (DECRETO-LEI Nº 3.914, de 9 de dezembro de 1941).

Segundo Heleno Fragoso, o Decreto – lei se restringiu em dar destaque as peculiaridades que diferenciam as infrações penais que são consideradas como crime das que são contravenções penais, cujo as quais notoriamente são restringidas a pena de prisão. (FRAGOSO apud BITENCOURT, 2012, p. 271). Em consequência disso a doutrina findou conceituando o crime, pois o legislador não forneceu o conceito. Alguns doutrinadores na seara penal almejaram tecer o melhor conceito para o crime e, muitos deles afirmam que ele classifica-se como sendo formal, material e analítico. (GRECO, 2013, p. 140).

Segundo Fernando Capez "Considerar a existência de um crime sem levar em conta sua essência ou lesividade material afronta o princípio constitucional da dignidade da pessoa humana". (CAPEZ, 2012, p. 134). Portanto, crime é o resultado do encaixe de uma conduta socialmente rejeitável que oferece perigo aos bens jurídicos, no texto normativo. Conforme Guilherme de Sousa pode-se conceituar o crime como o que a sociedade vê por um comportamento passível de ser coibido por lei, pois ofendendo um bem jurídico de outrem, deva receber uma penalização. (NUCCI, 2012, p. 174). Desta forma, Ivette Senise Ferreira explica que não existe um consenso comum entre os doutrinadores pois:

> "As várias possibilidades de ação criminosa da área informática, assim entendida em seu sentido lato, abrangendo todas as tecnologias da informação, do processamento e da transmissão de dados, originaram uma forma de criminalidade que, apesar da diversidade de suas classificações, pode ser identificada pelo seu objetivo ou pelos meios de atuação, os quais fornecem um denominador comum, embora com diferentes denominações nos vários países ou nos diferentes autores." (FERREIRA, 2001, pág 208).

Dado o exposto, os conceitos discernidos para os crimes que se realizam por via informática a fim de cometerem ilícitos penais, seja por intermédio da transmissão de dados via rede ou não, são vastos pois variam conforme o modo de raciocinar de cada doutrinador acerca da ilicitude. Segundo Fernando José da Costa (2011, pág. 51) "trouxe a internet um novo mundo, denominado digital. Nele as pessoas navegam, se comunicam e de um mundo virtual praticam condutas e consequências em um mundo real.". Por isso, entende-se que a internet pode ser benéfica, pois é de extrema utilidade a sociedade, como também pode ser por meio dela que condutas criminosas podem ser praticadas e seus efeitos difundidos pelo mundo real.

3.1 Deep Web

Existe uma parte da internet que não está registrada por isso não se pode encontra-la por vias normais. Para que essa parte da web possa ser acessada deve-se fazer uso de um software capaz de permitir o acesso, esse software assegura e preserva o anonimato da identidade dos usuários, o exemplo mais conhecido é o Tor. Devido o fato de serem preservadas as identidades dos usuários alguns criminosos se utilizam desse artifício para executarem atos ilícitos. Em consequência disso a Deep Web é abordada sempre com um sentido negativo. Acontece que a Deep Web não foi criada para atividades ilícitas, mas devido as suas disposições ela acabou por ser desvirtuada. O Tor proporciona a segurança das comunicações aos usuários como também o acesso a artigos, sites e blogs[27] que não pode se encontrar na Surface Web, em contrapartida o anonimato concedido por ela findou virando meio de práticas ilícitas, como venda de drogas ou armas por exemplo. O presente estudo também vista esclarecer os conceitos de Deep Web, Darknet e Dark Web que são erroneamente confundidos.

[27] Guimarães e Cabral ressaltam que "Blog é uma palavra que resulta da simplificação do termo weblog. Este, por sua vez, é resultante da justaposição das palavras da língua inglesa *web* e *log*. *Web*aparece aqui com o significado de rede (da internet) enquanto que *log* é utilizado para designar o registro de atividade ou desempenho regular de algo. Numa tradução livre podemos definir blog como um diário online. Blogs são páginas da internet onde regularmente são publicados diversos conteúdos, como textos, imagens, músicas ou vídeos, tanto podendo ser dedicados a um assunto específico como ser de âmbito bastante geral. Podem ser mantidos por uma ou várias pessoas e têm normalmente espaço para comentários dos seus leitores. Blogueiro é o nome dado a quem publica num blog e blogosfera é o conjunto de blogs." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: <https://www.significados.com.br/blog/> Acesso em: 17 de fevereiro de 2017.

> "É aqui que chegamos ao centro do debate: por um lado o Tor permite, entre outras coisas, assegurar a privacidade das comunicações entre utilizadores e visualizar artigos e blogs que não se encontram na Surface Web; por outro lado o anonimato serve de ferramenta para que ocorra a prática de atividades ilícitas. Existe uma linha muito ténue que separa a esfera pública da esfera privada. O Tor permite reforçar a segurança ao utilizar a Internet. Cabe ao bom senso de cada um a forma como utiliza as ferramentas ao seu dispor." (DUARTE e MEALHA, 2016, Pág. 2)

O lado da internet que está exposto ao uso de todas as pessoas, cujo qual não pode ser acessada pelas vias de busca comum a população, segundo David Duarte e Tiago Mealha possuem várias nomenclaturas, são elas "Deep Web, Deep Net, Hidden Web ou Invisible Web", eles a classificam da seguinte forma:

> "No ano de 2000, Michael k. Bergman afirmou que pesquisar na Internet pode ser como pescar na superfície de um oceano- um grande peixe pode ser apanhada na rede contudo, existe uma imensidão de peixes mais ricos que se encontram nas profundezas e, consequentemente não foram pescados." (DUARTE e MEALHA, 2016, Pág. 8).

Grande parte das informações e dados da rede encontram-se em uma profundidade tamanha que as vias de busca comuns oferecidas pela internet não são capazes de reconhecer esse conteúdo, em grosso modo a Surface Web seria apenas a ponta do Iceberg enquanto a Deep Web consistira em todo o resto. Desse modo, em virtude da magnitude de tamanho da Deep Web se torna impossível medi-la, estima-se que seja 500 vezes maior que a Surface Web e, por mais incrível que seja, ela continua crescendo. Em virtude de suas características ela ganhou uma fama negativa, porém o risco ao acessar a Deep Web depende estritamente do usuário e de suas intenções ao utilizá-la, obviamente que devido o fato de ser criptografada[28] e prezar pelo anonimato abre uma brecha para práticas ilícitas.

3.1.1 Surface Web

Como já supracitado a Surface Web refere-se aos sites que podem ser livremente acessados através da internet por meio dos instrumentos de procura que ela mesma viabiliza. Por meio dessa via são construídos históricos dos dados acessados pelos usuários automaticamente por intermédio de programas como o Web Crawlers[29], eles estabelecem uma listagem de

[28] Segundo Guimarães e Cabral "criptografia é um mecanismo de segurança e privacidade que torna determinada comunicação (textos, imagens, vídeos e etc) ininteligível para quem não tem acesso aos códigos de "tradução" da mensagem. Nas comunicações digitais, a criptografia auxilia na proteção de todos os conteúdos transmitidos entre duas ou mais fontes, evitando a intercepção por parte de cibercriminosos, *hackers* e espiões, por exemplo." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: <https://www.significados.com.br/criptografia/ >.Acesso em: 18 de fevereiro de 2017.

[29] Para Pozzebom "O processo que um Web crawler executa é chamado de Web crawling ou spidering. Muitos sites, em particular os motores de busca, usam crawlers para manter uma base de dados atualizada. Os Web crawlers são principalmente utilizados para criar uma cópia de todas as páginas visitadas para um pós-

sites conhecidos, como o Youtube[30] por exemplo, pegando cópias de cada website, os registrando, recolhendo informações de relevância que possam assegurar a segurança do site ou até uma recuperação. Assim, o aglomerado de endereços de páginas na web obtém o seu devido registro e o apanhado de todas elas formam a Surface Web, que atualmente engloba aproximadamente 15 bilhões de endereços eletrônicos. (DUARTE e MEALHA, 2016, Pág. 8)

3.2 Darknet

A Darknet consiste em uma rede de teias interligadas no qual o seu acesso é restringido a softwares especificamente desenvolvidos para tanto. Ela está dividida em duas espécies; a friend-to-friend e o Tor. Na Darknet estilo friend-to-friend é permitido aos usuários à comunicação entre pessoas que eles conhecem e também nesse ambiente existe a utilização de senhas e assinaturas digitais para fins de autenticação. Por outro lado, na Darknet estilo Tor o software preserva o anonimato resguardando os seus usuários. Em um apanhado geral os maiores usuários dos artifícios da darknet são: Whistleblowers[31], hackers[32], consumidores e vendedores de comércio ilegal, consumidores de pornografia ilícita e por fim o cidadão que resguarda pela sua privacidade (DUARTE e MEALHA, 2016, Pág. 9).

Tendo em vista os aspectos mencionados, observa-se que o acesso a Darknet só é possível através de softwares criados especificamente para tanto. O veículo de acesso Tor é insta-

---

processamento por um motor de busca que irá indexar as páginas baixadas para prover buscas mais rápidas. Crawlers também podem ser usados para tarefas de manutenção automatizadas em um Web site, como checar os links ou validar o código HTML. Os crawlers também podem ser usados para obter tipos específicos de informação das páginas da Web, como minerar endereços de email (mais comumente para spam).” POZZEBOM, Rafaela. Marketing Gidital. Oficina da Net. 2013. Disponível em: <https://www.oficinadanet.com.br/artigo/otimizacao__seo/qual-a-diferenca-entre-robo-spider-e-crawler>. Acesso em 26 de fevereiro de 2017.

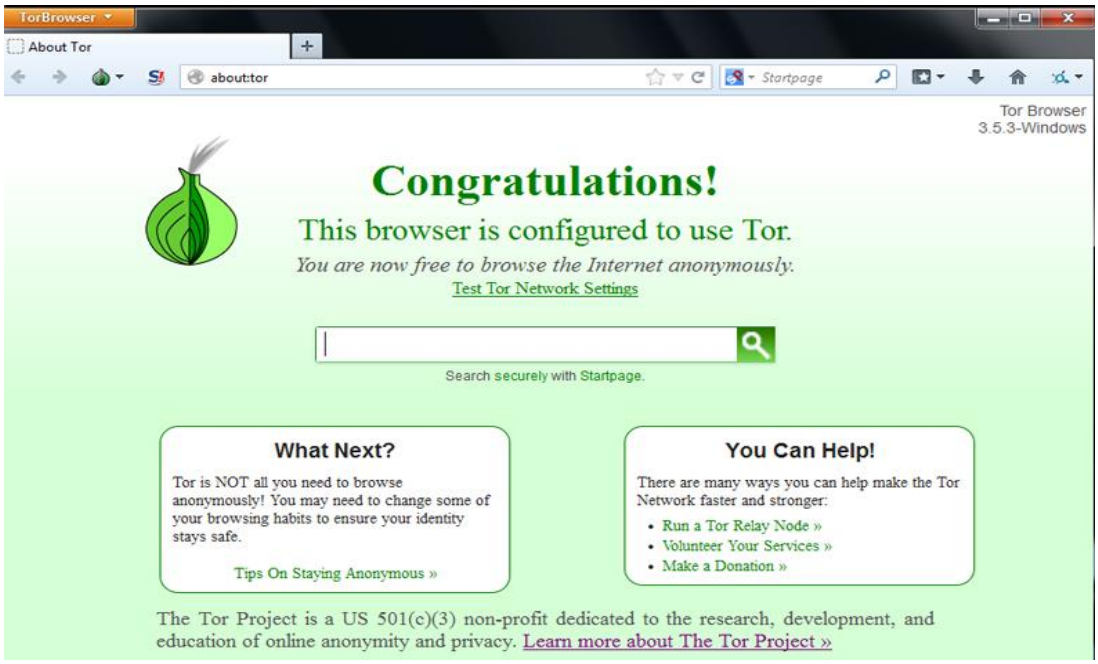
[30] Guimarães e Cabral entendem que “YouTube é um site de compartilhamento de vídeos enviados pelos usuários através da internet. O termo vem do Inglês “*you*” que significa “você” e “*tube*” que significa “tubo” ou “canal”, mas é usado na gíria para designar “televisão”. Portanto, o significado do termo “youtube” poderia ser “você transmite” ou “canal feito por você”. No YouTube, os vídeos estão disponíveis para qualquer pessoa que queira assistir. Também é possível adicionar comentários sobre o vídeo.” GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: < https://www.significados.com.br/youtube/>.Acesso em: 26 de fevereiro de 2017.

[31] Para Rocha “Em inglês, um *whistleblower* é alguém que alerta para a existência de irregularidades na gestão e no funcionamento de empresas ou instituições. Literalmente interpretável como «soprador de apito», *whistleblower* tem origens na gíria, mas acabou por adquirir o significado que tem atualmente por extensão metafórica. Não tem por enquanto em português um termo equivalente de uso estável. Com efeito, este anglicismo pode realmente ser traduzido por denunciante **ou** informador e por outras palavras sinónimas como denunciador**,** delator**,** alcaguete **ou** caguete (Brasil).” ROCHA, Carlos. CiberDúvidas. 2013. Disponível em: <https://ciberduvidas.iscte-iul.pt/consultorio/perguntas/whistleblower-ou-seja-autor-de-uma-denuncia/32088 >. Acesso em: 26 de fevereiro de 2017.

[32] Em consonância com Guimarães e Cabral “*Hacker* é uma palavra em inglês do âmbito da informática que indica uma pessoa que possui interesse e um bom conhecimento nessa área, sendo capaz de fazer *hack* (uma modificação) em algum sistema informático.” GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: <https://www.significados.com.br/hacker/>.Acesso em: 26 de fevereiro de 2017.

lado por meio do seu browser ou por intermédio de algum proxy que realiza a mesma função. Ainda convém lembrar que o Tor é o mais usado, porém existem outros softwares que são pouco utilizados, mas desempenham as mesmas funções.

Figura 4 – Tor Browser



Fonte: < https://www.torproject.org/projects/torbrowser.html.en> - Acesso em: 29 de mar de 2017

3.3 Dark Web

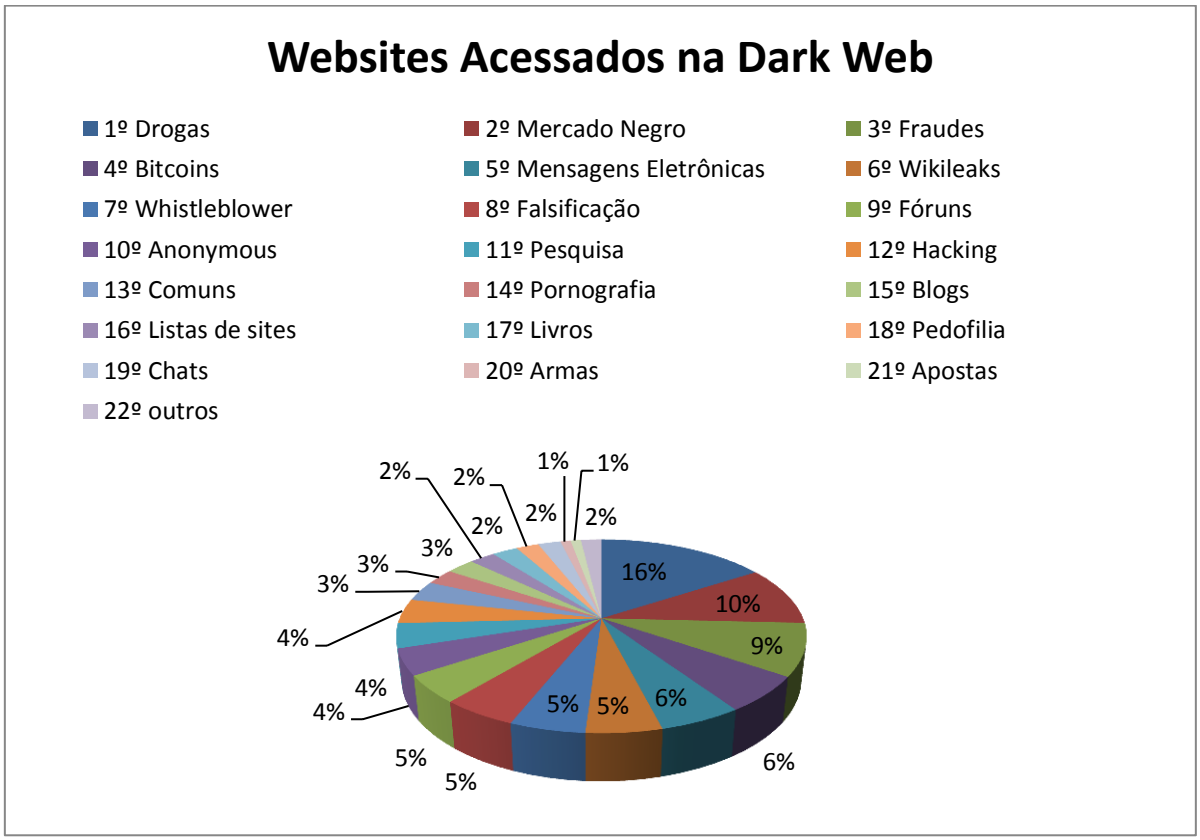
A Dark Web é praticamente a junção da Deep Web e a Darknet. A Deep Web é composta por vários sites não registrados cujo acesso e consultas são viabilizados através da Darknet por meio de softwares como o Tor, formando assim a Dark Web. Estima-se que os conteúdos mais visualizados na Dark Web são os da pornografia infantil, os tráficos de órgãos e mercados negros. Ao mesmo tempo o nível de visualizações também é crescente nas páginas que divulgam documentos sigilosos do Governo como o WikiLeaks[33], os Bitcoins[34] e

[33] "A *WikiLeaks* é uma organização transnacional sem fins lucrativos, com sede na Suécia, que, por meio de seu *site*, busca divulgar informações e documentos de cunho confidencial sobre questões de interesse geral. UOL Apoio Escolar." Disponível em: < http://clickeaprenda.uol.com.br/portal/mostrarConteudo.php?idPagina=23889 >. Acesso em 1 de março de 2017.

[34] Para Guimarães e Cabral "Bitcoin (também conhecida pela sigla BTC), é uma moeda virtual (ou digital) criada por Satoshi Nakamoto em 2009. Significa moeda bit (sendo que coin é moeda em inglês, e bit corresponde ao dígito binário, termo que expressa menor unidade de informação no contexto informático). A Bitcoin não é apenas uma moeda é também um protocolo e um software que possibilita transações peer-to-peer instantâneas (não envolve intermediários) e pagamentos em termos mundiais. A Bitcoin também apresenta taxas de processamento baixas ou nulas." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: < https://www.significados.com.br/bitcoin/ >.Acesso em: 1 de março de 2017.

tutoriais de fraude cibernética. Portanto, no gráfico abaixo se observa a percentagem das páginas mais acessadas na Dark Web divididas em grupos (DUARTE e MEALHA, 2016, Pág. 11):

Figura 5 – Gráfico dos Web sites mais acessados da Dark Web

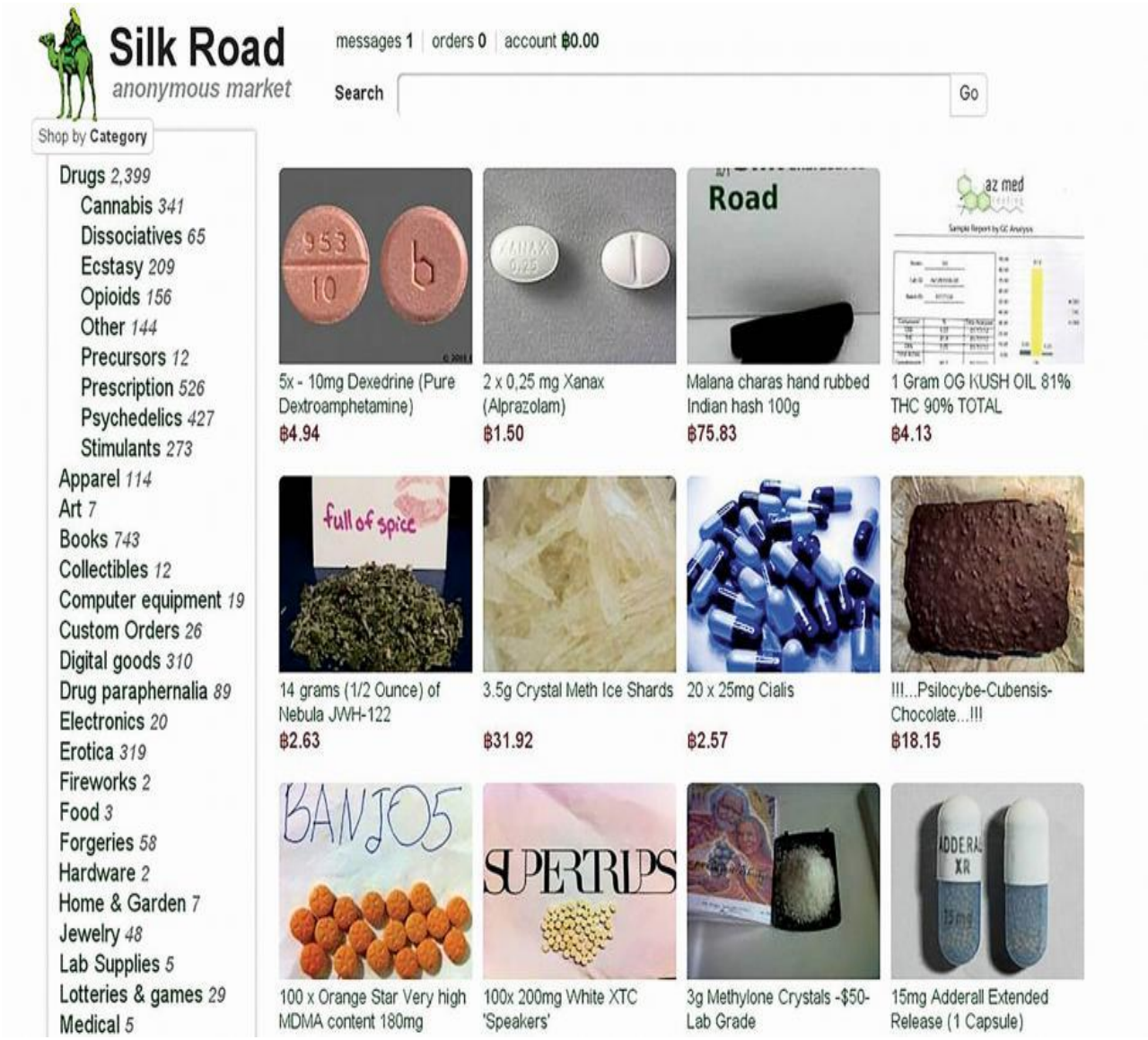


Fonte: Elaborada pela própria autora.

Pode-se afirmar que 26% da Dark Web é composta por websites de Drogas e do Mercado Negro. As Drogas são categorizadas nos sites com catálogos de preços para que os usuários possam fazer os seus pedidos, funciona basicamente como uma página de compra e venda similar as existentes na Surface Web, assim como demonstrado na imagem em seguida, que trata do site de Drogas mais conhecido na Dark Web, o Silk Road[35] Anonymous Market:

[35] Para a Bitcoinbrasil "Silk Road significa Rota da Seda. O maior mercado anônimo de compra e venda de drogas da internet. [...] Operando desde o começo de 2011, o website, acessível somente através de softwares anonimizantes como o Tor, se tornou praticamente sinônimo das ilegalidades praticadas na chamada internet profunda – e, na parte que nos toca, inegavelmente era um dos grandes destinos de bitcoins, única moeda que era aceita nas transações. [...] O Silk Road era conhecido por contar com uma garantia quase inquebrável da proteção à privacidade de vendedores e compradores, e de fato foi assim durante parte da sua existência. Bitcoin Brasil. O fim do silk Road e o impacto no Bitcoin. 2013." Disponível em: < https://www.bitcoinbrasil.com.br/o-fim-do-silk-road-e-o-impacto-no-bitcoin/ >. Acesso em: 1 de março de 2017.

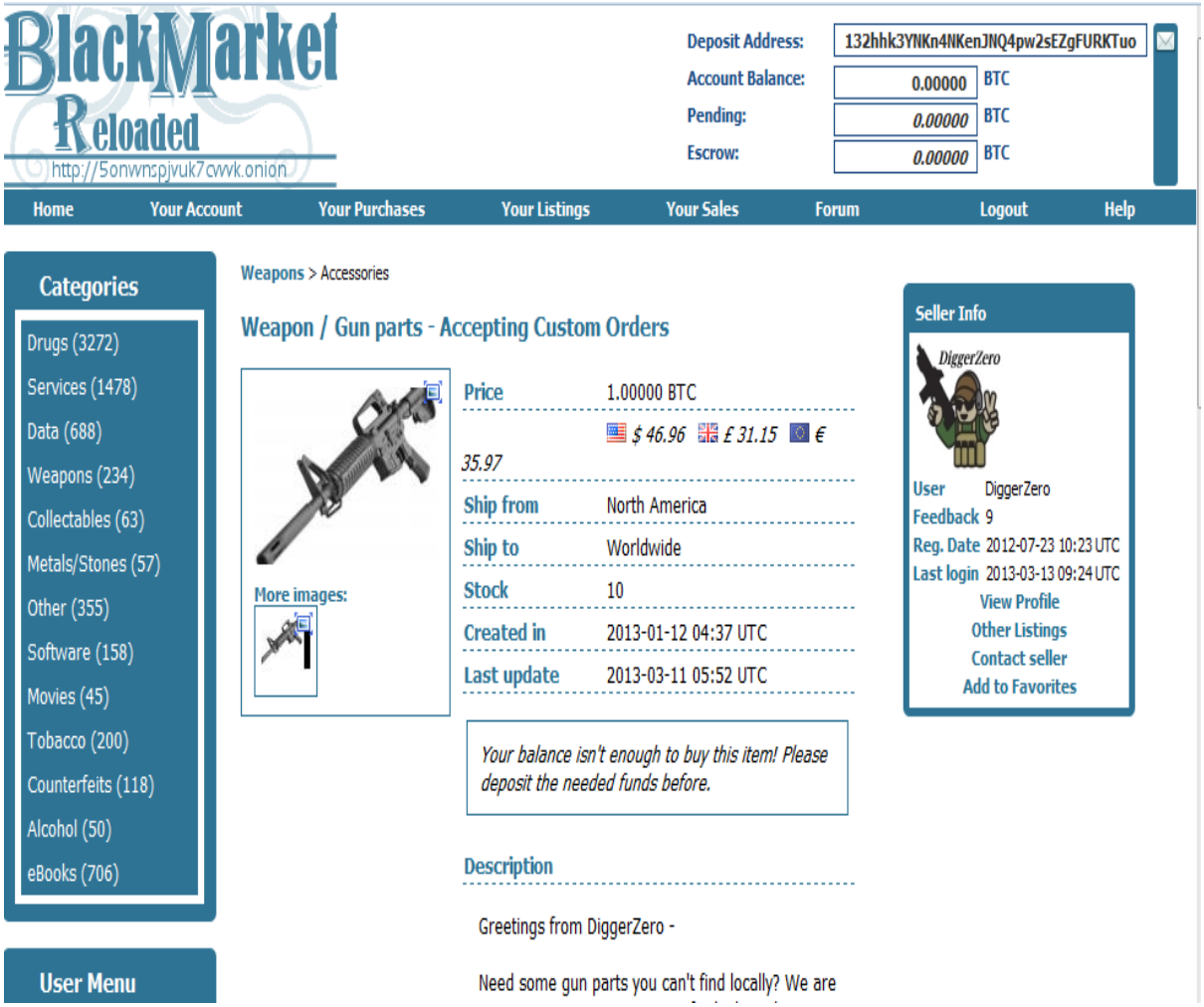
Figura 6 – Página referente a Dark Web do Silk Road Anonymous Market.



Fonte: Dark Web. Disponível em: <https://silkroaddrugs.org/silk-road-2-0-url/ > acesso em: 31 de março de 2017.

Quanto ao Mercado Negro, a compra e venda possui grande variedade, desde órgãos humanos, a tabaco ou armas, todos catalogados com preços e informações sobre os mesmos. A página do Black Market Reloaded é um exemplo de como se executa o funcionamento desse mercado na Dark Web como demonstra a imagem:

Figura 7 – Mercado Negro, Black Market Reloaded sítio da Dark Web



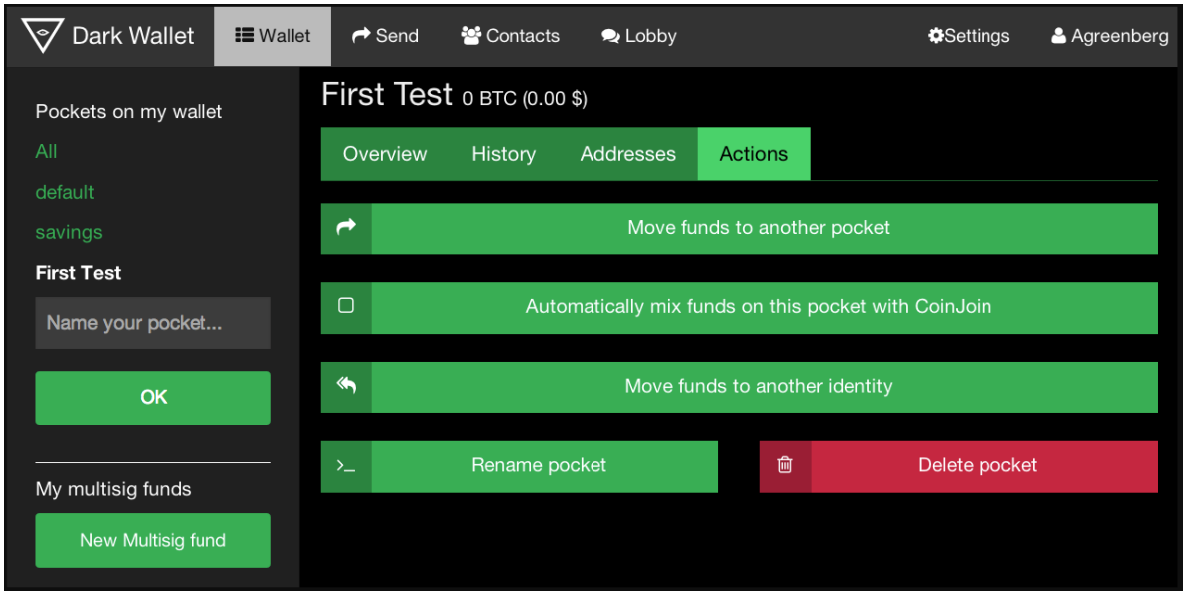
Fonte: Dark Web. Disponível em: < http://kernelmag.dailydot.com/features/report/5733/the-fall-of-an-online-gun-dealer/ > Acesso em: 31 de marco de 2017.

3.4 Bitcoins

A Dark Wallet[36] é uma espécie de carteira virtual onde são computados os Bitcoins para realizarem transações na Dark Web. É o espaço onde o usuário pode preservar os fundos, transferir ou investir no mercado:

[36] Carteira, Bolsa.

Figura 8 – Dark Wallet



Fonte: < https://darkwallet.is/> Acesso em: 31 de março de 2017.

> "Inventada e partilhada em 2009 pelo japonês Satoshi Nakamoto, a Bitcoin é uma moeda encriptada que todas as pessoas podem adquirir em troca de dinheiro, produtos ou serviços. O número de pessoas a utilizar este método tem vindo a crescer largamente e uma das razões para tal é o facto das taxas de pagamento serem de 2 a 3 % mais baratas do que o pagamento por cartão de crédito. Ao contrário do método tradicional, as taxas são suportadas pelo comprador, e não pelo vendedor." (DUARTE e MEALHA, 2016, Pág. 12).

Em face a essa realidade, algumas organizações têm demonstrado interesse sobre os Bitcoins e estão aderindo a esta forma de carteira digital.

Figura 9 – Plataforma de Compra e Venda de Bitcoins

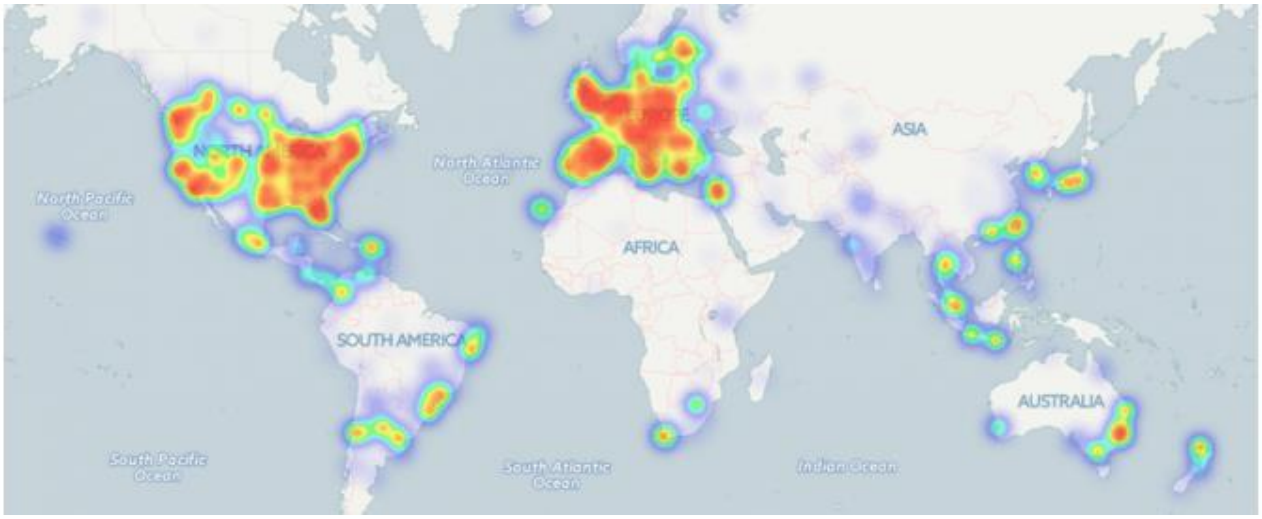
Fonte: Arena Bitcoins. Disponível em: <http://s.newsweek.com/sites/www.newsweek.com/files/styles/embedded_full/public/2015/02/16/0220silkroad09.jpg?itok=9jh1k1sF> Acesso em: 30 de março de 2017.

Elas deram início a essa prática aceitando donativos em Bitcoin(BTC). No Brasil, o número de lojas que aceitam pagamento com Bitcoins já passa de quinze mil, o RexBit mostra em seu site vários mapas nacionais e internacionais traçando lojas e organizações adeptas a essas transações conforme as imagens a seguir:

Figura 10 – Plataforma de Compra e Venda de Bitcoins

Fonte: REXBIT. Disponível em: < https://www.bitcoinnews.com.br/tag/rexbit/ >. Acesso em 31 de março de 2017.

Figura 11 – Mapa Internacional de Bitcoins, lojas e organizações que aceitam a moeda



Fonte: REXBIT. Disponível em: < https://www.bitcoinnews.com.br/tag/rexbit/ >. Acesso em 31 de março de 2017.

Outro fator existente é que devido a crescente demanda pelo Bitcoins, já existem sites brasileiros com gráficos e conversores on-line, convertendo o Real para Bitcoins e disponibi-

lizando suas estatísticas também em tempo real do valor deles no mercado como mostram as imagens:

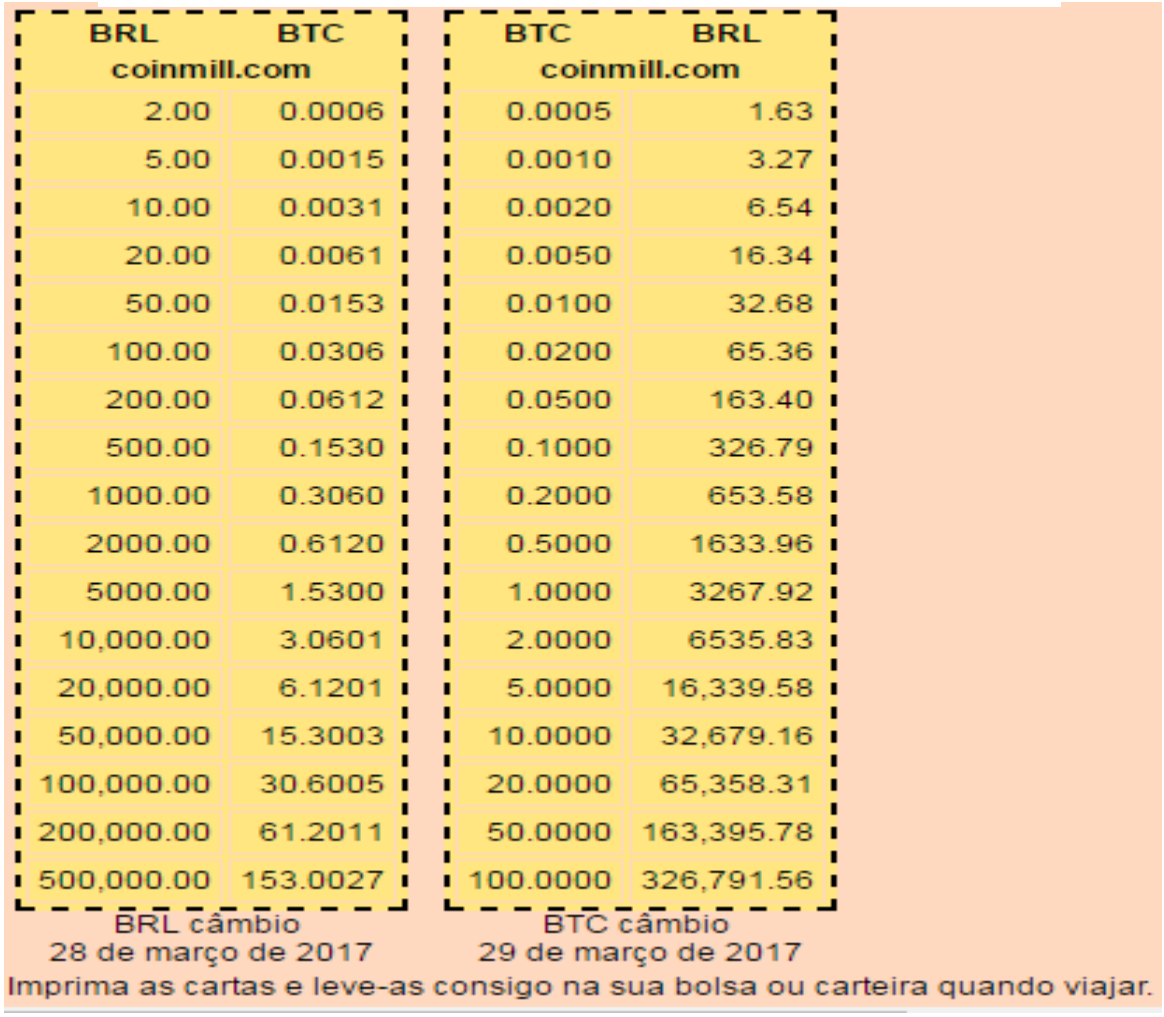
Figura 12 – Conversor de Bitcoins para o Real

Fonte: Arena Bitcoins Disponível em: <http://s.newsweek.com/sites/www.newsweek.com/files/styles/embedded_full/public/2015/02/16/0220silkroad09.jpg?itok=9jh1k1sF>_Acesso em: 30 de março de 2017.

Figura 13 – Gráfico de Bitcoins registrado de acordo com as horas, início do dia 23/03/2017 às 11h ao dia 29/03/2017 às 19h

Fonte: Arena Bitcoins Disponível em: <http://s.newsweek.com/sites/www.newsweek.com/files/styles/embedded_full/public/2015/02/16/0220silkroad09.jpg?itok=9jh1k1sF> Acesso em: 30 de março de 2017.

Figura 14 – Gráfico Cambial entre o real brasileiro e o BTC



BRL	BTC
coinmill.com	
2.00	0.0006
5.00	0.0015
10.00	0.0031
20.00	0.0061
50.00	0.0153
100.00	0.0306
200.00	0.0612
500.00	0.1530
1000.00	0.3060
2000.00	0.6120
5000.00	1.5300
10,000.00	3.0601
20,000.00	6.1201
50,000.00	15.3003
100,000.00	30.6005
200,000.00	61.2011
500,000.00	153.0027

BRL câmbio
28 de março de 2017

BTC	BRL
coinmill.com	
0.0005	1.63
0.0010	3.27
0.0020	6.54
0.0050	16.34
0.0100	32.68
0.0200	65.36
0.0500	163.40
0.1000	326.79
0.2000	653.58
0.5000	1633.96
1.0000	3267.92
2.0000	6535.83
5.0000	16,339.58
10.0000	32,679.16
20.0000	65,358.31
50.0000	163,395.78
100.0000	326,791.56

BTC câmbio
29 de março de 2017

Imprima as cartas e leve-as consigo na sua bolsa ou carteira quando viajar.

Fonte: Coinmill. < http://pt.coinmill.com/> Acesso em: 30 de março de 2017.

> "Bitcoins podem ser adquiridas diretamente a pessoas, através de máquinas multibanco ou em leilões. Não existe uma tabela fixa de conversão de Bitcoins mas estima-se que o seu valor é 7 vezes superior ao ouro e 18 vezes superior ao dólar americano. A definição de Bitcoin não é consensual, sendo que nalguns países, como a Rússia, o Vietname e o Equador, é proibida a sua circulação. Devido ao seu formato anónimo, a Bitcoin é a moeda utilizada para as transações efetuadas na Dark Web, nomeadamente na famosa plataforma de compra e venda de drogas, a Silk Road, bem como para aquisição de material ilegal como pornografia infantil, armas, assassinos, etc. Estes factos têm suscitado críticas à utilização desta moeda por parte do FBI." (DUARTE e MEALHA, 2016, Pág. 13).

O Bitcoin funciona como moeda digital que movimenta o mercado eletronicamente e é manuseado por meio de um algoritmo. Quando duas ou mais pessoas fecham uma transação econômica eletrônica as partes envolvidas assinam o negócio com um tipo de chave que é criptografada, no qual deve indicar as relações e ditames do acordo. Com isso, gera-se um registro virtual desse acordo que permanecerá registrado no histórico, como também será reportado a cada usuário envolvido no negócio em questão para assegurar a transação.

3.5 Internet no Brasil

Conforme a Internet foi se propagando foram surgindo novos aparelhos na informática como os notebooks, tablets, smartphones e entre outras inovações tecnológicas. Essas inovações digitais trouxeram inúmeros benefícios à sociedade, mas por outro lado, uma ampla quantidade de crimes passaram a serem executados no meio cibernético. Estes crimes usaram as novas ferramentas tecnológicas contra elas mesmas, invadindo os seus sistemas operacionais ou até mesmo arquivos privados. Em virtude disso, havia a necessidade de que se constituísse uma lei capaz de abarcar os crimes cibernéticos e seus derivados a fim de resguardar os direitos ora desprotegidos. (SILVA, Patrícia Santos, 2015, Pág. 13)

Dado o exposto, foi elaborada a Lei 12.737 especificamente para os crimes de natureza cibernética no país. Aprovada em 2012 é conhecida como "lei dos crimes cibernéticos" ou "lei Carolina Dieckmann". A referida lei passa a punir os indivíduos que invadem dispositivo cibernético alheio burlando os mecanismos de proteção para ter acesso aos dados sem consentimento do proprietário. Vale ressaltar que existem os crimes que podem ser cometidos por meio do auxílio da informática ou sem ajuda dela, exemplos disto são os crimes contra a honra. Os indivíduos que pecam por infrações como estas se utilizam das redes sociais ou do meio digital apenas como veículo para cometerem os delitos. Portanto, em acontecimentos como estes o bem jurídico tutelado não fica amparado pela lei de crimes cibernéticos, mas pelo próprio Código Penal brasileiro, segundo Patrícia Santos:

> "Importante destacar, que há também os crimes que são cometidos tanto pelo uso da informática como sem o auxílio desta, podendo citar como exemplos: a injúria, a calúnia, difamação, racismo, pedofilia e outros. Para os criminosos que atuam neste meio, a informática funciona nesses casos apenas como mais uma ferramenta por onde podem cometer tais crimes. Desta forma, nesses casos não se está lesando bem jurídico novo (advindo da própria informática), como a lei nova prevê, mas atinge-se bens jurídicos tradicionais do Código Penal. " (SILVA, Patrícia Santos,2015, Pág. 13).

Além disso, sabe-se que a proteção da sociedade é de extrema importância, ter um alicerce jurídico no âmbito digital se tornou uma necessidade, pois a internet passou a ser o veículo de comunicação mais utilizado pela população brasileira. Promover o desenvolvimento de pesquisas sobre os crimes cibernéticos, as proporções das condutas criminosas e a proteção dos indivíduos é dever do Estado e deve ser exercido apropriadamente.

3.6 Bem Jurídico

Os bens jurídicos no âmbito cibernético, dependendo do contexto em que estiverem, podem ser semelhantes ou iguais ao bem jurídico comum tutelado pelo Direito Penal, a diferença é que um está no ambiente real e o outro está no ambiente virtual. Bem jurídico se encaixa em tudo aquilo que é passível de ser objeto do Direito, correspondem a valores materiais e imateriais de social relevância. O Direito Penal vela e protege a sociedade, resguardando esses bens. (LIMA, 2011, Pág. 2).

Em razão da evolução que se deu quanto à informática os crimes executados através desse meio atingem os bens jurídicos já tutelados penalmente, como também os bens jurídicos que emergiram desse feito. Nesse sentido, Crespo discerne:

> "Ao considerarmos as condutas ilícitas por meio da informática, verificamos a possibilidade de lesão a outros bens jurídicos. Assim, pode-se falar em condutas dirigidas a atingir não só aqueles valores que já gozam de proteção jurídica, como a vida, a integridade física, o patrimônio, a fé pública, mas, também as informações armazenadas (dados), a segurança dos sistemas de redes informáticas ou de telecomunicações." (CRESPO, 2011, Pág. 56).

Ressalta-se ainda que a seara informática se renova a cada dia, pois vive um processo de desenvolvimento constante, criando sempre novos meios e objetos melhores que são bastante propícios a novos crimes, dessa forma essas ações podem ensejar em novos tipos de bens jurídicos passiveis de tutela do Estado.

3.7 Crimes Próprios

São considerados crimes cibernéticos próprios àqueles que necessariamente precisam da informática para serem executados, de forma que sem o meio digital seria impossível a sua realização. Segundo Patrícia Santos da Silva, a criminalidade digital compõe nova tipificação penal e atingem a informática de várias maneiras.

> "Existem muitas opções de ataques que podem ser realizados contra um computador. Dentre as muitas áreas vulneráveis, há aquelas em que a ação delitiva atua na unidade por onde entram os dados, na saída dos dados eletrônicos, na unidade centralizada onde são processados os dados, num dispositivo de armazenamento ou ainda na transmissão dos dados." (SILVA, Patrícia Santos, 2015, Pág. 42)

Portanto, pode-se concluir que por meio da ação de criminosos, via internet, que cometerem atos ilícitos gerando dano a algum bem jurídico tem-se o que se classifica de crime próprio dentro da seara digital. (CRESPO, 2011, Pág 57)

3.8 Crimes Impróprios

Os Crimes Impróprios diferem dos crimes supracitados porque segundo Castro (2003, Pág. 10) eles podem ser executados através ou não dos meios digitais. Nesse sentido, a internet aparece unicamente como facilitador do ilícito. A utilização da Web por si só não é unicamente uma nova forma de conteúdo para o Direito tutelar, mas ela pode ser manuseada também como instrumento, podendo ser usada por qualquer cidadão comum sem habilidade específica no ramo, como via para cometer atos ilícitos ferindo bens jurídicos fora do ambiente digital.

3.9 Sujeitos Do Crime

É necessário observar a interação do sujeito ativo e do sujeito passivo nos crimes cibernéticos para melhor compreender como se encaixa o posicionamento dos criminosos no ambiente virtual e quem são aqueles que sofrem os danos praticados por essas ilicitudes. (SILVA, Patrícia Santos, 2015, Pág. 47)

3.9.1 Sujeito Ativo

É classificado como sujeito ativo o indivíduo que direta ou indiretamente exercer alguma conduta relatada no tipo penal. Primeiramente, qualquer pessoa é passível de se tornar sujeito ativo nos crimes cibernéticos, pois para alguns atos ilícitos não é preciso grandes conhecimentos na seara digital, o estelionato, por exemplo, é uma prática corriqueira no ambienta virtual, os criminosos se utilizam da web para iludir suas vítimas e tirar proveito delas, cometendo assim uma fraude eletrônica (CASTRO, 2003, Pág. 11-12). Ainda assim, o indivíduo que é conhecedor das fragilidades da internet, dos sistemas operacionais dos equipamentos eletrônicos ou mesmo das falhas de rede e, se articula nesse ambiente para realizar atos ilícitos também é classificado como sujeito ativo (LIMA, 2011, Pág. 40). Embora Carla Rodrigues Araújo de Castro na sua doutrina considerar que qualquer indivíduo pode ser um criminoso vitualmente, Paulo Marco Ferreira Lima entende que mesmo com a possibilidade de qualquer um praticar atos ilícitos via web, ainda são aqueles com amplos conhecimentos sobre a informática que dominam a criminalidade virtual, como os Hackers, Crackers e Phreakers, por exemplo.

> "São os hackers, em regra, invasores dos sistemas eletrônicos que, por espírito de emulação, estariam desafiando seus próprios conhecimentos técnicos e a segurança

> de sistemas informatizados de grandes companhias e organizações governamentais. “ (LIMA, 2011, Pág 41).

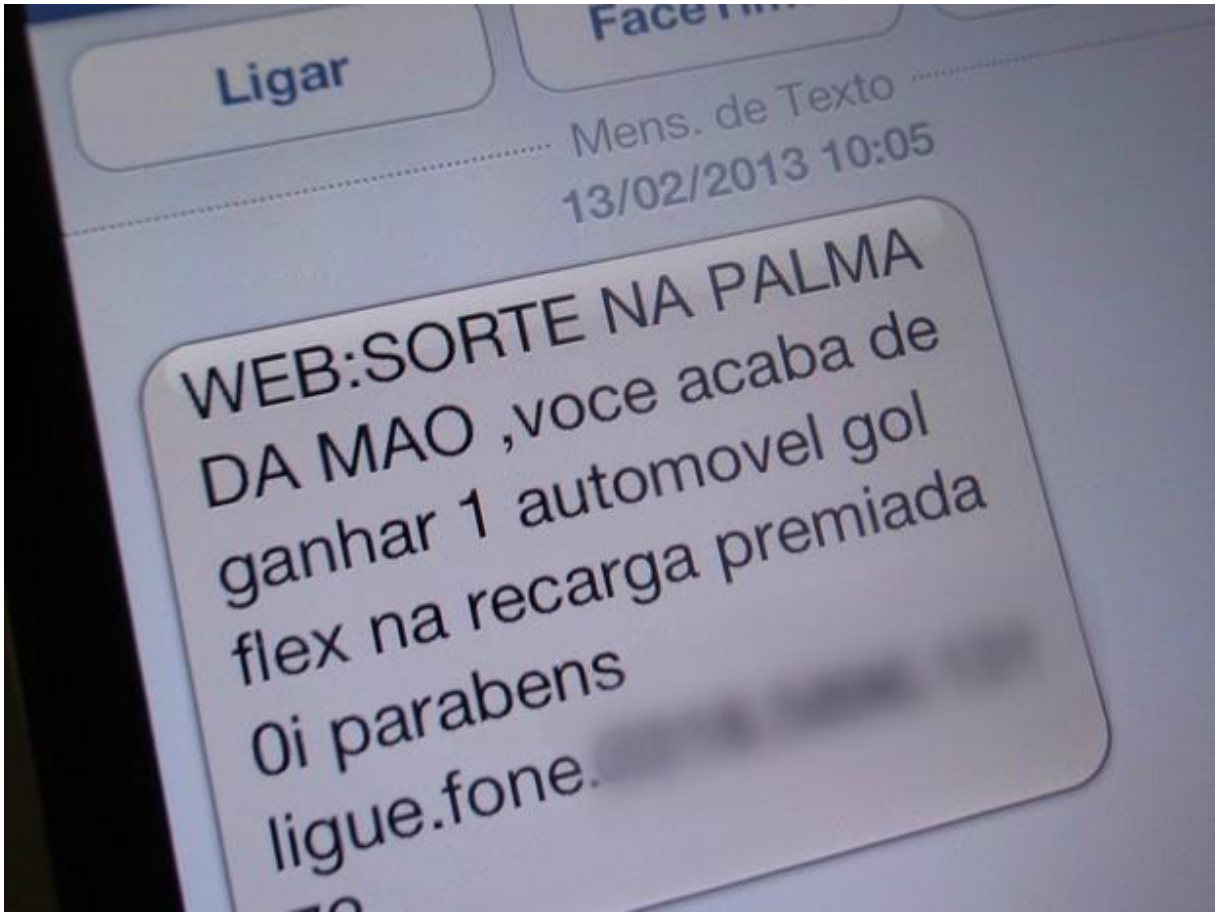
Os Hackers são indivíduos que muitas vezes se utilizam dos seus conhecimentos tecnológicos para realizarem invasões de redes ou sistemas de governo por meio de falhas ou brechas dos dispositivos visando sua autopromoção no ambiente virtual a fim de praticar atos criminosos ou até mesmo de chamar atenção de grandes corporações para suas habilidades como hacker. Conforme Marcelo Xavier de Freitas Crespo:

> “Hacker é o nome genérico dado aos chamados “piratas” de computador. Essa expressão surgiu nos laboratórios de computação do MIT (Massachusetts Institute of Technology), onde estudantes passavam noites em claro averiguando tudo o que se podia fazer com o computador. Apesar da fama de “criminosos virtuais”, nem todo hacker deseja o prejuízo alheio. Há aqueles que se dizem “hackers do bem”, pois invadem os computadores e deixam mensagens informando a vítima do risco existente, aconselhando-a a providenciar uma proteção mais efetiva. Outros passam a trabalhar em empresas a fim de desenvolver programas que sejam capazes de frear as invasões.” (CRESPO, 2011, Pág 95).

No entanto, os crackers estão voltados inteiramente para o crime, através dos seus conhecimentos cibernéticos eles invadem sistemas, derrubam páginas da web, quebram códigos de segurança, roubam senhas e informações sigilosas, enfim, por meio de atos ilícitos se utilizam da informática apenas para obter vantagens para si (CRESPO, 2011, Pág. 96).

Ainda convém lembrar os phreakers, que agem no ambiente telefônico burlando os sistemas de telecomunicação rastreando ligações, conversas registradas nos aparelhos por meio de aplicativos de redes sociais, clonagem de números utilizando a linha telefônica e inserindo débitos a conta da vítima, enviando torpedos fraudulentos com propostas de prêmios e fazendo ligações gratuitas driblando as empresas de telecomunicações (CRESPO, 2011, Pág. 97). Um exemplo comum são os “torpedos premiados”, uma prática de estelionatários que tem se difundido por todos o Brasil, como demonstra a imagem:

Figura 15 – Fraude Telefônica em torpedos via web



Fonte: <http://g1.globo.com/al/alagoas/noticia/2013/06/estelionatarios-continuam-com-golpe-da-mensagem-premiada-em-maceio.html> Acesso em : 2 de abril de 2017

3.9.2 Sujeito Passivo

O sujeito passivo é aquele que sofre a ação danosa praticada pelo sujeito ativo, no caso dos crimes cibernéticos são os indivíduos que tem os seus dispositivos ou sistemas eletrônicos invadidos, hackeados e tendo suas informações extraídas ou duplicadas, sendo de alguma forma lesionados por essas ações, sejam elas realizadas por meio da internet ou não (LIMA, 2011 Pág 36). O sujeito passivo conforme Carla Rodrigues Araújo de Castro poderá ser qualquer cidadão como também as grandes empresas e corporações. Uma pessoa que se conecta a internet está sujeita a qualquer tipo de ataque comum de hackers, crackers ou phreakers, porém os grandes alvos que ficam sujeitos a ataques mais elaborados são justamente as grandes corporações, por terem voluptuosas quantidades de dinheiro movimentando o mercado, acabam chamando a atenção desses criminosos. Vladimir Aras conceitua que:

> "Qualquer profissional que pretenda ser bem-sucedido, qualquer empresa ou empreendimento que busque o êxito, deverá estar na rede e cercar-se de conhecimentos e especialistas em diversos campos, a fim de que se tornem visíveis e alcançáveis os horizontes desse mar cibernético" (ARAS, 2001, Pág. 122)

Portanto, mesmo com a existência de cidadãos comuns navegando na web e utilizando equipamentos eletrônicos que facilitem a realização de cibercrimes por parte dos hackers, os indivíduos comuns são atingidos, mas ainda assim, eles não são os seus principais alvos. Os criminosos anseiam mais atingir as corporações, bancos e sistemas eletrônicos do governo com os seus golpes vislumbrando a maior quantidade de dinheiro e informações possível.

3.10 Os Cibercrimes No Estatuto Da Criança E Do Adolescente

O Estatuto da Criança e do Adolescente (Lei 8.069 de 13 de julho de 1990) falava unicamente em ser considerado como ato pornográfico infanto-juvenil a publicação e divulgação de cenas de sexo. Com o advento da Lei 11.829/08 que modificou o Estatuto da Criança e do Adolescente no que tange a pornografia infantil, os tipos penais dos artigos 240 e 241 passaram a considerar como violação a conduta de dispor a venda, armazenamento, disponibilização e transmissão midiática de cenas de sexo infant-juvenil. Desse modo os artigos modificados puderam abranger melhor essa forma perversa de comércio da pornografia infantil.

3.10.1 Artigo 241-A do ECA

Conforme as mudanças ocorridas no ECA pela Lei 11.829/08 o artigo 241-A passou a possuir a seguinte redação, in verbis:

> "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: (Incluído pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
> § 1o Nas mesmas penas incorre quem: (Incluído pela Lei nº 11.829, de 2008)
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; (Incluído pela Lei nº 11.829, de 2008)
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
> § 2o As condutas tipificadas nos incisos I e II do § 1o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste go." (Incluído pela Lei nº 11.829, de 2008). (LEI Nº 8.069, DE 13 DE JULHO DE 1990.).

Desta forma, o artigo trata como crime a distribuição de conteúdo sexual infantil em imagens ou vídeos por meio qualquer apetrecho midiático ou pela web, que também incorrerá em mesmo crime a pessoa ou empresa que garantir que seja armazenado esse tipo de conteúdo

em páginas na web permitindo o acesso de usuários. Entretanto, a responsabilidade pelo crime só recairá sobre os provedores da web se depois de notificados oficialmente por representante legal não seja cancelado o acesso ao conteúdo sexual infantil, obviamente que o mesmo se aplica em caso de decisão judicial. Ressalta-se ainda que o fato de apenas existir imagem ou vídeo de cunho pornográfico infantil independentemente do acesso dos usuários também é caracterizado como crime. O crime que refere-se a pornografia infantil também se consuma no local e no momento em que o administrador da página da web torna público o acesso a quem surfa na Surface Web, ou seja, no endereço da pessoa que fez a publicação do conteúdo. No tocante a troca de arquivos, segundo o próprio caput do artigo, refere-se ainda a transmissão, disponibilização em mesma rede, compartilhamento, download, cópia, via e-mail e entre outros, tudo isso proporciona a distribuição do material ilícito. Conforme entende o TRF-2ª Região, observa-se:

> "DIREITO PROCESSUAL PENAL. HABEAS CORPUS. IMAGENS E VÍDEOS. PORNOGRAFIA. CRIANÇAS E ADOLESCENTES.MATERIALIDADE COMPROVADA. ORDEM DENEGADA.
> 1. É cediço que, em razão do princípio da presunção de inocência, qualquer medida de constrição de liberdade antes do trânsito em julgado somente deve ser adotada se patente sua necessidade, mormente em razão da presença dos elementos do artigo 312[37] do Código de Processo Penal. No caso em tela, dúvidas não há que restou demonstrada de modo eficaz pelo Juízo a quo a presença destes elementos.
> 2. Restou demonstrado que o acusado mantinha, em seu computador, imagens e vídeos de crianças e adolescentes em cenas de sexo explícito e pornográficas, razão pela qual estaria incurso nas penas dos arts. 241-A e 241-B da Lei nº 8.069/90. Há indícios de que os vídeos eram compartilhados na rede mundial de computadores, havendo provas de que a prática delitiva se desenvolveu de forma continuada ao longo de um largo intervalo de tempo. Materialidade comprovada.
> 3. [...].
> 4. Ordem denegada. " (TRF2 - HC 201102010006429 RJ 2011.02.01.000642-9. Relator: Juiz Federal Convocado ALUISIO GONCALVES DE CASTRO MENDES. Julgamento: 23/02/2011. Órgão: PRIMEIRA TURMA ESPECIALIZADA.)

Portanto, é indispensável que exista na denúncia a probabilidade do material ilícito estar disponível na web ou no próprio computador gravado.

---

[37] "Art. 312. Considera-se proposta a ação quando a petição inicial for protocolada, todavia, a propositura da ação só produz quanto ao réu os efeitos mencionados no art. 240 depois que for validamente citado.
Art. 240. A citação válida, ainda quando ordenada por juízo incompetente, induz litispendência, torna litigiosa a coisa e constitui em mora o devedor, ressalvado o disposto nos arts. 397 e 398 da Lei no 10.406, de 10 de janeiro de 2002 (Código Civil).
§ 1º A interrupção da prescrição, operada pelo despacho que ordena a citação, ainda que proferido por juízo incompetente, retroagirá à data de propositura da ação.
§ 2º Incumbe ao autor adotar, no prazo de 10 (dez) dias, as providências necessárias para viabilizar a citação, sob pena de não se aplicar o disposto no § 1º.
§ 3º A parte não será prejudicada pela demora imputável exclusivamente ao serviço judiciário.
§ 4º O efeito retroativo a que se refere o § 1º aplica-se à decadência e aos demais prazos extintivos previstos em lei." BRASIL, **Código Civil**, Lei 10.406, de 10 de janeiro de 2002. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm >. Acesso em: 11 de março de 2017.

3.10.2 Artigo 241-B do ECA

Conforme as mudanças ocorridas no ECA pela Lei 11.829/08 o artigo 241-B passou a possuir a seguinte redação, in verbis:

> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
> § 1o A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
> § 2o Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por: (Incluído pela Lei nº 11.829, de 2008)
> I – agente público no exercício de suas funções; (Incluído pela Lei nº 11.829, de 2008)
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo; (Incluído pela Lei nº 11.829, de 2008)
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário. (Incluído pela Lei nº 11.829, de 2008)
> § 3o As pessoas referidas no § 2o deste artigo deverão manter sob sigilo o material ilícito referido. (Incluído pela Lei nº 11.829, de 2008). (LEI Nº 8.069, DE 13 DE JULHO DE 1990.).

O texto do referido artigo retrata que se enquadra como crime, se provado pericialmente, que o indivíduo investigado baixava o material, mas não compartilhava ou deixava disponível a outrem. Dado o exposto, refere-se à ilicitude o ato de comprar, guardar, manter conteúdo pornográfico infantil em seu computador ou em dispositivos de mídia removível como Pen-drives, HDs e DVDs. No caso de plataformas virtuais como o iCloud[38], Google Drive[39] ou Dropbox[40] que armazenam arquivos e forem utilizados para guardar pornografia

[38] Para Barros "O iCloud é o sistema de armazenamento na nuvem da Apple que atua de maneira bastante sofisticada. O serviço funciona no iPhone, iPad e iPod Touch e é bastante simples de ser configurado. O conceito-base do iCloud é o armazenamento de arquivos em uma "nuvem", um servidor online de grande capacidade. Com isso, você não precisa mais do disco rígido do seu aparelho para guardar seus dados. O serviço de nuvem possibilita uma economia de espaço no seu computador ou dispositivo móvel, e permite que seus arquivos sejam acessados por meio de qualquer produto Apple conectado à Internet." BARROS, Thiago. Revista eletrônica Techmundo. 2014. Disponível em: <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2011/06/como-funciona-o-icloud.html >. Acesso em: 5 de março de 2017.

[39] Conforme Pias "O Google Drive é o novo serviço de disco virtual que o Google lançou ontem (24/04), oferecendo 5 GB de espaço gratuito para seus usuários. O serviço permite o armazenamento de arquivos na nuvem do Google e possui aplicativos para sincronização para Windows, Mac e Android. Os arquivos armazenados no Google Drive, podem ser compartilhados com seus amigos e colaboradores através da conta do Google. Você poderá decidir com quem irá compartilhar cada arquivo além de decidir o nível de permissão de cada pessoa, escolhendo quem apenas poderá visualizar, editar ou comentar nos seus arquivos." PIAS, Pedra. Revista eletrônica Techtudo. 2012. Disponível em: http://www.techtudo.com.br/artigos/noticia/2012/04/o-que-e-google-drive-e-como-usar.html. Acesso em: 16 de março de 2017.

infantil a competência só pertencerá a Justiça Estadual se o provedor contiver servidor no Brasil, caso não contenha, a competência será da Justiça Federal. Com relação à posse o Ministério Público Federal no Roteiro de Atuação Crimes Cibernético concerne:

> "Os crimes, cujo núcleo seja "possuir", são permanentes. Os doutrinadores dizem não ser possível a tentativa em crimes permanentes, pois o começo da execução (a posse) exauriria a modalidade criminosa. Em outras palavras, não haveria "execução" do crime antes da efetiva posse do objeto material. A tentativa de aquisição de imagens de abuso de crianças (por exemplo, tentar fazer o download e haver um bloqueio pelo provedor) seria apenas ato preparatório aos crimes tipificados no ECA. E, por isso, na modalidade "possuir", não haveria o requisito da transnacionalidade, uma vez que não há início de execução (do crime de posse!) fora do País. Aliás, a maioria do entorpecente consumido no País vem do exterior, de modo que, por analogia, entendimento contrário levaria a se sustentar que todos os casos de posse de entorpecente seriam de competência da JF.
> No entanto, se o agente guarda o material pornográfico de modo que permite seu compartilhamento via internet, irrestritamente, com outras pessoas, disponibilizando esse material em sua página nas redes sociais, por exemplo, não se trata de mera posse, mas de ato que equivale à publicação da pornografia, o que constitui o crime do art. 241-A, do ECA.
> É importante fazer uma perícia bem feita para ver se o agente também não cometeu algum ato concreto de abuso sexual. É oportuno ressaltar que se o material pornográfico infantil que o agente possui envolve ele próprio, isso constitui prova do crime de estupro de vulnerável, que deve levar à responsabilidade do autor na forma da lei." (Roteiro de atuação: crimes cibernéticos / 2. Câmara de coordenação erevisão. – 3.ed. rev. e ampl. – Brasília: MPF, 2016. Pág; 288).

Existe diferença quanto àquele que adquire e aquele que possui o conteúdo ilícito, Alexandre Assunção e Silva concerne sobre o assunto da seguinte maneira:

> "No caso do art. 241-B do ECA, na modalidade adquirir, o tipo penal protege indiretamente a incolumidade sexual coletiva de crianças e adolescentes, pois quem adquire pornografia infantil real estimula diretamente a prática dos crimes de produzir, vender e divulgar tal material (que produzem lesão direta a bens jurídicos relevantes)." (SILVA, 2009, Pág. 453).

Observa-se que o mesmo se aplica ao crime de receptação[41] do Código Penal. O indivíduo que compra ou recebe coisa proveniente de furto ou roubo estimula a prática do crime, todos aqueles que têm o domínio de qualquer página na web possuem o conhecimento de quantos acessos ela recebe, portanto, os usuários que navegam em páginas de pornografia

---

[40] Em conformidade com Dâmaso "O Dropbox é um serviço de armazenamento em nuvem muito popular entre os usuários que oferece diversos recursos online, muitos deles ainda desconhecidos pela maioria. O Dropbox oferece uma versão gratuita com acesso a 2 GB de espaço inicialmente. Mas é possível aumentar a capacidade de armazenamento do serviço." DÂMASO, Lívia. Revista eletrônica Techtudo. 2014. Disponível em: <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2014/01/dez-dicas-interessantes-mostram-o-que-o-dropbox-e-capaz-de-fazer-veja.html >. Acesso em: 16 de março de 2017.

[41] **"**Receptação. Art. 180 - Adquirir, receber, transportar, conduzir ou ocultar, em proveito próprio ou alheio, coisa que sabe ser produto de crime, ou influir para que terceiro, de boa-fé, a adquira, receba ou oculte: (Redação dada pela Lei nº 9.426, de 1996). Pena - reclusão, de um a quatro anos, e multa. (Redação dada pela Lei nº 9.426, de 1996)." BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm >. Acesso em: 20 de março de 2017.

infantil e copiam as imagens se tornam possuidores do conteúdo e acabam estimulando os sites para que se mantenham ativos e prosperem.

3.10.3 Artigo 241-C do ECA

Conforme as mudanças ocorridas no ECA pela Lei 11.829/08 o artigo 241-C passou a possuir a seguinte redação, in verbis:

> " Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: (Incluído pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
> Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)." (LEI Nº 8.069, DE 13 DE JULHO DE 1990.).

Dado o exposto, o artigo estabelece como crime a edição ou montagem de fotos e vídeos que simulem a participação de crianças ou adolescentes em cenas pornográficas, mesmo que a montagem seja de péssima qualidade e seja visivelmente perceptível a sua falsificação. Outro fator importante é que também concorre pelo mesmo ato ilícito o agente que disponibiliza, vende ou guarda esse tipo de conteúdo sexual infantil, o artigo vela pela integridade das vítimas.

3.10.4 Artigo 241-D do ECA

Conforme as mudanças ocorridas no ECA pela Lei 11.829/08 o artigo 241-D passou a possuir a seguinte redação, in verbis:

> " Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: (Incluído pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
> Parágrafo único. Nas mesmas penas incorre quem: (Incluído pela Lei nº 11.829, de 2008)
> I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso; (Incluído pela Lei nº 11.829, de 2008)
> II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita. (Incluído pela Lei nº 11.829, de 2008)" (LEI Nº 8.069, DE 13 DE JULHO DE 1990.).

O legislador nesse artigo delimitou a criança como vítima a fim de excluir os adolescentes em virtude dos namoros que acontecem virtualmente pela web. Dado o exposto, é crime o agente que estimula a criança a participar de atos libidinosos, que a faz assistir a pornografia, incita a criar interesse sexual ou a constrange para que se exiba pornograficamente. Geralmente esse tipo penal ocorre em redes sociais como o Facebook[42] por exemplo, o criminoso se apresenta a vítima com uma imagem falsa simulando possuir a mesma idade e os mesmos interesses para obter a sua confiança e praticar atos libidinosos via webcam ou se encontrando pessoalmente com a vítima. (Roteiro de atuação: crimes cibernéticos / 2. Câmara de coordenação erevisão. – 3.ed. rev. e ampl. – Brasília: MPF, 2016. Pág; 293).

3.11 Cyberbullying

O bullying é a conduta repetitiva de violências físicas ou verbais de um indivíduo ou um grupo de pessoas a uma vítima singular que geralmente não tem possibilidade de defesa, portanto o cyberbullying é a inserção desse tipo de agressão no ambiente virtual. Na internet essa violência emerge através da intimidação, exclusão social, formação de memes[43] com o intuito de escarnecer da vítima e popularizar a sua humilhação, esta agressão causa danos físicos e psicológicos a vítima. Os danos causados pelo cyberbullying são de difícil reparação, pois muitas vezes com a veiculação de memes com esse tipo de humilhação na internet levam anos para serem apagados ou esquecidos já que podem ter sido gravados em qualquer dispositivo eletrônico que tenha se conectado na web ou em apetrechos de mídias removíveis, prosperando o dano as vítimas. O cyberbullying atinge tanto aos jovens e crianças quanto aos adultos, todos estão sujeitos a essa agressão. Até o presente momento não existe uma tipificação penal para o cyberbullying, por isso, a depender de como ocorreu a agressão e de como obteve respaldo na sociedade as atitudes do bullying virtual serão enquadradas nos crimes de

[42] Em consonância com Guimarães e Cabral "Facebook pode ser traduzido literalmente como "livro de caras", onde "*face*" é cara (ou caras) e "*book*" é livro. Facebook é a rede social mais popular no Brasil, tendo sido criada em 2004. Seus fundadores, Mark Zuckerberg, Eduardo Saverin, Andrew McCollum, Dustin Moskovitz e Chris Hughes, tiveram a ideia de uma nova rede social e a elaboraram ainda quando eram estudantes, na Universidade de Harvard, em Massachussets, nos Estados Unidos." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: < https://www.significadosbr.com.br/facebook >.Acesso em: 20 de fevereiro de 2017.

[43] Para Guimarães e Cabral "Meme é um termo grego que significa imitação. O termo é bastante conhecido e utilizado no "mundo da internet", referindo-se ao fenômeno de "viralização" de uma informação, ou seja,qualquer vídeo, imagem, frase, ideia, música e etc, que se espalhe entre vários usuários rapidamente, alcançando muita popularidade." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: <https://www.significados.com.br/meme/ >.Acesso em: 10 de fevereiro de 2017.

ameaça[44] ou nos crimes contra a honra que são a Injúria[45], Calúnia[46] e Difamação[47]. (Roteiro de atuação: crimes cibernéticos / 2. Câmara de coordenação erevisão. – 3.ed. rev. e ampl. – Brasília: MPF, 2016. Pág; 306-309).

Quando a prática do cyberbullying for proveniente de uma criança ou de um adolescente se caracteriza como ato infracional, ficando sujeito à medida socioeducativa se o autor for adolescente e caso o mesmo seja uma criança ficará sujeito à medida protetiva, sendo competência da Justiça Estadual, Vara da Infância e Juventude. Por outro lado, se o autor da humilhação é desconhecido ou anônimo e a vítima se tratar de criança ou adolescente será competência da Justiça Federal. Segundo o artigo 21 do Marco Civil da Internet, se em virtude de cyberbullying forem veiculadas na internet imagens vexatórias de cunho sexual, independente de ordem judicial a própria vítima poderá informar aos provedores de serviço da Internet para que sejam retiradas as imagens.

3.12 Fraude Bancária

Ao analisar a fraude bancária via internet nota-se que esse feitio não é de fácil execução, burlar a segurança digital de instituições bancárias ou comerciais para hackear dados do sistema requer muita habilidade por parte dos criminosos. Em virtude disso, os criminosos concentram os seus esforços para sondar possíveis fragilidades do sistema ou dos usuários. Portanto, para conseguir efetuar o crime, a retórica e a eloquência são usadas para persuadir e convencer as vítimas a caírem nesse tipo de golpe, induzindo-as a fornecerem informações essenciais ou realizarem ações que facilitem o ato ilícito. Em consequência disso, quando o golpista finalmente possui os dados necessários da vítima ele passa a realizar atos ilícitos em nome dela como: criar contas em bancos, abrir empresas, acessar páginas, comprar bens, realizar transações bancárias e entre outros, por isso a maioria dessas fraudes virtuais são consideradas crimes contra o patrimônio, estelionato ou furto qualificado. (Roteiro de atuação:

[44] " Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave: Pena - detenção, de um a seis meses, ou multa. Parágrafo único - Somente se procede mediante representação." BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm >. Acesso em: 20 de março de 2017.

[45] "Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa." BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm >. Acesso em: 20 de março de 2017.

[46] "Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa." BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm >. Acesso em: 20 de março de 2017.

[47] "Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa." BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm >. Acesso em: 20 de março de 2017.

crimes cibernéticos / 2. Câmara de coordenação erevisão. – 3.ed. rev. e ampl. – Brasília: MPF, 2016. Pág; 296). A Ministra Laurita Vaz esclarece no CC 67.343-GO com o seguinte entendimento, concerne à ementa:

> "CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSO PENAL. FRAUDE ELETRÔNICA NA INTERNET. TRANSFERÊNCIA DE NUMERÁRIO DE CONTA DA CAIXA ECONÔMICA FEDERAL. FURTO MEDIANTE FRAUDE QUE NÃO SE CONFUNDE COM ESTELIONATO. CONSUMAÇÃO. SUBTRAÇÃO DO BEM. APLICAÇÃO DO ART. 70 DO CPP. COMPETÊNCIA DA JUSTIÇA FEDERAL PARANAENSE.
> 1. O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que, iludida, entrega voluntariamente o bem ao agente.
> 2. Hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de dois mil e quinhentos reais de conta bancária, por meio da "Internet Banking" da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima, o Banco. A fraude, de fato, foi usada para burlar o sistema de proteção e de vigilância do Banco sobre os valores mantidos sob sua guarda. Configuração do crime de furto qualificado por fraude, e não estelionato.
> 3. O dinheiro, bem de expressão máxima da idéia de valor econômico, hodiernamente, como se sabe, circula em boa parte no chamado "mundo virtual" da informática. Esses valores recebidos e transferidos por meio da manipulação de dados digitais não são tangíveis, mas nem por isso deixaram de ser dinheiro. O bem, ainda que de forma virtual, circula como qualquer outra coisa, com valor econômico evidente. De fato, a informação digital e o bem material correspondente estão intrínseca e inseparavelmente ligados, se confundem. Esses registros contidos em banco de dados não possuem existência autônoma, desvinculada do bem que representam, por isso são passíveis de movimentação, com a troca de titularidade. Assim, em consonância com a melhor doutrina, é possível o crime de furto por meio do sistema informático.
> 4. A consumação do crime de furto ocorre no momento em que o bem é subtraído da vítima, saindo de sua esfera de disponibilidade. No caso em apreço, o desapossamento que gerou o prejuízo, embora tenha se efetivado em sistema digital de dados, ocorreu em conta-corrente da Agência Campo Mourão/PR, que se localiza na cidade de mesmo nome. Aplicação do art. 70 do Código de Processo Penal.
> 5. Conflito conhecido para declarar competente o Juízo Federal de Campo Mourão - SJ/PR." (STJ, CC 67343/GO, Ministra Laurita Vaz, DJ 11/12/07, Pág.170).

Segundo a jurisprudência do STJ, não se confunde estelionato com furto qualificado, a fraude no furto qualificado consiste em ludibriar a vítima para aproveitar a oportunidade de desatenção da mesma para sem que possa perceber extrair um bem, a fraude no estelionato é o meio que o agressor se utiliza para obter o consentimento da vítima que ludibriada confere de forma voluntária o bem.

4. PROCEDIMENTO GERAL E LIMITAÇÕES DA RESPOSTA ESTATAL

A Internet faz parte do cotidiano da população mundial se tornando cada vez mais uma necessidade do que um simples apetrecho, ela traz facilidade e comodidade, é extremamente útil, pois por meio dela se podem fazer inúmeras operações sociais, econômicas, laborais e entre outras. Entretanto, em consequência da gama de opções e liberdades que a internet traz aos seus usuários, alguns indivíduos aproveitaram a oportunidade para a prática de atos ilícitos. Contudo, a ciência forense na busca de melhor proteger os bens jurídicos que restaram desamparados em virtude da contínua transformação tecnológica, almeja coibir e amenizar os crimes cibernéticos.

4.1 Limites do Procedimento de Investigação

Os cibercrimes são investigados pela ciência forense através de métodos similares que são utilizados para analisar os crimes de caráter não virtual, são eles: obtenção, preservação, análise e exposição de evidências. Esses procedimentos investigativos requerem análises criteriosas e seus processos possuem uma rotina comum a ser seguida. Dificilmente a exposição de evidências é definitiva no processo, pois o direito ao contraditório permite a contestação sobre a legitimidade do processo de investigação e a veracidade do diagnóstico da perícia, ensejando necessariamente em novas análises investigativas no procedimento forense. Levando-se em consideração esses aspectos, para que as provas digitalmente produzidas possam ter validade é necessário seguir os requisitos propostos pelo Ministério Públicos Federal no Roteiro de Atuação Crimes Cibernéticos, que concerne:

> "**1. Admissível:** ou seja, estar em plena conformidade com a lei para que possa ser apresentada à justiça.
> **2. Autêntica:** as provas devem ser comprovadamente relacionadas ao incidente/crime investigado. O trabalho de uma documentação de qualidade é essencial para o cumprimento deste item.
> **3. Completa:** o conjunto de evidências deve fornecer uma apresentação completa acerca do evento investigado. Nunca deve depender de elementos faltantes ou duvidosos. Deve " contar a história" completa, e não apenas fornecer perspectivas particulares.
> **4. Confiável:** não deve haver incertezas acerca da autenticidade e veracidade das evidências, bem como sobre as formas como foram coletadas e posteriormente manuseadas durante a investigação.
> **5. Convincente**: além de todas as características anteriores, deve ser documentada e apresentada de forma clara e organizada." (Roteiro de atuação: crimes cibernéticos / 2. Câmara de coordenação erevisão. – 3.ed. rev. e ampl. – Brasília: MPF, 2016. Pág; 156).

Tendo em vista os aspectos observados dos requisitos supracitados, vê-se que são bastante similares, entretanto, possuem diferenças únicas que podem ser observadas no desempenho funcional desse processo investigativo, pois é incumbência do investigador compreender as diferenças e lidar com elas com maestria, conforme Cristiana Isabel Castro Lima em sua dissertação de mestrado Química na análise de Vestígios de Crime afirma que "Enquanto o vestígio abrange, a evidência restringe e o indício circunstancia" (LIMA, 2013, Pág. 11).

Em conformidade com essa afirmação, a autora entende que vestígio abrange a concepção de ser todo sinal, rastro, marcas, pegadas, presença, objetos ou acontecimento fático que esteja potencialmente ligado a um sujeito em virtude de um evento penal relevante. Em relação ao ambiente virtual na investigação de crimes cibernéticos o objeto da celeuma não é uma coisa palpável, pelo fato de ser um artifício intangível o vestígio digital é representado por alguma intervenção humana que tenha causado um tipo de registro virtual. Tudo que os usuários fazem na internet é rastreável e deixa algum registro formando vestígios, portanto alguns exemplos de vestígios na web são as mensagens, os logins[48] de acesso, o recebimento e envio de arquivos e entre outros. Portanto, caso o investigador venha a retirar esses vestígios da web para uma análise ele pode fazer a ligação deles com o ato ilícito em foco mostrando as evidências auferidas.

Os vestígios devem ser extraídos num contingente abrangente o suficiente para construir uma linha de raciocínio lógico de evidências que sejam intrinsecamente ligadas ao processo, não fugindo do nexo causal. Por outro lado o indício aparece como aquela ocorrência que reconhecida e comprovada, logo quando ligada ao ato ilícito, leva-se por inferência, enfim, a existência de outras ocorrências. Portanto, a evidência se trata do vestígio que através de análises mais sólidas se encaixa na circunscrição do ato ilícito (Roteiro de atuação: crimes cibernéticos / 2. Câmara de coordenação erevisão. – 3.ed. rev. e ampl. – Brasília: MPF, 2016. Pág; 156).

É indiscutível que a investigação deve se desenvolver preservando a segurança das evidências, indícios e vestígios apurados. Assim sendo, é preciso manter a proteção das provas coletadas longe de ameaças digital como os vírus, logo, é extremamente necessário que sejam usados equipamentos que possam assegurar a confiabilidade das evidências, alguns dos

[48] Segundo Guimarães e Cabral "*Login* é um termo em inglês usado no âmbito da informática, um neologismo que significa ter acesso a uma conta de email, computador, celular ou outro serviço fornecido por um sistema informático. Esta palavra é formada pela junção de *log* e *in.* Em inglês *log* pode ser uma espécie de registro e *in* significa dentro. Assim, um *login* é entrar no registro ou no contexto da tecnologia aceder a uma base de dados. *Login* também é o nome escolhido pelo usuário quando tem que fazer a autenticação para usar um determinado sistema ou serviço. O *login* é feito com o nome de usuário e com a senha que foi escolhida." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: <https://www.significados.com.br/login/ >.Acesso em: 10 de março de 2017.

sistemas recomendados são o Linux[49] e o Mac OS[50] por serem menos suscetíveis a ataques cibernéticos, diferentemente do Windows[51] que se mostra mais vulnerável. Outros cuidados que devem ser tomados para preservação do processo é quanto ao navegador que será utilizado, não é prudente o uso do Internet Explorer[52] devido o seu histórico de erros, mas em contrapartida o Mozilla Firefox[53] tem correspondido melhor às expectativas colaborando no processo investigativo e minimizando possíveis falhas.

Na Web qualquer tipo de comunicação e interação entre usuários, páginas, downloads ou arquivos deixam rastros. Devido esse fato, do mesmo modo que um indivíduo experiente que comete cibercrimes age de forma eficiente na web para não deixar rastros, um investigador tem que ser ainda mais habilidoso e precavido para que o criminoso não note que está sobre suspeita em uma investigação. Atualmente existem vários artifícios para facilitar a mínima produção de rastros possível, várias das técnicas para diminuir a exposição do usuário são usados para a realização de atos ilícitos, os proxies, por exemplo, são as ferramentas mais efetivas para garantir uma navegação anônima na web. Portanto, os investigadores devem estar bem atentos quanto às novas tecnologias para não comprometer o processo de investigação.

4.2 Limites da Privacidade on-line

Ao analisar a conjuntura da internet e a forma como é utilizada pode-se perceber que ela possui características negativas, com isso, deve-se questionar quais consequências à nave-

[49] A Origiweb concerne "Sistema operacional, multitarefa, para computadores pessoais (PCs) desenvolvido pelo finlânes Linus Torvalds, em 1991. Disponibilizado gratuitamente na Internet, passou a receber a colaboração de outros programadores, o que tem contribuído para seu aperfeiçoamento." Dicionário de Tecnologia. Origiweb. 2017. Disponível em: < http://www.origiweb.com.br/dicionario-de-tecnologia/Linux >. Acesso em: 30 de março de 2017.

[50] Conforme Brito "Mac OS X foi o sistema operacional oficial dos computadores Mac, da Apple. Inicialmente, o sistema foi criado com base no NeXTSTEP, que por sua vez, era um sistema operacional Unix baseado no Mach, mais com código fonte do Unix BSD." BRITO, Edivaldo. Revista eletrônica Techtudo. 2016. Disponível em: <http://www.techtudo.com.br/tudo-sobre/mac-os.html >. Acesso em: 30 de março de 2017.

[51] Em concordância com Guimarães e Cabral "Windows é uma palavra de origem inglesa e sua respectiva tradução em Português é janelas. Windows foi um dos primeiros sistemas operacionais criados e comercializados para computadores em larga escala. É o nome dado ao sistema operacional para computadores desenvolvido pela empresa Microsoft. É um dos mais, se não for o mais utilizado em todo o mundo." GUIMARÃES, DILVA. CABRAL, PAULO. Dicionário de Significados. 2017. Disponível em: < https://www.significadosbr.com.br/windows >.Acesso em: 10 de março de 2017.

[52] "Programa de navegação pela Internet, desenvolvido pela Microsoft, lançado em outubro de 1995." Dicionário de Tecnologia. Origiweb. 2017. Disponível em: <http://www.origiweb.com.br/dicionario-de-tecnologia/Internet-Explorer>. Acesso em: 1 de abril de 2017.

[53] Para o Dicionário informal **"**O Mozilla Firefox é um navegador livre e multi-plataforma desenvolvido pela Mozilla Foundation (em português: Fundação Mozilla) com ajuda de centenas de colaboradores. A intenção da fundação é desenvolver um navegador leve, seguro, intuitivo e altamente extensível." Dicionário Informal. 2017. Disponível em: <http://www.dicionarioinformal.com.br/significado/firefox/594/>. Acesso em: 1 de abril de 2017.

gação na web traria a privacidade. A partir do momento em que um usuário começa a navegar pela internet, ou seja, fica on-line, tudo o que ele acessa através de páginas, fazendo uploads ou downloads, trocando mensagens, para todos esses eventos são gerados registros por softwares que permitem a leitura do tráfego de dados on-line, esse mecanismo é proveniente de dispositivos de inteligência artificial (IA) que são programados para executarem esse tipo de tarefa automaticamente. Por meio deles pode-se identificar a rotina de cada usuário, a IA processa a informação produzida e produz caminhos de navegação na web de acordo com o gosto de quem a utiliza. Essa invasão a privacidade é facilmente percebida nas redes sociais como o Instagram[54] e o Facebook que oferecem geralmente propagandas, páginas relacionadas ou pessoas conveniadas a mesma rede social que talvez o usuário possa conhecer.

Devido à facilidade em identificar a rotina cibernética dos indivíduos que utilizam a web, as plataformas de domínio que detém essas informações perceberam o quão valoroso esse sistema é e passaram a fazer comércio de informações pessoais e rotineiras dos usuários, com isso, as grandes empresas passaram a se utilizar dessas informações para localizarem seus alvos e tomarem atitudes economicamente mais estratégicas. Portanto, as grandes organizações compram esse tipo de informação para produzirem propagandas específicas para os seus alvos, elas são colocadas em pontos específicos na web que possuem mais acesso ou visibilidade do seu público a fim de fomentar a oferta e demanda de seus produtos. Entretanto, também foi percebido pelos indivíduos que navegam na internet que as suas informações pessoais viraram motivo de negócio sem o seu devido consentimento, pois todo o conteúdo publicitário voltado para a sua navegação é extremamente específico e singular de acordo com quem utiliza a web. Logo, os indivíduos que navegam na web têm a sua privacidade mercantilizada e violada. Porém, a privacidade na seara digital é abordada de forma diferente da privacidade contextualizada globalmente, dada a omissão normativa no que tange a cibernética a sociedade finda desprotegida e desamparada, pois a lei não é eficiente nem muito menos eficaz na sua execução, deixando transparecer uma grande lacuna entre ela e a sociedade tecnológica atual (DUARTE e MEALHA, 2016, Pág. 14).

Portanto, existe uma grande dificuldade em discernir aonde começa e termina o espaço privado digital e como isso se reflete no mundo exterior, com isso, não se sabe ao certo até onde a sociedade pode dispor de sua privacidade em virtude dessa insegurança. Um dos principais alertas correspondentes à violação a dados privados foi levantado por Edward Snowden

[54] "Nome próprio. Trata-se de uma rede social compatível para celulares que possuem o sistema Android, que compartilha fotos e vídeos. É gratuita." Dicionário Informal. 2017. Disponível em: <http://www.dicionarioinformal.com.br/instagram/ >. Acesso em: 2 de abril de 2017.

que deflagrou um grande sistema de interceptações cibernéticas e telegráficas do governo dos Estados Unidos contra o resto do mundo, isso foi fato gerador de intrigas e desconfianças entre alguns países e as Nações Unidas, pois até os cabos de fibra ótica apresentaram fragilidades e brechas para invasão. Dessa forma, observa-se que a privacidade é extremamente comprometida e desprotegida no ambiente virtual.

4.3 Limites Constitucionais nos Crimes Cibernéticos

O surgimento da sociedade digital se deu inicialmente através dos mecanismos criados para o melhoramento das atividades habituais ou cotidianas, são apetrechos que proporcionam essa facilitação e mobilidade, eles resguardam bens jurídicos fundamentais para a sociedade. Portanto, a sociedade encontra-se vinculada a informática devido o grande processo de transformação social tecnológico que viveu a partir dos anos 90, contudo, a criminalidade também ficou intrinsecamente ligada à seara digital, pois também passou pelo mesmo processo de informatização e se aprimorou nesse meio. Desse modo, com o aparecimento de novos meios de crimes, os virtuais, também surgiram novos bens jurídicos a serem tutelados e em virtude disso a ordem constitucional sofreu um impacto que consequentemente refletiu na esfera penal. (MONTEIRO NETO, 2008, Pág. 6; OLIVEIRA, 2013, Pág. 11). Devido a esse impacto, o ordenamento constitucional findou tendo que de algum modo tentar abarcar essas novas possibilidades jurídicas que nasceram, por isso, a Constituição Federal tentou ampliar o seu entendimento para a proteção desses novos bens jurídicos (MONTEIRO NETO, 2008, Pág. 9).

Portanto, para o homem contemporâneo faz parte da sua rotina a informatização para que possa se atualizar com relação aos acontecimentos e fatos recorrentes no mundo social, econômico e cultural. Assim sendo, a democracia moderna se vincula a informática e a informação por se tratar de um artifício fundamental atualmente. A Constituição reserva como um dos direitos a liberdade o direito pertinente à informação, que foi previsto no artigo 5° caput e em poucos incisos que garantem: o anonimato (IV), proteção contra o dano moral ou a imagem (V), a liberdade intelectual (IX), acesso a informação (XIV, XXXIII e LXXII), esse pequeno trecho constitucional está intimamente vinculado à informática e a liberdade da sociedade de poder acessar a informação mas não protege a cibernética devidamente. Conforme Simão Prado Lima, em sua análise sobre os crimes virtuais e a eficácia da legislação, entende da seguinte maneira:

> "Se faz salientar que é crescente a necessidade de intervenção do Estado na fruição dos meios tecnológicos de produção e difusão da informação, como preconizado na Constituição Federal. No entanto, tal intervenção não pode ser desordenada, sob pena de ferir o princípio da intervenção mínima. Desse modo, tal intervenção deve ser focada na fiscalização e inibição de práticas nocivas." (LIMA, Simão Prado, 2017, Pág. 68).

Dessa forma, pode-se entender que cabe ao Direito Penal manusear novos artifícios repressivos e preventivos referentes à proteção dos bens jurídicos no que tange as novas violações advindas da cibernética. Contudo, devido o fato de não se ter tomado um posicionamento jurídico pertinente à cibernética, a carência de normas regulamentadoras faz com que o ambiente virtual passe a sensação de "desamparo legislativo" a sociedade. Portanto, acaba-se ferindo princípios basilares no Estado de Direito como: a dignidade da pessoa humana ou, o princípio da anterioridade que no texto constitucional retrata que não há crime sem lei anterior que o defina, com isso, são se pode punir um ato ilícito sem prévia cominação legal e como a seara digital é um ambiente escasso de legislação o cidadão fica claramente desamparado.

4.4 Limites estabelecidos pela Ineficácia da legislação

O Direito Penal não se atualizou seguindo as mudanças tecnológicas que vem ocorrendo atualmente na sociedade. A Constituição Federal busca proteger a sociedade estendendo a sua interpretação para abranger os interesses sociais envolvidos no ambiente virtual. O espaço cibernético também é um âmbito mercantil no qual muitos contratos são celebrados diariamente pelos internautas, entretanto, não existe uma regulamentação jurídica para esse tipo de celebração de contrato via internet, o Código Civil e o Código de Defesa do Consumidor não conseguem abarcar e reger todas essas negociações e possibilidades emergentes da web, por isso, existe a necessidade da criação de uma lei que possa assegurar todo aparato social virtual (VEDOVATE, 2005, Pág. 13). Segundo Simão Prado Lima em sua análise sobre os crimes virtuais e a eficácia da legislação entende que são aplicados por analogia, in verbis:

> "Os casos dos contratos celebrados pela via digital são mais um exemplo de que o Brasil não possui legislação específica sobre os ilícitos cometidos através desse meio. Muitas vezes, é utilizado o princípio da analogia como único meio hábil a não deixar o infrator cibernético impune. Contudo, tal princípio não é aplicável no Direito Penal, por ferir do princípio da taxatividade, sendo necessária a criação de leis mais específicas. São exemplos de normas aplicadas, com a utilização da analogia, aos crimes virtuais: Calúnia (art. 138 do Código Penal); Difamação (art. 139 do Código Penal); Injúria (art. 140 do Código Penal); Ameaça (art. 147 do Código Penal); Furto (art. 155 do Código Penal); Dano (art. 163 do Código Penal); Apropriação indébita (art. 168 do Código Penal); Estelionato (art. 171 do Código Penal); Violação ao direito autoral (art. 184 do Código Penal); Pedofilia (art. 247 da Lei nº 8.069/90 - Estatuto da Criança e do Adolescente); Crime contra a propriedade industrial (art.

> 183 e ss. da Lei nº 9.279/96); Interceptação de comunicações de informática (art. 10 da Lei nº 9.296/96); Interceptação de E- mail Comercial ou Pessoal (art. 10 da Lei nº 9.296/96); Crimes contra software - "Pirataria" (art. 12 da Lei nº 9.609/98)." (LIMA, Simão Prado, 2017, Pág. 3).

Com isso, os atos ilícitos desferidos contra informações virtuais, programas, aplicativos, disseminação de vírus e como também inúmeras outras condutas prejudiciais aos internautas realizadas na web não são consideradas crimes ou muito menos estão tipificadas, não sendo possível assim nem ao menos o uso da analogia para punir esse tipo de conduta, pois feriria o princípio da taxatividade que diz que não basta a existência de uma norma que tipifique um ato, a lei deverá ser clara e concisa dando ciência ao cidadão de que tal conduta é passiva de punição. O ordenamento jurídico brasileiro possui em seu acervo poucas leis que deliberam sobre a informática, por isso, não consegue abranger toda a seara cibernética. O doutrinador Alexandre Atheniense em sua obra entende que deveriam se buscar as seguintes medidas:

> "Entendo que as soluções legais a serem buscadas deverão objetivar a circulação de dados pela internet, controlando a privacidade do indivíduo sem cercear o acesso à informação. Neste sentido é necessário aprimorar nossas leis de proteção de dados, inclusive com a regulamentação da atividade dos provedores que controlam a identificação do infrator, bem como um maior aparelhamento das delegacias especializadas." (ATHENIENSE, 2004, p. 1).

Em virtude da existência de uma lacuna legislatória para discernir sobre a cibernética alguns casos específicos chamaram atenção da sociedade com relação a este ponto. No mês de maio em 2012 a atriz Carolina Dieckmann teve o seu computador invadido e fotos pessoais suas divulgadas na internet, porém, pelo princípio da taxatividade não existia lei específica que delimitasse a conduta do agressor, desse modo, esse acontecimento fomentou a criação de um projeto de lei que vulgarmente ficou conhecido pelo nome da atriz já supracitado, o PL n° 2.793/2011 que logo se tornou a lei ordinária 12.737/2012. Outro projeto de lei que também merece destaque é o PL n° 84/1999 que se tornou lei ordinária 12.735/2012. Essa norma foi criada para alterar algumas partes do Código Penal, Código Militar e a Lei n° 7.716 com o intuito de regulamentar um número reduzido de condutas ligadas ao sistema informático. Essas leis ordinárias tipificam brevemente o uso da informática e cibernética, pontuando apenas a invasão de artifícios virtuais alheios por agressores que tenham finalidade perversa e sem o consentimento do dono dos dados (WANDERLEI, 2012, Pág. 43). Segundo Simão Prado Lima essas atitudes tomadas pelo legislador não são suficientes, in verbis:

> "Todas essas ações não são suficientes para coibir as práticas do infrator cibernético. Há a necessidade de regulamentação da internet, o que está sendo discutido pela sociedade atualmente, através do chamado Marco Civil da Internet. Tal instituto con-

> siste em uma espécie de constituição da internet contendo princípios que nortearão o correto uso da internet no Brasil, além de projetar diretrizes para o Poder Público no sentido de buscar o desenvolvimento saudável da internet no Brasil." (LIMA, Simão Prado, 2017, Pág. 3).

Portanto, o Marco Civil, lei n° 12.965/14, mesmo regularizando a seara civil causa pouco respaldo no âmbito criminal, dessa forma, não é suficientemente abrangente para resguardar os novos bens jurídicos emergentes.

Conforme vem se apresentando a conduta dos criminosos virtuais, eles fazem uso dos aparatos tecnológicos para disfarçarem e encobrirem os seus crimes, desse modo eles podem permanecer no anonimato com facilidade. Portanto, em virtude da expansão tecnológica se torna cada vez mais evidente que o ordenamento jurídico necessita de uma legislação adequada para regulamentar os atos ilícitos praticados através da cibernética, é essencial para que os delitos cometidos virtualmente não fujam do controle, como no ano de 2011, por exemplo, no qual as páginas do governo foram abatidas. As ilicitudes praticadas no ambiente virtual precisavam de limites, por isso quando a Lei 12.737/12 entrou em vigor ficou conhecida vulgarmente por AI-5 virtual devido a sua represália e retenção de IPs dos provedores. Pode-se observar que o legislador é facilmente influenciado pela mídia, como no caso da atriz Carolina Dieckmann que teve dados pessoais hackeados e disponibilizados na web, devido a grande repercussão midiática o legislador rapidamente buscou meios de sanar a lacuna normativa, por isso, em virtude desse modo errôneo de agir por parte de quem legisla passa a imagem de que o maquinário estatal só funciona para determinadas pessoas.

As leis 12.735/12 e 12.737/12 trazem consigo a ideia de que as normas atualmente vigentes são suficientes para regulamentar as novas ilicitudes provenientes da cibernética e que seria preciso apenas alguns "reparos" para proteger amplamente a sociedade. Segundo Simão Prado Lima as normas não são suficientes, in verbis:

> "Ambas as leis aqui analisadas tiveram o objetivo de preencher lacunas legislativas que impediam a tipificação de atos ilícitos praticados pelos meios digitais. Desta feita, desejou- se cumprir os princípios que norteiam o Direito Penal, a saber, o da legalidade e a proibição da analogia. Tiveram como foco a proteção da informação. No entanto, devem ser criados mecanismos específicos no combate aos crimes virtuais. O mundo virtual ainda percebe um vazio normativo, o que contribui para a falta de punição estatal." (LIMA, Simão Prado, 2017, Pág. 4).

Por fim, observa-se que as leis estudadas não objetivaram reformular a cibernética no âmbito jurídico, mas apenas reestruturar as normas já existentes focando basicamente na informação, desse modo o ambiente virtual continua desregulamentado.

4.5 Possíveis Medidas de Prevenção e Repressão Contra os Crimes Cibernéticos

O trânsito de informações na rede de computadores por meio de internautas ou sistemas organizacionais é o que faz a sociedade virtual, contudo, o transitar dos dados na web acaba passando por vários ambientes cibernéticos ficando sujeitos a qualquer indivíduo que queira armazená-lo, com ou sem o consentimento do dono original, podendo ser visualizado inúmeras vezes, manipulado ou deletado. Dado o exposto, procura-se um meio de equalizar o fluxo de dados disponíveis com a devida proteção. Para garantir a proteção dos dados, precisamente, é necessário adotar medidas que possam assegurar o trânsito das informações livres de plágios, desvios e com a disponibilidade adequada, que seja adotada uma estratégia eficiente o suficiente para acompanhar o avanço do crescimento tecnológico na sociedade, pois do mesmo modo que cresce a tecnologia também crescem os crimes cibernéticos que causam consequências reais.

Em virtude da internet não estabelecer fronteiras, deixando os seus usuários livres em um mundo abertos a novas percepções, pode-se ter interações com qualquer parte do mundo, ter acesso a várias culturas, imagens, vídeos e qualquer outro fator de interesse para o internauta. Os crimes cibernéticos acontecem da mesma forma que os crimes comuns, eles variam conforme a forma e o objetivo dos criminosos, mas se utilizam de uma única via de execução que é a informática. Esses crimes virtuais só tem o internauta como vítima se ele não for previamente instruído sobre essas agressões, já que esse tipo de ato ilícito é um dos únicos que a vítima sai com êxito ao reagir à agressão.

Em consequência disso, um dos órgãos que vem se destacando na buscar para melhor proteger e instruir a sociedade é o Ministério Público do Estado da Bahia que criou um núcleo específico para atender a demanda dos atos ilícitos virtuais, esclarecer as dúvidas da população e contribuir no combate a esses delitos com o Núcleo de Combate aos Crimes Cibernéticos (NUCCIBER).

> "Com a finalidade de articular, em conjunto com os Promotores de Justiça, medidas judiciais e extrajudiciais necessárias à efetivação do combate aos crimes cibernéticos de competência e âmbito estadual, o Núcleo de Combate aos Crimes Cibernéticos do Ministério Público do Estado da Bahia – NUCCIBER – fornece todo o suporte basilar que fundamente tais medidas ou que possibilite a identificação da autoria delitiva para prosseguimento em investigações tradicionais.
> À denúncia de crime cibernético pode ser efetuada em qualquer canal de acesso ao cidadão, a saber, pessoalmente, por telefone, site ou e-mail. Ao receber a denúncia de um crime virtual em um dos departamentos da Instituição, esta será encaminhada ao Promotor de Justiça competente para atuar e dar andamento a solução desta demanda. Havendo a flagrante necessidade de atuação, o Núcleo de Combate aos Crimes Cibernéticos do Ministério Público do Estado da Bahia – NUCCIBER – é acionado para prestar auxílio. A partir do recebimento de ofício requerendo investiga-

> ções preliminares, o Núcleo diligência a situação.” (PATURY, SALGADO, TEIXEIRA FILHO. 2017. Pág. 10).

Pode-se observar que preliminarmente a investigação se inicia por meio de artifícios disponibilizados na web no qual se retira todas as informações pertinentes a respeito do caso em questão com o intuito de encontrar o dispositivo informático percussor do ato ilícito. O NUCCIBER faz muito uso de medidas preventivas fomentando a devida instrução legal da população em conformidade com a Lei 12.965/14, in verbis:

> “Art. 25. As aplicações de internet de entes do poder público devem buscar:
> I - compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;
> II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;
> III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;
> IV - facilidade de uso dos serviços de governo eletrônico; e
> V - fortalecimento da participação social nas políticas públicas.
> Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.
> Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem:
> I - promover a inclusão digital;
> II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e
> III - fomentar a produção e circulação de conteúdo nacional.
> Art. 28. O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da internet no País.” (LEI Nº 12.965, DE 23 DE ABRIL DE 2014).

Portanto, estabelecendo assim a inclusão digital mais segura da população, fomentando uma navegação na web mais ética.

4.5.1 Palestras

A realização de palestras educativas nas escolas e universidades, que possam ensinar como melhor usar a internet, evitando a exposição desnecessária dos usuários, reprimindo o ciberbullying, a disseminação de imagens íntimas nas redes sociais e o envio de mensagens com informações pessoais a pessoas desconhecidas. Alertando sobre o uso moderado da internet para uma melhor vida saudável e social. Pois o jovem que compartilha algo na web está lançando uma informação sua a todo o publico mundial e o Estado deve conscientizar a população de que após se publicar algo na internet se perde o controle dessa publicação, já que quando ela é disponibilizada no mundo virtual permite-se que qualquer pessoa a veja ou faça

download. Outro perigo emergente na web são os fakes[55], que se tratam de pessoas que criam uma espécie de personagem para poder obter vantagens sobre outras extraindo informações ou as persuadindo a prática de algum ato. Desse modo, não existe uma barreira de proteção adequada para os usuários (PATURY, SALGADO, TEIXEIRA FILHO. 2017. Pág. 11).

Levando-se em consideração esses aspectos, o Ministério Público Federal deve desenvolver palestras sobre os danos que a internet pode vir a causar, tanto na rede pública de ensino quanto na rede particular, a fim de instruir os alunos, pais e professores, conforme as necessidades sociais de cada público, como uma medida preventiva visando minimizar o número de vítimas das agressões cibernéticas.

4.5.2 Treinamento e Capacitação na Seara Jurídica

É necessário, para um melhor combate contra os crime cibernéticos, a capacitação e treinamento dos membros do Poder Judiciário sobre os perigos que a internet reserva, cursos sobre as redes sociais e suas possíveis manipulações indevidas como também as particularidades dos crimes digitais, os conceitos sobre esse novo perigo eminente, o respaldo na sociedade, os novos bens jurídicos emergentes, juntamente com as possíveis formas de investigação.

> "Em um primeiro momento a oficina versa sobre Introdução à Crimes Cibernéticos. Neste encontro é repassada a parte conceitual desta nova modalidade de delito, ressaltando as formas de configuração de um Crime Cibernético e suas classificações. Importante também é reforçar os termos técnicos da área de Tecnologia da Informação mais usuais e de grande valia para fomentar o diálogo entre os órgão investigativos. Na explanação seguinte, os profissionais desenvolvem as noções preliminares da prática investigativa. Casos concretos de investigação como cyberbulling, fraudes eletrônicas e bancárias, práticas de phishing Scam, crimes cometidos através de e-mails, pedofilia, racismo, dentre outros são apresentados, debatidos e trabalhados nas oficinas. " (PATURY, SALGADO, TEIXEIRA FILHO. 2017. Pág. 13).

Assim também, instruindo os profissionais sobre a preservação da privacidade, a maneira correta de se executar a liberdade de expressão na web sem ferir a ética, a responsabilização pelos conteúdos publicados em suas redes sociais como também o respaldo das mesmas, tudo isso vislumbrando o combate a inércia estatal em face aos delitos virtuais.

4.5.3 Oficinas Tecnológicas

A promoção de oficinas por parte do Ministério Público que tenham como ponto principal o estudo sobre as inovações tecnológicas e seu respaldo na sociedade, como o cidadão

[55] Personagem falso criado para persuadir, enganar ou buscar informações de internautas.

pode se portar perante a cibernética dentro dos limites legais permitidos. Fomentar os debates sobre estudos de casos de crimes cibernéticos a fim de alertar a população sobre os perigos e instruir como combater esse tipo de conduta ilícita. Viabilizar trocas de informações entre os Ministérios Públicos para melhor aproveitamento de técnicas, aprendizado e compartilhamento de experiências, tornando o sistema mais eficiente no que tange a resposta estatal para os ilícitos virtuais (PATURY, SALGADO, TEIXEIRA FILHO. 2017. Pág. 14).

4.5.4 Atendimento a Sociedade

O Ministério público deve procurar gerar o atendimento à população, fazendo mutirões para alertar o cidadão sobre os crimes cibernéticos e como evita-los, promovendo projetos e programas para envolver a sociedade nesse combate, como também atender as dúvidas do povo sobre o assunto. Realizar parcerias com organizações que possam ajudar a desenvolver e ampliar o alcance do combate aos crimes cibernéticos, principalmente nas comunidades mais isoladas e periféricas da sociedade (PATURY, SALGADO, TEIXEIRA FILHO. 2017. Pág. 14).

Além disso, inserir propagandas nos meios de comunicação e principalmente nas redes sociais orientando sobre os perigos da web, mostrar o que dispõe o ordenamento jurídico sobre os atos ilícitos na internet e conduzir a que órgão as vítimas de crimes cibernéticos devem recorrer para buscar auxílio.

4.5.5 Criação de uma nova Lei

O Brasil ainda não foi contemplado com uma legislação específica que regulamente todas as hipóteses pertinentes aos crimes cibernéticos, por isso deixa a sociedade desprotegida nesse aspecto. Assim, é necessário o estudo e uma análise minuciosa de uma possível redação legal que possa regulamentar as condições e políticas que devem ser adotadas na web, a tipificação de condutas danosas ou reprováveis pela sociedade, os crimes cibernéticos e também as devidas punições, a regulamentação dos provedores, bem como das plataformas dos sistemas, a criminalização da propagação de vírus e qualquer outra conduta ou artifício referente a seara digital que respalde negativamente no âmbito social ou fira a dignidade da pessoa humana. O ordenamento jurídico brasileiro precisa de uma regulamentação específica que possa proteger os novos bens jurídicos que emergiram da tecnologia (PATURY, SALGADO, TEIXEIRA FILHO. 2017. Pág. 6).

5. CONCLUSÃO

Atualmente o número de acessos à internet cresce a cada dia. Desse modo, é preciso a devida regulamentação do Estado na seara virtual para reprimir as condutas que excedam os limites da privacidade e liberdade on-line, pois os atos praticados virtualmente tem respaldo no mundo real. Portanto, para que o ordenamento jurídico possa inibir os crimes cibernéticos é necessária à tipificação dessas condutas delituosas. Entretanto, acontece que atualmente nenhuma conduta foi tipificada com as suas devidas punições.

A iniciativa do legislador na elaboração das Leis 12.735/2012, 12.737/2012 e 12.965/2014 foi de grande importância, pois pouco se falava no em regulamentação cibernética, contudo, essas leis não são efetivamente suficientes. A alteração do Código Penal é imprescindível, pois, já que ele é da década de 1940 fica claramente desatualizado em relação à evolução tecnológica que a sociedade vive atualmente, a referida norma não se impõe quanto à cibernética. As leis fizeram poucas alterações no referido código, deixando condutas virtuais não tipificadas, fomentando a ideia de que "a internet é um mundo sem leis". O Marco Civil serve de auxílio ao Direito Penal, contribui para que a web se torne um ambiente mais pacífico. Porém, é uma lei de cunho cível e não penal, portanto, auxilia no combate aos crimes cibernéticos, mas não os combate diretamente, por isso, sozinho não trará ampla proteção para a sociedade ou aos novos bens jurídicos que surgiram da tecnologia.

No ambiente digital o modo de agir do homem pode gerar impactos positivos ou negativos, por isso, para prevenir a sociedade de condutas negativas geradas na web é imprescindível a atuação do Estado para reprimir esses atos. De fato, em virtude de como a população se utiliza da web atualmente, não é prudente ao Estado adotar medidas unicamente repressivas quanto às condutas ilícitas praticadas virtualmente, a adoção de medidas preventivas também é extremamente essencial, pois o trabalho em conjunto entre o cidadão e o maquinário estatal, através da instrução e capacitação do povo, é forte aliado na redução dos cibercrimes.

O Ministério Público deve conscientizar a população sobre o uso da internet, ensinando que suas ações no mundo virtual geram consequências no mundo real. Por fim, além de legislar sobre a regulamentação da cibernética preenchendo as lacunas existentes o Estado deve fomentar a educação e inclusão digital.

REFERENCIAS

ATHENIENSE, A. R. **Crimes virtuais, soluções e projetos de Lei**. DNT. [s.l.]. 29 out. 2004. Disponível em: <http://www.dnt.adv.br/noticias/direito-penalinformatico/crimes-virtuais-solucoes-e-projetos-de-lei/>. Acesso em: 27 mar 2017.

ARAS, Vladimir. **Crime de Informática. Uma Nova Criminalidade**. Jus Navigandi. Teresina, ano 6, n. 51, Outubro de 2001. Disponível em: <http://jus.com.br/artigos/2250/crimes-de-informatica>. Acesso em: 1 jan 2017.

CAPEZ, Fernando**. Curso de Direito Penal:** Parte Geral. 16 Ed. 2 tiragem. Vol. I. São Paulo: Saraiva, 2012.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2 Ed. rev, ampl e atual. Rio de Janeiro, 2003.

CERT. **Cartilha de Segurança para Internet**. ISBN: 978-85-60062-54-6. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, CERT.br. Edição: 2ª. Editora: Comitê Gestor da Internet no Brasil. Cidade: São Paulo. Ano: 2012. Disponível em: < https://www.cert.br/docs/whitepapers/ddos/ >. Acesso em: 20 fev 2017.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 2002.

COSTA, Fernando Jose da. Locus Delict nos Crimes Informáticos. Tese de Doutorado da Usp. 2011. Disponível em: <http://www.teses.usp.br/teses/disponiveis/2/2136/tde-24042012-112445/pt-br.php.>. Acesso em: 4 mar 2017.

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

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal:** Parte Geral. 18 Ed. rev, ampl, e atual. São Paulo: Saraiva, 2012. Vol. I.

BRASIL. Acordão. STJ. Processo: CC 67343/GO (2006/0166153-0). Conflito de Competência. Relatora: Ministra Laurita Vaz. Órgão julgador: Terceira Seção. 28/02/2007. DJ 11/12/07, Pág. 170. Disponível em: < http://www.prgo.mpf.mp.br/fato_tipico/pagina_edicoes002-jurisprudencia.html > Acesso em: 1 mar 2017.

BRASIL. Código Civil, Lei 10.406, de 10 de janeiro de 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm > Acesso em: 2 fev 2017.

BRASIL. Estatuto da criança e do Adolescente. Lei n° 8.069 de 13 de julho de 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8069.htm > Acesso em: 2 fev 2017.

BRASIL. Lei de introdução do Código Penal (decreto-lei n. 2.848, de 7-12-940) e da Lei das Contravenções Penais (decreto-lei n. 3.688, de 3 outubro de 1941) . Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm > Acesso em 20 fev 2017.

BRASIL. STJ, CC 67343/GO (2006/0166153-0), CONFLITO DE COMPETÊNCIA, RELATORA: MINISTRA LAURITA VAZ, ORGÃO JULGADOR: TERCEIRA SEÇÃO,

28/03/2007, DJ 11/12/01, PÁG. 170. Acesso disponível em: < http://www.prgo.mpf.mp.br/fato_tipico/pagina_edicoes002-jurisprudencia.html > Acesso em: 1 mar 2017.

BRASIL. TRF2 - HC 201102010006429 RJ 2011.02.01.000642-9. Relator: Juiz Federal Convocado ALUISIO GONCALVES DE CASTRO MENDES. Julgamento: 23/02/2011. Órgão: PRIMEIRA TURMA ESPECIALIZADA. Disponível em: <https://trf-2.jusbrasil.com.br/jurisprudencia/18422705/habeas-corpus-hc-201102010006429-rj-20110201000642-9/inteiro-teor-104014751?ref=juris-tabs#>. Acesso em: 10 fev 2017.

COIN MAPS. Disponível em:< https://www.bitcoinnews.com.br/bitcoinbrasil/novo-mapa-interativo-da-coinmap-mostra-estabelecimentos-que-aceitam-bitcoin/ >. Acesso em: 12 fev 2017.

CONVERSOR DE MOEDA CORRENTE. Disponível em: < http://pt.coinmill.com/BRL_BTC.html >. Acesso em: 16 fev 2017.

DE ARRUDA, Matheus Fernando et al. **Reflexão sobre a Relação entre a Internet e o Estado ns Sociedades Contemporâneas**: A Importância de Uma Regulamentação que Compreenda a Dinâmica do Desenvolvimento Tecnológico e Valorize os Direitos Fundamentais. Revista de Direito, Governança e Novas Tecnologias, v. 2, n. 1, p. 55-73, 2016.

DUARTE, David; MEALHA, Tiago. **Introdução à deep web**. IET Working Papers Series, p. 1-26, 2016.

MONTEIRO NETO, J. A. **Aspectos Constitucionais e Legais do Crime Eletrônico**. Fortaleza, 2008.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**: Parte Geral e Parte Especial. 8 Ed. rev, ampl, e atual. São Paulo: Revista dos Tribunais, 2012.

LIMA, Cristiana Isabel Castro. **Química na análise de vestígios de crime**. PhD Thesis. 2013.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. 2 Ed. São Paulo: Atlas, 2011.

LIMA, Simão Prado. **Crimes virtuais**: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade. In: Âmbito Jurídico, Rio Grande, XVII, n. 128, set 2014. Disponível em: < http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=15260&revista_caderno=3 >. Acesso em: 12 mar 2017.

OLIVEIRA, J. C. de. **O Cibercrime e as Leis 12.735 e 12.737/2012**. São Cristóvão, 2013.

PATURY, Fabrício Rabelo. SALGADO, Fernanda Veloso. TEIXEIRA FILHO, Manoel do Bomfim B. **A Política Criminal do Núcleo de Combate aos Crimes Cibernéticos do Ministério Público do Estado da Bahia no enfrentamento aos ilícitos cometidos no âmbito digital**. 2017. Disponível em: <file:///G:/Crimes%20Cibern%C3%A9ticos/a_politica_criminal_do_nucleo_de_combate_aos_crimes_ciberneticos_do_ministerio_publico_do_estado_da_bahia._-_fabricio_rabelo_patury_e_fernanda_veloso_salgado.pdf> Acesso em: 4 abr 2017.

PLATAFORMA BITCOINS. Disponível em: < http://www.arenabitcoin.com.br/?gclid=COX-8uuB_NICFRAHhgodEaMHDg >. Acesso em: 15 fev 2017.

REXBIT. Disponível em: <https://www.bitcoinnews.com.br/tag/rexbit/>. Acesso em: 10 fev 2017.

SILVA, Alexandre Assunção e. **Violação a princípios constitucionais e penais na legislação de combate à pornografia infantil**. p. 453, Segunda Seção. São Paulo: Revista dos Tribunais. 2009.

SILVA, Patrícia Santos da. **Direito e crime cibernético**: análise da competência em razão do lugar no julgamento de ações penais [recurso eletrônico] / Patrícia Santos da Silva, Matheus Passos Silva (coord.). Brasília: Vestnik, 2015.

TOR. Disponível em: < https://www.torproject.org/images/tbb-screenshot3.jpg> . Acesso em: 5 fev 2017.

VEDOVATE, L. L. V. **Contratos Eletrônicos**. INTERTEMAS. v. 10, n. 10. Presidente Prudente, 2005.

WANDERLEI, F. P. **Crimes Cibernéticos**: Obstáculos para Punibilidade do Infrator. Araguaína, 2012.

WENDT, Emerson. **Inteligência cibernética** : da ciberguerra ao cibercrime a (in)segurança virtual no Brasil [recurso eletrônico] / Emerson Wendt. – livro digital. – São Paulo : Editora Delfos, 2011.