DOS CRIMES VIRTUAIS COMETIDOS SE UTILIZANDO DO ANONIMATO DA DEEP WEB

Laura Campos de FREITAS[1]
Jurandir José dos SANTOS [2]

RESUMO: O avanço tecnológico trouxe o uso desenfreado da internet, que tem aspectos positivos e negativos. Em que pese a internet transpor limites territoriais, facilitar nossa vida em diversos sentidos, e possibilitar a interação humana, ela também pode ser prejudicial, uma vez que o anonimato oriundo de ambiente obscuro como a Deep Web pode potencializar o cometimento de crimes que são dificilmente esclarecidos, posto a complexidade vislumbrada neste meio para identificar os criminosos. A Convenção de Budapeste regula tais crimes, traz conceitos, definições e até mesmo aspectos procedimentais para prevenir e combater essas práticas, contudo o Brasil não é signatário deste acordo de cooperação internacional. Ademais a legislação brasileira se encontra ultrapassada com relação a tal tema, e por isso há que se encontrar maneiras legislativas e jurisprudenciais tendentes a reprimir a prática destes delitos.

Palavras-chave: Crimes virtuais. Deep Web. Internet. Fraude.

1 INTRODUÇÃO

O direito sempre esteve presente na vida social, servindo para regular e solucionar os conflitos que surgem ao longo dos tempos. Ocorre que a vida não é estática, tal qual o direito, constantemente transformam-se os hábitos, costumes, relações e interesses, consequentemente, em muitos casos a ordem jurídica não está avançada o suficiente para abarcar situações cotidianas que vão surgindo no decorrer dos anos.

Com o desenvolver da sociedade, surgiram novas tecnologias, as quais permitiram ao ser humano maior facilidade em suas tarefas cotidianas, o que fez

[1] Discente do 4º ano do curso de Direito do Centro Universitário “Antonio Eufrásio de Toledo” de Presidente Prudente. E-mail: laurita_flo@hotmail.com.

[2] Docente do Curso de Direito do Centro Universitário “Antônio Eufrásio de Toledo” de Presidente Prudente, Especialista em Direito Civil e Processual Civil pela Associação Educacional Toledo de Presidente Prudente, Mestre em Direito Constitucional pela Instituição Toledo de Ensino de Bauru-SP. Promotor de Justiça. Orientador do trabalho. E-mail: jurandirjsts@hotmail.com.

com que nascessem novos paradigmas nas relações, que se tornaram virtualizadas, em virtude da origem da internet.

A internet, hoje, já é utilizada por bilhões de pessoas em todo mundo, veja que a informática está presente quase que na vida de todos. Ademais, nos últimos anos, nos vemos diante de uma total eclosão do sistema informático no mundo, e esse fenômeno está extremamente relacionado com as infinitas possibilidades que os meios informáticos oferecem no manejo das comunicações, armazenagem de dados e de informação.

Note-se, várias dessas relações não são abarcadas pela legislação vigente, isso por que, como já mencionado, o Direito não acompanha o ritmo das relações sociais.

São indiscutíveis as benesses trazidas por essa nova ferramenta, além disso, a Rede Mundial de Computadores traçou novos paradigmas no modo de agir, viver e se relacionar em sociedade. Segundo Augusto Rossini (2004, p. 110):

> A convenção de Budapeste, de 21 de novembro de 2001, celebrada pela Comunidade Europeia após o fatídico 11 de setembro do mesmo ano, muito bem sintetiza a preocupação hoje coletiva de se regulamentar esta nova realidade. Desta forma, a parte substantiva desta Convenção é profundamente analisada, a fim de se verificar de que maneira ela se harmoniza com o ordenamento jurídico brasileiro.

A Convenção de Budapeste trata especificamente dos delitos informáticos, e foi assinada por diversos países da Europa. Traz em seu bojo definições, conceitos, regramentos e aspectos procedimentais e protocolares para combate a crimes virtuais. Contudo, salienta-se que o Brasil não é signatário desta Convenção.

Podemos vislumbrar a internet como sendo um campo muito vasto, ainda não completamente conhecido e desbravado, existindo inúmeras situações em que o usuário é extremamente ignorante, o que leva pessoas mal-intencionadas, que encontram proteção no anonimato trazido pela rede mundial, praticarem atos ilícitos.

Portanto, é possível observar, o advento de uma figura delinquente e ágil, capaz de ludibriar e extrair vantagens ilícitas nas mais variadas situações, haja vista a internet ser um campo muito amplo, como já abordado.

Por isso, faz-se necessário conhecer a evolução histórica da informática, para compreender o surgimento desta nova espécie de criminoso.

2 CONTEXTO HISTÓRICO

Desde os primórdios, o homem sempre buscou elaborar técnicas e métodos para garantir o armazenamento e distribuição de informações. Cumpre destacar que a escrita foi a primeira delas, que, tempos de outrora, se manifestava como controle sobre a administração de domínios territoriais, pelo poder estatal, nas grandes civilizações.

Em que pese, a escrita demonstrar grande evolução, foi tão somente o desenvolvimento científico que possibilitou a manipulação de informações, de forma mais eficaz, através dos métodos computadorizados, que vieram com a criação da informática.

Por primeiro, o que regia essa novidade, era a cibernética, ciência voltada ao estudo das relações entre homem e máquina, uma vez que a partir de então, o ser humano passou a dispor de ferramentas sofisticadas que iam além de sua capacidade intelectual. Logo, nota-se que o surgimento da informática pode ser justificado por questões de ordem científica, social e ideológica.

De acordo com o entendimento referente ao relacionamento entre máquinas e homens de Flamarion Tavares Leite (2001, p. 89-90) *apud* Augusto Rossini (2004 p. 20):

> Com efeito, a automação já fora utilizada vários séculos antes da era cristã, podendo-se citar a pomba voadora de Arquitas de tarento (séculos V – IV a.C.), o sinalizador automático, construído por um discípulo de Platão para chamar às aulas os alunos da Academia (século IV a.C.), o caracol ambulante de Demétrio de Faléria (séculos IV-III a.C.), os atores automáticos que encenavam uma peça sobre o retorno à pátria dos heróis da Guerra de Tróia (século I a.C.). Na Idade Média, destaca-se o relógio de Gaaz (século V) dotado de um conjunto de figuras as quais, ao aceno de uma figura central, saíram de seus nichos e assinalavam as horas, martelando num sino. A essa época pertencem os pássaros cantores e leões urradores construídos por Leão, o Filósofo, para distração de Teófilo, imperador de Bizâncio. Na Renascença, J. Müller, matemático e arquiteto germânico, montou uma mosca que corria ao redor de uma mesa e uma águia que, postada à entrada de Nuremberg, movia a cabeça e agitava as

> asas para saudar o Imperador Maximiliano. Leonardo da Vinci construiu um leão automático que, depois de perambular pela sala do trono, detinha-se aos pés do rei Luís XII e abria o peito com as próprias garras, deixando cair brancas flores-de-lis.

Veja, a partir da leitura do texto acima, conclui-se que seria deveras cansativo e demandaria elaboração de outro texto, apenas para exemplificar as formas como o homem desenvolveu novas tecnologias para obter tudo o que precisava.

Dito isso, vale demonstrar como é formado um computador, ou seja, é máquina formada por um sistema eletrônico (hardware) apto a receber instruções a fim de armazenar informações, conforme os programas nele contidos (softwares). Portanto, nota-se que se trata de sistemas interligados que são comandados por dispositivos lógicos.

Necessário destacar que nem sempre foi assim, mas o formato atual de computador, para ser o que é hoje, passou por muitas transformações, tendo em vista que no início tal máquina tinha apenas finalidade de fazer cálculos matemáticos e ordená-los.

Ademais, os primeiros computadores fabricados no mundo tinham destinação específica, qual seja, uso militar e científico. Como se vê, não era algo de fácil acesso.

É por isso que, pesquisas científicas demonstram que os primeiros criminosos virtuais surgiram apenas no século XX, nascendo assim as primeiras referências sobre esses crimes cibernéticos. A propagação dessa modalidade criminosa teve seu início na década de 1970, momento em que os HACKERS tiverem grande destaque, por realizar ataques e furtos em softwares.

Cumpre destacar que nos anos 80, essa espécie de criminosos evoluiu, passando a cometer crimes como pedofilia, tráfico de drogas, pirataria, invasão de sistemas, tudo isso se utilizando da rede mundial de computadores. Foi nesse momento em que se iniciou uma busca para fiscalização e punição dos criminosos.

Ainda nos dias atuais, não há com grande profundidade regulamentação específica para esse tipo de ilícitos, tampouco tipificação e punição adequadas. Isso se dá em razão da facilidade de acesso à internet, e os crimes mais corriqueiros relacionados à informática não são abarcados pela legislação vigente,

ou se forem, não são suficientes para catalogar os crimes cometidos se valendo de ferramentas computadorizadas. Ocorre que muitos desses delitos não acampados pela legislação, justamente não o são, pois, com a evolução tecnológica eis que surge uma nova classe de criminoso, que vêm praticando crimes jamais imaginados antes, os denominados Delitos de Ocasião, não fosse o mundo cibernético, talvez nunca tivessem possibilidade de cometer tais crimes.

É preciso salientar que a internet possibilita que o usuário demonstre através dela, uma face e personalidade ocultas, não aparentes em sua vida social, haja vista que estando atrás de uma tela de computador, o utente não está vulnerável, podendo se utilizar de inúmeros traços e características, não revelados em sua realidade cotidiana.

Tal situação se intensifica com a com a globalização, decorrendo desta evolução célere do ambiente virtual, fazendo surgir um universo novo, o qual se denomina Deep Web, local em que o usuário se beneficia do anonimato, o que traz uma maior segurança, possibilitando a prática de vários ilícitos, dentre eles, principalmente a Pornografia Infantil, que foi alvo da primeira investigação no Brasil, de ilícitos perpetrados na Darknet

Veja, que tal investigação se mostra como apenas um passo dado, no sentido de coibir tais práticas, contudo, cumpre destacar que a Ordem Jurídica Brasileira ainda se encontra extremamente afastada de rigorosa regulamentação que tenha intuito controlar tais crimes.

Portanto, se mostra preocupante a situação em que se vive atualmente, com o surgimento de diversas modalidades criminosas frente ao advento tecnológico, no entanto, com legislação um tanto quanto deficiente nesse quesito, e que se não forem tomadas medidas para inibir trais práticas, ainda que preventivamente, estaremos diante de um retrocesso jurídico.

Nessa Toada, ainda mais inquietante é a dificuldade em encontrar tais criminosos, uma vez que ao se utilizar do anonimato, se acobertam por de trás da rede, justamente para não serem localizados e continuarem a prática de tais delitos.

3 CRIMES VIRTUAIS

Inicialmente, insta destacar as várias terminologias adotadas para se mencionar a esta categoria delitiva. Note-se, que comumente são aplicados diversos termos para se referir a práticas criminosas, que envolvem o agente, se utilizando de um computador conectado à rede mundial, como meio para cometer o crime.

Crime cibernético, crime digital, cyber crime, e-crime, crime eletrônico e crime informático são todas as sinonímias usadas ao se falar em crimes virtuais.

Para conceituar o delito informático, importante demonstrar os posicionamentos doutrinários acerca do tema, senão vejamos o entendimento bastante amplo de Guilherme Guimarães Feliciano (2000, p. 42):

> Conheço por criminalidade informática o recente fenômeno histórico-sócio-cultural caracterizado pela elevada incidência de ilícitos penais (delitos, crimes e contravenções) que têm por objeto material ou meio de execução o objeto tecnológico informático (hardware, software, redes, etc.).

Ademais, importante mencionar o conceito trazido por Augusto Rossini (2004, p. 110):

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

Do exame de tais concepções, inicialmente se verifica que o conceito abarca tanto os crimes, como as contravenções. Outrossim, possível notar que acopla também os conceitos de delito doloso, culposo, bem como os comissivos e os omissivos. Logo, se houver previsão para o tipo na forma culposa, poder-se-á tratar-se de delito virtual, assim como, esses crimes podem se consumar na omissão do agente, como exemplo, pode-se destacar a hipótese em que uma empresa de hospedagem de sites, verifica que o ilícito está sendo cometido, quando da inclusão de imagens com conteúdo pornográfico de menores em página de sua hospedagem, e nada faz para afastar tal prática.

Do conceito de Rossini, extraímos que os delitos informáticos alcançam as condutas praticadas no âmbito virtual, bem como qualquer conduta que possua

relação com sistemas informáticos. Ele ainda traz o seguinte exemplo: Uma fraude em que o computador é usado como instrumento do crime, fora da internet.

Por outra forma, pode-se dizer que crime virtual nada mais é do que fato típico, antijurídico e culpável, ocasião em que se utiliza um meio específico para que se consume esta modalidade. Por isso, os e-crimes são considerados como crime de meio, isto é, trata-se de espécie criminosa que ocorre apenas no ambiente virtual.

Araújo Júnior (1995 p. 127 e 133) *apud* Augusto Rossini (2004 p. 107) conceitua crime virtual da seguinte forma:

> (...) caracteriza-se por ser uma conduta lesiva, dolosa, à qual pode corresponder ou não a obtenção de uma indevida vantagem, porém cometida, sempre, com a utilização de dispositivos de sistemas de processamento ou comunicação de dados. É preciso, entretanto deixar claro, que nem toda conduta lesiva praticada contra ou através de computadores será crime informático.

Por tal conceito, possível notar que a doutrina diverge, pois alguns entendem que o conceito abarca delitos dolosos e culposos, bem como os comissivos e omissivos, ao passo que outros defendem o posicionamento de que se trata apenas de crimes virtuais aqueles que tenham em seu bojo o elemento DOLO.

Contudo, vale destacar, que a doutrina majoritária entende que estamos diante de um crime de meio, posto que o agente faz uso de um computador, para chegar ao fim, ou seja a consumação do delito.

Há ainda conceito bastante utilizado que é aquele elencado pela Organização para a Cooperação Econômica e Desenvolvimento da ONU, senão vejamos: O crime de informática é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento automático de dados e/ou transmissão de dados.

Tal conceito se mostra como um dos melhores, no entanto comporta críticas doutrinárias. Em que pese estar inserida nele a expressão “conduta não ética”, a mesma não carrega compatibilidade com o ordenamento brasileiro, até por que, partimos de um pressuposto de que todo crime, tipificado, com pena cominada, traz carga antiética, isto é, não faria sentido as normas penais não trazerem consigo o fundamento de repulsa da sociedade. Logo, é notório que tal conceito já seria bem completo sem tal expressão.

A doutrina costuma trazer os motivos que levam um indivíduo a realização de tais delitos, e são muitos, mas podemos exemplificar alguns, como a espionagem profissional, em que uma empresa contrata especialista (Hacker), com a finalidade de adentrar o sistema da concorrência para descobrir seus planos e estratégias, bem como se apropriar de seus programas.

Outro motivo que leva o agente a praticar tais crimes é o proveito próprio, ocasião em que o delinquente invade sistemas no intuito de obter vantagens ilícitas, como roubar dinheiro, fraudar sistemas, cancelar dívidas, etc.

A vingança também é motivadora, quando por exemplo um funcionário é demitido de uma empresa, porém não tem seu acesso ao sistema cancelado de imediato, e por isso se utiliza dessa falha para causar prejuízos a sua ex contratante.

É cediço que a curiosidade e a busca de aventuras também movem aqueles que invadem sistemas apenas para descobrir como eles funcionam.

Por fim, existem aqueles delinquentes que praticam esses tipos de crimes, impulsionados tão somente pela maldade e prazer que sentem pela destruição.

3.1 Classificação dos Delitos Informáticos

Esses crimes podem ser classificados em três grupos distintos, quais sejam o grupo dos crimes virtuais puros ou próprios, o grupo dos crimes virtuais impuros ou impróprios, bem como o grupo dos crimes virtuais mistos.

3.1.1 – Crimes virtuais puros/próprios: nesta categoria, se incluem os crimes cometidos, onde o único meio utilizado para a consumação delitiva é o computador.

Segundo Túlio Vianna (2003, p. 40-41), trata-se de delitos virtuais puros, os seguintes:

> Aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados). Além do delito de acesso não autorizado a sistemas computacionais há ainda outras modalidades de crimes que têm como objeto a inviolabilidade dos dados informatizados e, portanto, podem ser classificados como delitos informáticos próprios (puros).

Logo, se materializam apenas no mundo virtual, ou seja, não há exteriorização no mundo real. Assim é toda conduta ilícita que tenha por exclusivo objetivo o sistema computadorizado. Aqui, o agente quer atingir o computador, seus sistemas e dados contidos nele.

Nesta categoria se enquadram os Hackers, que são pessoas com amplo conhecimento técnico e cientifico na área da informática, que se utilizam disto para invadir sistemas ou prejudica-los.

3.1.2 – Crimes Virtuais Mistos: Segundo Guilherme Guimarães: “são aqueles em que o uso da internet ou sistema informático é condição *sine qua non* para a efetivação da conduta, embora o bem jurídico visado seja diverso ao informático”. Aqui se encaixam, por exemplo, as condutas de Hackers que se utilizam da internet para realizar no *internet banking* transferências de valores ilícitas.

3.1.3 – Crimes Virtuais impuros/impróprios: Nestas hipóteses, o agente utiliza o meio, que é o computador, com o fim de produzir resultado naturalístico, que se exteriorize no mundo real. Segundo Rita de Cássia Lopes da Silva (2003, p. 97):

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

Logo, extrai-se que a lesão afeta bem jurídico diverso do sistema informático, causando resultados no mundo real.

3.2 Deep Web

Trata-se de palavra de origem norte-americana, que quando traduzida significa “internet profunda”, local onde o usuário não encontra limites para seus atos, visto que não há filtros, logo, imagens de extrema violência, por exemplo, podem ser incluídas neste meio, que não haverá qualquer crivo.

A característica mais perigosa desse âmbito virtual é, sem sombra de dúvidas, o anonimato, logo quem se utiliza da Deep Web é dificilmente rastreado e localizado, tendo em vista que as ferramentas utilizadas neste ambiente são usadas para tornar praticamente impossível a identidade e localização do utente.

Não se sabe ao certo qual a origem da também conhecida como Dark net, alguns dizem que fora instrumento criado pelo exército japonês, com o intuito de resguardar informações deveras sigilosas, de maneira codificada, em rede anônima.

Outros defendem que o surgimento desta rede veio de criação chinesa, com a finalidade de navegar em sites, que o governo proibia a entrada.

Contudo, a expansão deste sistema se deu com “The Onion Routing”, um sistema de comunicações secreto criado pelo Laboratório de Pesquisas da Marinha dos Estados Unidos, que objetivava enviar dados e análises de sistemas anonimamente, ocasião em que disponibilizou tal sistema para quem quisesse fazer uso dele.

Atualmente, a Deep Web se perfaz num mundo virtual obscuro, com obstáculos para o acesso, e caracterizado pelo anonimato de seus usuários, que notadamente, se utilizam deste meio para praticar os mais diversos ilícitos.

Trata-se de qualquer conteúdo da internet que não pode ou não é localizado através de mecanismos básicos de pesquisa como o Google. Note que se mostra como um conteúdo invisível, tudo o que se encontra em seu interior, não é de total acesso a qualquer pessoa.

De acordo com Michael K. Bergman:

> Sites projetados propositalmente, mas que não se teve o interesse de registrá-lo em nenhum mecanismo de busca. Então, ninguém pode encontrá-los! Estão escondidos. Eu os chamo de Web Invisível.

Vale anotar que a Deep Web é ambiente muito extenso, quase que 500 vezes maior que a internet convencional (surface web), além de ser divida em camadas, quanto mais profundo o acesso, existem mais obstáculos para adentrá-los e maior o sigilo das informações.

Nessa toada, faz-se, comumente uma comparação entre um iceberg e o mundo virtual, em que a camada visível é a internet convencional, chamada de surface, e a parte muito maior que se encontra submersa corresponderia a Deep Web.

Para acessar as informações ali presentes, é preciso alterar as configurações de conexão, bem como utilizar navegador com capacidades específicas, por exemplo o TOR (The Onion Router), isso por que o conteúdo que ali

se encontra está hospedado em diversos bancos de dados, e não pura e simplesmente em uma página.

Ademais, é possível contratar inúmeros serviços na Dark net, a maioria deles de conteúdo antijurídico, como por exemplo, quando um usuário faz um pagamento para assistir ao vivo alguém ser torturado.

Nessa perspectiva, o utente consegue acessar este mundo sombrio da internet através de seu aparelho telefônico smartphone, o que no caso é bem simples, basta baixar o aplicativo “orfox” na loja virtual de aplicativos que contém sistema capaz de camuflar a rede, possibilitando a conexão direta ao TOR.

Como já amplamente abordado, aquele que ingressa nesta web busca privacidade, fornecida pelo anonimato, o que faz com que se disseminem práticas ilícitas, no entanto, há lado positivo na utilização desta ferramenta, por exemplo, nesse ambiente é possível encontrar obras e livros que estavam perdidos ou ainda proibidos, logo se mostra como enorme fonte de disseminação de conhecimento.

4 DOS CRIMES PRATICADOS E AUXILIADOS PELO ANONIMATO

É cediço que a revolução tecnológica impulsionou a potencialização dos crimes virtuais, grande parte desses crimes é praticada com a internet ou a utilização de computadores.

Note-se, o criminoso acompanha a sociedade, e ao haver a migração de várias atividades para o ambiente sistêmico, o cidadão delinquente irá perquirir este mesmo percurso. O ponto crucial da prática dos delitos cibernéticos está vinculado à camuflagem, que se perfaz na dificuldade de se identificar o agente.

Diante disso, é possível cometer diversas modalidades de ilícitos, notadamente na Deep Web, vejamos:

4.1 Tráfico de Drogas

Como se sabe a partir do século XX o mundo iniciou uma guerra às drogas, no intuito de combater veemente sua venda e utilização. Contudo, é de se

esclarecer que não houve êxito, ao contrário, não houve controle nessa comercialização e pior, desde então quando se fala em tráfico, já desde logo se associa esta atividade à violência perpetrada pelos Estados contra aqueles que são usuários, bem como aqueles vendedores.

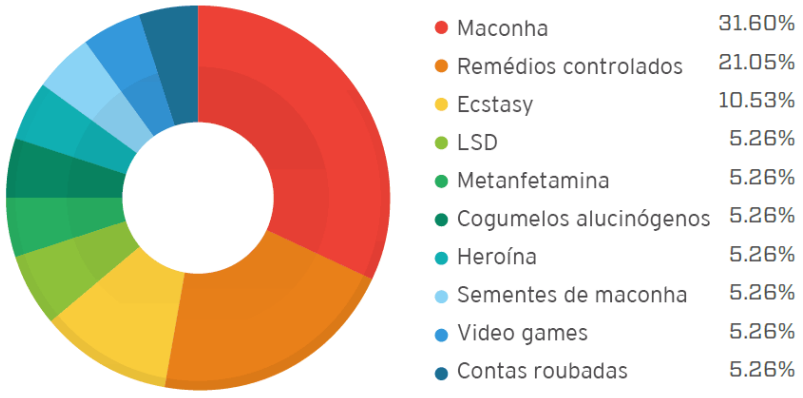
Com a revolução tecnológica, essa guerra passou a existir também no ambiente virtual, assim como no ambiente silencioso da Dark net.

Existem, nesse mundo virtual sombrio, alguns sites especializados na venda de drogas, que além de tudo, garantem facilidade ao comprador e ao vendedor, decorrente do sigilo.

Este mecanismo de venda de substâncias ilícitas funciona como qualquer e-commerce, onde traz estrelas aos melhores vendedores, fóruns de debate, onde se esclarecem quaisquer dúvidas, garantia de atendimento ao cliente, além de todo pagamento ser realizado através de bitcoins.

Bitcoins são as criptomoedas utilizadas na internet em geral, sobre as quais não recai qualquer regulação estatal. Ademais, por não ser controlado por nenhuma entidade financeira, seu valor de mercado é sempre variante. O usuário pode adquiri-la através da troca por dinheiro real, em seu computador ou smartphone. Veja, seu valor se altera de acordo com a lei de oferta e procura, ou seja, quanto maior a busca pela mesma, mais alto será seu preço.

Segundo pesquisa realizada pela Trend Micro, a droga mais procurada na Deep Web é a maconha, seguida de remédios controlados como por exemplo o Rivotril, que é medicamento de tarja preta, e que só é possível comprar com receita médica e ecstasy, senão vejamos:



Divisão de fornecedores, baseada em dados de 3 de junho de 2015

Através da leitura do gráfico, é possível notar que o comércio mais movimentado neste submundo é exatamente a venda de drogas.

Importante mencionar uma importante evolução investigativa nesse âmbito que ocorreu em 2013. O FBI, através de seus agentes de repressão às drogas, conseguiu fechar as portas de página da Deep Web que chegou a faturar 1,2 bilhões de reais, conforme mostra a notícia abaixo:

> Oficiais de repressão às drogas dos Estados Unidos conseguiram tirar uma pedra que estava em seu caminho há tempos. Na quarta-feira (02), o FBI derrubou o popular site de comércio Silk Road e apresentou acusações contra Ross William Ulbricht. O governo afirma que Ulbricht era quem comandava a página desde janeiro de 2011, sob o pseudônimo de "Dread Pirate Roberts".
> A Silk Road funcionava como uma espécie de Ebay de drogas e outras mercadorias ilegais, servindo como um mercado anônimo que conecta compradores e vendedores, e completo por um sistema de custódia para reduzir o risco de transações.
> As autoridades vinham tentando encerrar a Silk Road há anos, mas, até agora, revelou-se uma tarefa bem difícil. O site se escondia profundamente na Darknet - o lado mais oculto e obscuro da Web, e somente era acessível com o uso do software de anonimato Tor e da rede. A página também contava com Bitcoins para permitir que compradores e vendedores trocassem dinheiro sem a necessidade de revelarem suas identidades.

A derrubada do maior site de venda de drogas disponível na Deep Web foi algo que assustou os usuários, posto que eles acreditavam estar totalmente camuflados e seguros por de trás desta rede.

Contudo, a vitória dos agentes de segurança não foi suficiente para inibir tal prática, e nos dias atuais ainda existe vasta gama de sites que oferecem tal serviço no mundo obscuro da internet.

4.2 Pornografia Infantil

Na Deep Web, outra forma do agente cometer ilícitos, é se valendo do mercado negro de pornografia infantil. Portanto os criminosos se favorecem do anonimato para postar e reproduzir fotos e/ou vídeos que possuam este conteúdo.

A lei n° 8.069/90 (Estatuto da Criança e do Adolescente) penaliza a conduta de expor imagens de crianças e adolescentes em cenas de sexo, vejamos:

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008)
>
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008)
>
> § 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena. (Redação dada pela Lei nº 11.829, de 2008)

Em que pese a legislação brasileira tipificar condutas como essa, quando o delito é perpetrado no âmbito da Deep Web, há grande dificuldade de se chegar ao autor e sua identidade, haja vista, que ele se encontra escondido, camuflado por trás de inúmeros ips.

Patrícia Peck Pinheiro (2010, p. 300-301) anota tais dificuldades:

> Para que se encontre o agente que praticou uma das condutas previstas nos citados artigos, muitas das vezes é necessária a quebra de sigilo, tendo em vista que será preciso rastrear aquele que praticou o ilícito, e após conseguir localizar o culpado, é necessário muitas das vezes que sejam as provas eletrônicas analisadas por uma perícia técnica rigorosa, para que sejam aceitas em processos.

Anote-se que além de todas essas dificuldades de se encontrar o criminoso, outra questão que se vislumbra aqui é a da Territorialidade. Por vezes a investigação é eficaz, ocasião em que se identifica o delinquente, no entanto, geralmente os sites escondidos no submundo virtual estão hospedados em provedores estrangeiros, países os quais impedem a retirada deste tipo de conteúdo em razão da livre manifestação de opinião que é preceito fundamental.

Porém, em 2018 o Brasil conseguiu grande avanço nas investigações de tais delitos, realizando a Operação Dark Net. A Polícia Federal deflagrou tal operação no ano de 2016, e desde então vem desenvolvendo metodologia para investigar e identificar usuários da Deep Web.

Apurar diversos responsáveis por tal conduta foi possível, pois os investigadores se infiltraram no submundo, e fizeram isso se valendo da Lei de Organizações Criminosas (que permite a infiltração). Deste modo, foram investigados os mais frequentes usuários que compartilhavam este tipo de conteúdo.

Cumpre salientar que a citada operação cumpriu mais de 100 mandados de busca e apreensão, além de inúmeras prisões no país, o que demonstra a evolução investigativa no Brasil, que, contudo, está longe de por fim, de uma vez por todas, o cometimento de tal crime.

5 DO DIREITO COMPARADO

Ao falar em direito “alienígena”, percebe-se que há certa evolução com relação ao ordenamento jurídico pátrio, isto é, algumas legislações estrangeiras se encontram a frente do Brasil, quando o assunto é regulamentação a respeito dos crimes virtuais. Podemos destacar alguns países que já possuem regulamentação sobre o tema, quais sejam, Estados Unidos, alguns países integrantes da União Europeia, Canadá, Argentina e Colômbia.

Notadamente em Portugal, Itália e Estados Unidos, as condutas criminosas cometidas através da Rede Mundial de Computadores, ou ainda pela utilização de artefatos de informática, são capituladas e tipificadas.

Sobre o assunto, Lucca e Simão Filho (2000, p. 233) discorrem:

> No direito Português é punido aquele que interfere no resultado do tratamento de dados mediante estruturação incorreta do programa, ou interfere de qualquer modo no processamento com intenção de obter para si ou para outrem enriquecimento ilegítimo, causando prejuízo alheio. No direito italiano, a fraude informática prevista no art. 640 do Código Penal, consiste em alterar o funcionamento de um sistema informático ou telemático para obter proveito indevido para si ou para outrem. E, ainda, nos Estados Unidos da América o Código Penal Federal estabelece exaustiva e detalhadamente as infrações relacionadas ao uso do computador e ao acesso aos sistemas de informática, sujeitos a severas penalidades nos arts. 1.029 e 1.030, sob o nome genérico de fraude [fraud].

Nota-se que o Direito Português, em outras palavras, tipifica uma conduta que pode ser denominada como Estelionato Virtual, pois se trata de um crime contra o patrimônio, onde há o emprego de ardil ou artifício capaz de induzir em erro a vítima, veja que no caso há uma incorreta estruturação do programa. Existe uma única diferença entre o estelionato normal e o praticado no mundo virtual, que se encontra no *modus operandi,* ou seja, ao passo que um ocorre no mundo físico e real, o outro faz uso da internet, e ocorre no mundo virtual.

Neste caso o usuário, normalmente, tem ampla noção na área, ocasião em que busca criar vários meios ardilosos para ludibriar de forma simples sua vítima. A esses especialistas damos o nome de “Crackers”, que são aqueles que possuem intenção de enganar terceiros, a fim de garantir indevidas vantagens através do uso da internet, que invadem sistemas, ou ainda os configuram de forma que possam adentrar facilmente e assim obter vantagem ilícita em prejuízo de outrem.

Nessa mesma toada, o Direito Italiano prevê a Fraude Informática que objetiva punir aqueles que alteram sistemas informáticos ou telemáticos com o intuito de conseguir vantagem indevida.

Possível notar que os Estados Unidos da América possuem grande preocupação no tocante ao tema, posto que exaustivamente capitulam e tipificam tais crimes em seu Código Penal Federal, trazendo o crime e as sanções correspondentes. Sobre o tema, Roque (2007, p. 311) anota:

> Nos Estados Unidos, legisladores federais e estaduais reconheceram os riscos associados com a nova tecnologia e estão respondendo com leis cada vez mais sofisticadas. Os crimes federais relacionados com o uso do computados, os EUA, estão contidos na Seção 1030 do Título 18 do Código dos Estados Unidos. Esta lei, especificamente, penaliza as condutas do uso sem autorização e alteração ou destruição de dados.

Vale salientar que os Estados Unidos sempre foram extremamente vanguardistas a respeito do tema, para demonstrar com exemplo, o estado da Flórida, possui legislação específica para crimes praticados através de computadores, desde 1985.

Em linhas gerais, a extrema preocupação norte-americana com os delitos praticados no âmbito virtual se justifica por que uma das primeiras manifestações virtuais ilegítimas surgiu lá, quando Robert Morris, estudante de pós-graduação, iniciou trabalho em programa informático, onde explorava defeitos de segurança contidos neste, com o intuito de demonstrar tais falhas, ademais criou os “*worms”,* vírus que tem capacidade de se expandir e ocupar parte do sistema computacional.

Acontece que, em que pese o único objetivo de Morris ser a demonstração das falhas contidas no sistema de segurança, a experiência começou a tomar grandes proporções e o vírus começou a se expandir e infectar várias máquinas, causando grandes prejuízos na época.

A partir disso, os EUA iniciam um verdadeiro combate à criminalidade informática, tanto no âmbito federal, com a Lei de Proteção aos Sistemas Computacionais (*Federal Computer System Protection Act of 1981*), que possuía objetivo de prevenir, bem como punir as fraudes cometidas através do uso de computadores, bem como na seara estadual. Surge ainda lei que dispõe de regulamentação a respeito de transferência eletrônica de fundos (*Eletronic Funds Transfer Act)* em 1982.

Por fim, cumpre demonstrar a principal lei que entrou em vigor nos EUA, e veio com o objetivo de responsabilizar criminalmente aqueles que cometem condutas ilícitas, no âmbito virtual (*Computer Fraud and Act* – Lei de Fraude e Abuso Computacional – datada de 1986), que visa aumentar a segurança e proteger a acessibilidade dos sistemas, para que criminosos não tivessem acesso a segredos nacionais.

6 CONCLUSÃO

Conclui-se que o espaço cibernético é extremamente vasto e capaz de trazer à tona características pessoais do usuário que estão ocultas, e que em virtude do anonimato, lhes dá certa coragem para demonstrá-las neste meio, especialmente no mundo virtual obscuro, a Deep Web.

Com isso, a prática delituosa no ambiente virtual vem crescendo em grande proporção a medida que as relações se tornam cada vez mais virtualizadas. Nota-se que o direito não é rápido o bastante para acompanhar a revolução tecnológica, e consequentemente nos vemos diante de uma falta de regulamentação e repressão por parte dos entes estatais.

Atualmente, qualquer pessoa pode se transformar em um criminoso cibernético, haja vista a facilidade de acesso a internet, bem como a dificuldade de identificação e rastreamento desse delinquente.

Isso demonstra que devem surgir novas formas de proteção aos bens jurídicos, para que o Direito Penal não esteja em descompasso com a atual realidade.

Tal deficiência acaba refletindo diretamente no Direito Processual Penal, que encontra, na persecução, obstáculos em matéria probatória, bem como na aplicação de medidas cautelares. Contudo, como foi abordado, o Brasil já vem avançando nesse sentido, elaborando profundas e extensas investigações, com o objetivo de deter e punir tais criminosos.

Também fora explanado que a Convenção de Budapeste trata especificamente destes delitos, e foi assinada por diversos países da Europa. Veja que é opção para o Brasil na tentativa de combate destes crimes, pois esta Convenção traz em seu bojo, definições, conceitos, protocolos e até mesmo aspectos procedimentais, que podem orientar o sistema jurídico brasileiro na batalha contra os crimes virtuais.

Após a realização desta pesquisa, conclui-se que se faz necessária imediata tipificação específica a respeito dos delitos informáticos, a fim de que o Brasil saia do retrocesso e se iguale a países mais avançados como os Estados Unidos.

REFERÊNCIAS BIBLIOGRÁFICAS

CHACOS, Brad. **FBI fecha site de drogas**. Ignow: 03 de outubro de 2013 Disponível em < http://idgnow.com.br/internet/2013/10/03/fbi-fecha-site-de-venda-de-drogas-silk-road-que-tinha-receita-de-us-1- 2-bilhao > Acesso em 04 de maio de 2019 às 17:23

BERGMAN, Michael K. **"The Deep Web: Surfacing Hidden Value"**. Disponível em< http://dx.doi.org/10.3998/3336451.0007.104 > Acesso em 01 de maio 2019 às 18:38

BRASIL. ECA- **Estatuto da criança e do adolescente**. Lei nº 8.069, de 13 de julho de 1990. Disponível em < http://www.planalto.gov.br/ccivil_03/leis/L8069.htm > Acesso em 04 de maio de 2019 às 18:07

FELICIANO, Guilherme Guimarães. **Informática e criminalidade: parte I: lineamentos e definições**. Boletim do Instituto Manoel Pedro Pimentel, São Paulo, v. 13, n. 2, p. 35-45, set. 2000. p. 42.

LUCCA, Newton De e Simão Filho, Adalberto [coordenadores] e outros. **Direito & Internet – Aspectos Jurídicos Relevantes**. Bauru: Edipro, 2000. p. 233

PINHEIRO, Reginaldo César. **Os cybercrimes na esfera jurídica brasileira**. In: Revista Eletrônica Jus Navigandi. Site: http://jus.com.br/revista/texto/1830/os-cybercrimes-na-esfera-juridica-brasileira Acesso em 29 de abril 2019 às 10:50h

PINHEIRO, Patrícia Peck. **Direito digital**. 4°. Ed. São Paulo: Saraiva, 2010.p.300 e 301

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004 p. 110

ROQUE, Sérgio Marcos. **Criminalidade Informática**. São Paulo: Adpesp Cultural, 2007 p. 311

SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**, 2003, p. 97

TREND MICRO. **Investigando a Deep Web**. Disponível em: < http://blog.trendmicro.com.br/investigando-a-deepweb/#.Vzibu_krLIU > Acesso em 04 de maio de 2019 às 16:49

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático: do acesso não autorizado a sistemas computacionais**. Rio de Janeiro: Forense, 2003.

CENTRO UNIVERSITÁRIO “ANTONIO EUFRÁSIO DE TOLEDO”. **Normalização de apresentação de monografias e trabalhos de conclusão de curso.** 2007 – Presidente Prudente, 2007, 110p.