CENTRO UNIVERSITÁRIO CURITIBA

FACULDADE DE DIREITO CURITIBA

ISADORA MARINA CASTELAN DE ALMEIDA PAGNOZZI

CRIMES VIRTUAIS: UMA ABORDAGEM JURÍDICA ACERCA DAS LIMITAÇÕES NO COMBATE AOS CRIMES CIBERNÉTICOS

CURITIBA

2018

ISADORA MARINA CASTELAN DE ALMEIDA PAGNOZZI

CRIMES VIRTUAIS: UMA ABORDAGEM JURÍDICA ACERCA DAS LIMITAÇÕES NO COMBATE AOS CRIMES CIBERNÉTICOS

Monografia apresentada como requisito parcial para obtenção do grau de Bacharel em Direito, do Centro Universitário Curitiba.

Orientador: RODRIGO RÉGNIER CHEMIM GUIMARÃES

CURITIBA

2018

ISADORA MARINA CASTELAN DE ALMEIDA PAGNOZZI

CRIMES VIRTUAIS: UMA ABORDAGEM JURÍDICA ACERCA DAS LIMITAÇÕES NO COMBATE AOS CRIMES CIBERNÉTICOS

Monografia aprovada como requisito parcial para obtenção do grau de Bacharel em Direito da Faculdade de Direito de Curitiba, pela Banca Examinadora formada pelos professores:

Orientador:_____

_____

Professor Membro da Banca

Curitiba, de de 2018.

A meus pais, Mauricio e Débora, que diante de todos os empecilhos impostos pela vida, me proporcionaram cursar o Ensino Superior sempre me apoiando e incentivando a concretizar meus objetivos.

A meus irmãos, Victória e Mondrian, razões do meu orgulho.

AGRADECIMENTOS

Agradeço primeiramente à minha família, meu baluarte, por todo o esforço desmedido empregado para a minha criação e amadurecimento, resultando na conclusão dessa fase da minha vida, e por todo o amor e paciência que dedicaram durante todos esses anos.

Ao Professor Rodrigo Régner Chemim Guimarães, que de boa vontade me orientou na realização desse processo, meus singelos agradecimentos.

Ao Fernando Peres, que de bom grado me concedeu seu tempo em entrevista e contribuiu com a realização desse trabalho, meus sinceros agradecimentos.

À minha irmã, Victória, que me forneceu apoio e palavras de auxílio ao longo de todo esse projeto.

Ao Fernando Augusto Ogura, respeitável amigo, por ter sido essencial na minha formação e preparação para o caminho que me aguarda. Agradeço imensamente.

Agradeço a todos os professores do Unicuritiba - Centro Universitário Curitiba, que me instruíram com maestria e preparo.

Por fim, agradeço a todos que de algum modo, contribuíram na minha formação, e aos meus amigos que tive a oportunidade de conhecer na graduação e que permaneceram do meu lado durante essa trajetória.

“O estudo em geral, a busca da verdade e da beleza são domínios em que nos é consentido ficar crianças toda a vida.”

(ALBERT EINSTEIN)

RESUMO

O presente trabalho tem por objetivo analisar o surgimento e a evolução da tecnologia e como ela afeta a vida em sociedade, principalmente no âmbito da criminalidade, de forma que surgem os crimes virtuais. Serão analisados aspectos de como ocorrem os crimes virtuais, bem como a classificação dos tipos de crime cibernéticos e o perfil dos criminosos. Tem por objetivo adentrar o universo da *deepweb*, a fim de se obter conhecimento acerca dos crimes que ocorrem na *internet*. Pretende analisar também quais dificuldades são encontradas na instrução probatória e na identificação do agente, e como a legislação nacional e internacional é aplicada nos *cyber crimes*, para compreender como os países se comportam diante de tal criminalidade e qual a importância do ordenamento jurídico coerente com a realidade para a eficaz aplicação das normas.

Palavras-chave: Crimes virtuais. *Internet. Deep Web.* Legislação. Criminosos virtuais. Instrução probatória.

SUMÁRIO

INTRODUÇÃO

É de notório saber que o avanço na tecnologia marcou a história da humanidade e vem se tornando cada vez mais uma ferramenta necessária e indispensável para os atos da vida comum. Porém, a facilidade e a rapidez com que as informações são compartilhadas através da internet ocasionou grande dificuldade no controle das atividades dos usuários, uma vez que esta permite o anonimato.

O surgimento de novas práticas ilícitas torna necessária a intervenção do Direito Penal na evolução dessas tecnologias, a fim de garantir a aplicação das normas penais de forma eficaz, abrangendo todo o universo criminoso existente na sociedade da informação.

É diante dessa realidade fática que o estudo do tema se torna mais relevante, na medida em que compreende-se em quais condições a legislação brasileira se encontra preparada para lidar com esse tipo de prática delituosa.

Ademais, é imprescindível o estudo de como é feita a investigação de crimes cuja identificação do agente se torna muito mais difícil visto a possibilidade do anonimato, e como se dá a instrução probatória e julgamentos nesses casos.

Entender o que são crimes virtuais e suas características auxilia na compreensão do tema, assim como para elaborar métodos de aperfeiçoamento nos meios investigativos e probatórios.

O primeiro capítulo do presente trabalho abordará o surgimento e a evolução da tecnologia na vida social e quais os primeiros delitos digitais que indicaram a necessidade de legislação específica.

O segundo capítulo considerará a classificação, bem como os principais tipos de crimes virtuais e como ocorrem, além de analisar quem são os criminosos cibernéticos.

O terceiro capítulo estudará parte do universo da *Deep Web*, como acessá-la e de que forma ocorrem crimes nesse meio. Nesse capítulo consta ainda uma análise das transações financeiras através das moedas virtuais e como são utilizadas como mecanismo para facilitação na prática de delitos.

O quarto capítulo abordará como devem ser instruídos de provas os processos que tratam de tais crimes e as principais dificuldades existentes na identificação do agente e na obtenção de provas que comprovem a autoria.

O quinto e sexto capítulo analisarão as leis nacionais e internacionais aplicáveis aos crimes virtuais e qual a real efetividade no resultado de punir ou inibir a prática delituosa por meio digital. Além disso, é pertinente estudar qual o posicionamento legal quando os crimes são comandados em outros países e executados em território nacional e qual a competência específica nessas circunstâncias.

2. A *INTERNET* E O DIREITO

O Direito como ciência social deve acompanhar a evolução do ser humano e da sociedade na qual ele está incluído, atendendo as necessidades de normas que regulamentam as condutas das relações humanas.

Com o surgimento da internet e a disseminação da cultura da globalização, a sociedade caminhou a "passos largos" em direção a uma geração dependente da informática, substituindo muitos atos da vida comum pelos sistemas informatizados. Devido à simplicidade e a rapidez com que a internet executa determinada função, o ser humano cada vez mais preferiu as ferramentas virtuais a tal ponto que, hoje, se uma pessoa não possui conta de e-mail ou rede social, é considerada de alguma forma "isolada" da sociedade**.** A respeito disso, Maciel Colli posiciona-se:

> O uso da internet possibilitou a superação da dificuldade ocasionada pela distância territorial e pela limitação comunicativa entre as pessoas em locais distantes. A voz e o papel foram desbancados do ranking instrumental de intercâmbio de mensagens. O texto exibido nas telas de computadores, produtos de linguagem binária interpretada e transmutada pelas plataformas dos computadores, elimina a distância e o tempo.[1]

Para entender essa evolução, é válido especular de onde surgiu a internet. A palavra significa "rede internacional" - advindo da união dos termos em inglês Inter (internacional) e net (rede) - e surgiu no fim do século XX. Inicialmente, despontou como ferramenta para internalizar as comunicações em casos de guerra e para estudar as relações entre ser humano e máquinas. Porém, o uso dos computadores era limitado a poucos usuários, pois basicamente era utilizado para uso militar e científico. Somente

---

[1] COLLI, Maciel. **Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos**. Curitiba: Juruá Editora, 2010, p. 39.

na década de 1990 a internet tornou-se uma ferramenta pública e de uso indispensável para a sociedade. Concomitantemente com a evolução tecnológica, e devido à sociedade substituir seus atos físicos pelos atos virtuais, surgiu o problema da criminalidade virtual. De acordo com Gustavo Têsta Correa, “A internet é um paraíso de informações, e, pelo fato de essas serem riqueza, inevitavelmente atraem o crime. Onde há riqueza, há crime."[2] A internet é um mecanismo tão recente e que modificou tão drasticamente a vida do ser humano que pode-se dizer que a humanidade ainda não se adaptou à maneira de viver do século XXI. Em uma era informatizada, o Direito não acompanha a realidade fática da sociedade, principalmente tratando-se de regulamentar as condutas humanas.

A partir de 1980 começou a propagação de diferentes tipos de crimes ocorridos virtualmente, tais como pirataria, transmissão de vírus, pedofilia, invasão de sistemas, entre outros. Conforme tais práticas foram tornando-se expressivas surgiu a necessidade de cuidados com a segurança virtual e, consequentemente, a interferência do Estado para regulamentar tais condutas.

O maior estímulo aos criminosos para o cometimento de crimes na internet é a crença de que lá estão mais protegidos. Isso acontece porque na própria sociedade não existe essa cultura de prevenção de possíveis ataques de criminosos. Talvez por ser um problema relativamente novo na sociedade não se imagina que, ao proteger os computadores e dispositivos, as condutas ilegais serão inibidas.

O Brasil começou a preocupar-se com tais questões recentemente. A promulgação da Constituição em 1988 estabeleceu que as questões de informática deveriam ser de competência do Estado. Damásio de Jesus complementa:

> O marco Civil da Internet é considerado a “Constituição da Internet”, garantindo direitos e deveres a todos os autores da Internet brasileira [...]. Fruto de um projeto nascido em 29 de outubro de 2009, [...] o Marco Civil foi uma

[2] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** 5 ed**.** São Paulo, Saraiva, 2010.

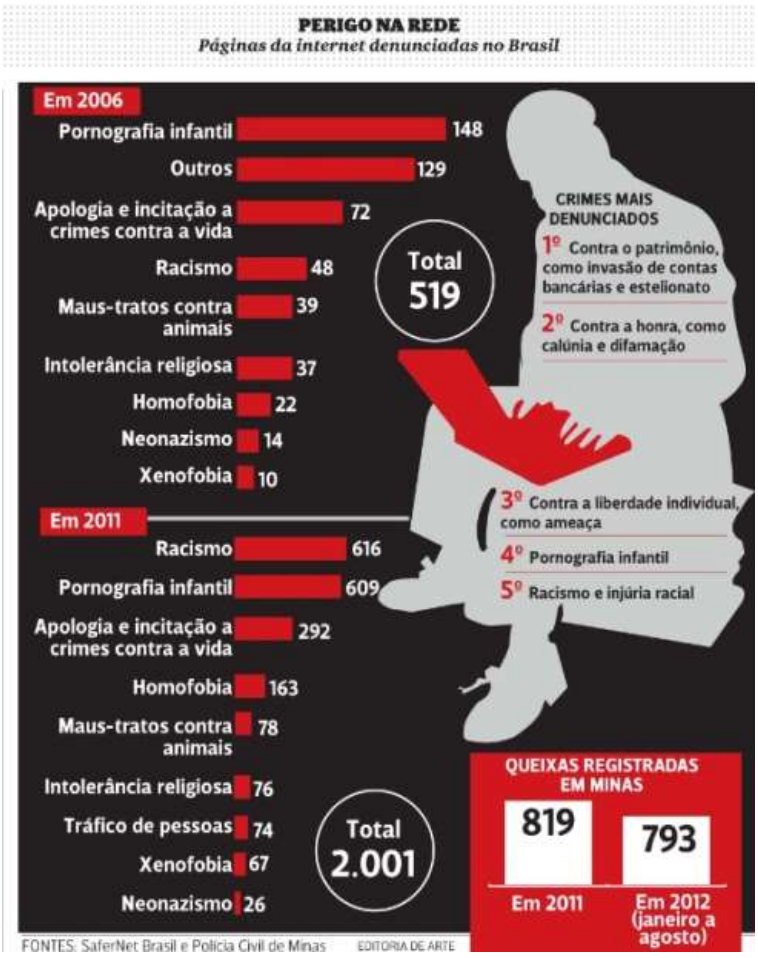
> construção colaborativa, disponível para consulta pública entre novembro de 2009 e junho de 2010, tendo recebido mais de duas mil contribuições.

Tal projeto de lei, após passar pela participação popular, ingressou no Congresso Nacional por iniciativa do Poder Executivo e foi sancionada pela Presidenta Dilma Rousseff em 2014, como Lei 2.216. Além disso, em 2012, com a promulgação das Leis 12.735 e 12.737 - as chamadas Leis de Crimes Informáticos - o legislativo tentou tipificar as condutas ilícitas cometidas no meio virtual.

Desde a década de 1970 existe menção à figura do hacker no âmbito criminal, à medida que a Internet foi se popularizando. Faz parte do entendimento a respeito do tema compreender de que forma surgiram os crimes virtuais. Uma vez que a Internet tornou-se alvo do interesse público, pode-se esperar que nela desenvolvam-se condutas criminosas, visto que o ser humano tende a criar meios ilícitos para todas as atividades do seu dia a dia. Dessa forma, depara-se com a figura do sujeito que pratica tais condutas, o qual pode-se chamar de “ciber criminoso”, conceito que será abrangido mais adiante.

3. CRIMES VIRTUAIS

Assim como as práticas de crimes comuns se aperfeiçoam com o tempo, os crimes virtuais também tomam novas formas através do avanço tecnológico que permite e facilita suas práticas. Com o grande número de usuários na internet - que ultrapassa 3 bilhões -, é cada vez mais difícil identificar os agentes que cometem crimes na internet. A Safernet Brasil[3] registrou o recebimento e processamento de 3.861.707 denúncias anônimas ocorridas no período de 11 anos, o que demonstra o alto índice de crimes virtuais.



[3] Disponível em: <http://indicadores.safernet.org.br/indicadores.html>. Acesso em: 15 de setembro de 2017.

Muito embora os primeiros casos de delitos praticados tendo como ferramenta o computador - elemento essencial para a caracterização do cibercrime - tenham sido datados na década de 1950, não existe uma data ou fato específico que caracterize o surgimento do primeiro vírus, uma das primeiras formas de delitos virtuais praticados na história da internet. Inclusive a doutrina diverge com relação ao primeiro delito na era informatizada. Para uns, ele teria ocorrido no Instituto de Tecnologia de Massachussets - Estados Unidos - em 1964, praticado por um aluno. Para outros na Universidade de Oxford em 1978, onde um aluno teria roubado informações da rede acerca de uma prova universitária.[4] Até então não existiam leis que regulassem os crimes virtuais nos Estados Unidos, sendo a Flórida o primeiro Estado a criar leis sobre crimes virtuais.

O primeiro estudo acadêmico realizado sobre crimes cibernéticos ocorreu na Europa, por volta de 1976, apresentado por Ulrich Sieber.[5] Já no Brasil, os primeiros indícios de crimes virtuais ocorreram através do *phising,* no ano de 1999, com o roubo de senhas bancárias. Depois disso, iniciou-se uma onda de crimes envolvendo *e-mails* de conteúdo sexual e chantagens, bem como vídeos encontrados na internet de sexo infantil explícito. Tais ocorrências alarmaram a população quanto à necessidade de legislação específica. Mediante isto, a doutrina começou a se manifestar conceituando e estudando mais profundamente os crimes virtuais, trazendo a base para o entendimento de tais delitos.

A definição de crimes virtuais é algo recente comparado aos conceitos de crimes tradicionais estudados há muito tempo. Um dos mais conhecidos é o de Krone (2005), que define crimes virtuais como delitos que vão desde atividades criminosas contra dados até as infrações de conteúdo e *copyright*[6]. Porém, para Geese-Zeviar[7] (1998), a

---

[4] JESUS, Damásio de; MILAGRE, José Antonio. **MANUAL DE CRIMES INFORMÁTICOS.** São Paulo: Saraiva, 2016.

[5] Disponível em: < http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>. Acesso em : 4 de setembro de 2017.

[6] KRONE, Tony. ***High Tech Crime Brief***. *Australian Institute of Criminology*. Canberra, Australia. ISSN 1832-3413. 2005.

[7] ZEVIAR-GEESE, G. ***The State of the Law on Cyberjurisdiction and Cybercrime on the Internet.*** *California Pacific School of Law. Gonzaga Journal of International Law*. Volume 1. 1997-1998.

definição é mais ampla, e inclui atividades como a fraude, o acesso não autorizado, a pornografia infantil e o assédio na internet. Este trata-se de um crime de meio, ou seja, um crime que se utiliza do meio virtual. Moisés Cassanti, em sua obra “Crimes virtuais, vítimas reais”, conceitua crimes virtuais como "toda atividade onde um computador ou uma rede de computadores é utilizada como ferramenta, base de ataque ou como meio de crime".[8] Nas palavras de Ivette Senise Ferreira, crimes cibernéticos são:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial.[9]

Pode-se dizer, portanto, que os crimes virtuais são todos aqueles que ocorrem através ou com o auxílio de meios virtuais, sendo utilizados para a prática de atos ilegais, servindo para renovar a execução de antigos delitos ou para criar novos crimes. Os criminosos virtuais utilizam vários métodos distintos para a prática de seus crimes.

3.1 O CIBERCRIMINOSO

O agente que pratica conduta típica, antijurídica e culpável constitui os elementos de crime, e será processado, julgado e punido por suas condutas. O mesmo ocorre com o sujeito que pratica tal ato virtualmente.

---

[8] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas reais.** Rio de Janeiro: Brasport, 2014, pg.3.

[9] FERREIRA, Ivette Senise. **Direito & Internet: Aspectos Jurídicos Relevantes**. 2 ed. São Paulo: Quartier Latin , 2005, p.261.

O *cibercriminoso*, como sujeito ativo, foi visto por muitos como sendo unicamente o jovem, uma vez que a internet é relativamente recente. Já outros passaram a ver qualquer pessoa que possua conhecimento informático, capaz de acessar um computador ou dispositivo, como um criminoso em potencial.

Os agentes responsáveis pelas práticas dos crimes virtuais podem ser tanto pessoas possuidoras de um conhecimento técnico mais profundo a respeito da internet - *hackers* ou *crackers* -, quanto usuários comuns que, através de suas condutas virtuais, cometem crimes contra outros usuários. Portanto, não se pode traçar um perfil estigmatizado sobre o *cibercriminoso*.

3.1.1 *Hackers X Crackers*

Dentre os *cibercriminosos* que possuem conhecimento técnico e especializado a respeito da internet e dos métodos de se obter informações por meios escusos, encontramos os famosos *Hackers* que, muito embora estejam sempre associados ao roubo de informações e dados, na visão dos especialistas em informática não constituem os verdadeiros criminosos da Internet. Esses seriam denominados *Crackers,* - do termo em inglês “to crack”, que significa para quebrar - ou seja, pessoas que utilizam de seu conhecimento informático para quebrar sistemas de segurança e roubar dados e senhas de acesso, bem como invadir redes de forma ilícita para fins criminosos.

Portanto, o termo *hacker* serve para definir um programador de sistemas, que não necessariamente tem por objetivo causar danos a outrem. Muito pelo contrário, o *hacker* de hoje é utilizado inclusive para investigar delitos virtuais e colaborar nas investigações e nos desenvolvimentos de softwares de segurança. Assim, podemos entender que *hacker* é apenas o gênero do qual o *cracker* é espécie.

3.2 CLASSIFICAÇÃO DE CRIME VIRTUAL

Há muitas classificações doutrinárias que definem os *cibercrimes*. Damásio de Jesus, por exemplo, separa os crimes virtuais em quatro categorias: próprios, impróprios, mistos, e mediatos. Para ele, crimes virtuais próprios são aqueles em que o sujeito utiliza necessariamente da ferramenta eletrônica para a prática do delito. Ou seja, são crimes que não podem se consumar sem o computador, uma vez que este caracteriza elemento intrínseco à prática do crime. São exemplos de crimes virtuais próprios: ataque de vírus e *malware*. Damásio ainda complementa: “Neles (crimes virtuais próprios), a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado”.[10]

Já os crimes virtuais impróprios são aqueles praticados com o auxílio do computador, quando este é utilizado para executar condutas já tipificadas no ordenamento jurídico como ilícitas. Isto é, a internet é usada como nova ferramenta para a prática de “velhos crimes”, como a pedofilia e o tráfico de órgãos. Damásio de Jesus explica:

> Os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.[11]

---

[10] JESUS, Damásio de; MILAGRE, José Antonio. **MANUAL DE CRIMES INFORMÁTICOS.** São Paulo: Saraiva, 2016, pg. 52.

[11] JESUS, Damásio de; MILAGRE, José Antonio. **MANUAL DE CRIMES INFORMÁTICOS.** São Paulo: Saraiva, 2016, pg. 52.

Os crimes virtuais mistos são aqueles complexos em que a legislação protege mais de um bem jurídico, ou seja, protege o bem jurídico informático e outro bem jurídico distinto. E por fim, os crimes virtuais mediatos tratam dos delitos praticados com o intuito de alcançar outro fim, que será consumado no mundo real. O exemplo citado por Damásio é do agente que utiliza do crime virtual para capturar dados da vítima e usa-os para desfalcar a conta corrente dela.

Considerados estes aspectos sobre a classificação, denota-se de relevante importância fazer breves considerações sobre como tais crimes ocorrem no meio virtual, e quais as formas mais comuns.

3.3 COMO OCORREM OS CRIMES VIRTUAIS

Os crimes virtuais podem ocorrer tanto pela prática maliciosa de um agente que visa roubar informações para fins criminosos quanto pelos atos de usuários contra outros usuários já tipificados pelo Código Penal. Alguns dos métodos mais comuns utilizados pelos *cibercriminosos* na execução de seus crimes são o *phishing*, o *trojan* e a engenharia social.

3.3.1 *Phishing*

Uma técnica virtual muito comum para o cometimento de crimes pela Internet é através do *"phishing"*, que significa pescaria. No caso, o criminoso encaminha *e-mails* e mensagens não solicitadas para a vítima, incentivando que ela acesse links de páginas

fraudulentas, faça *downloads* de arquivos de *malware* - vírus programado para coletar informações -, ou preencha formulários falsos, fornecendo ao invasor informações que serão úteis para chantagear a vítima ou até mesmo acessar senhas particulares de contas bancárias.

3.3.2. *Trojan*

O conhecido “Cavalo de tróia” é um arquivo aparentemente vindo de fonte segura, mas que contém um elemento malicioso que se alastra quando as vítimas abrem um programa ou arquivo sem se dar conta de que nele está o *trojan.* A grande dificuldade de identificar esse elemento reside na forma como ele se instala no computador da vítima. Através de programas funcionais - como jogos, protetores de tela - que são executados perfeitamente, a vítima acaba não tomando conhecimento da existência do problema. Enquanto isso, o cavalo de tróia trabalha executando funções como os *keyloggers* - ferramenta que captura tudo que a vítima digita, os cliques do *mouse, printscreens* de tela e da *webcam* -, que favorecem os interesses do invasor.

3.2.3. Engenharia Social

É o método utilizado para a exploração da vítima que possui como característica a enganação ou persuasão. Dessa forma, o criminoso se vale da confiança, da curiosidade ou do medo da pessoa para obter informações sobre ela ou conseguir que esta faça uma determinada ação em proveito próprio. É comum que o agressor faça-se passar por outras pessoas, um profissional ou uma instituição e, através de e-mails e

mensagens, conduz o ataque conforme adquire a confiança da vítima de que tal circunstância criada por ele é real.

3.3.4 *Sniffers*

São *softwares* usados para monitorar tráfego de dados e analisar possíveis problemas. Não são necessariamente utilizados de forma maliciosa, porém, eles captam todas as informações que passam por eles, inclusive senhas e usuários não criptografados. Podem ser instalados facilmente em qualquer computador que esteja conectado a uma rede aberta. Dessa forma, os *hackers* podem roubar dados, coletar informações sobre os usuários e espionar o tráfego da rede com o objetivo de obter senhas e dados de contas bancárias. Os *sniffers* não autorizados são praticamente impossíveis de se detectar, o que os torna mais perigosos, visto que a vítima provavelmente nem notará que está sendo espionada.

3.3.5 Crimes Contra a Honra

Existem diversas maneiras de invadir um computador. O problema é que essas invasões nem sempre visam causar danos apenas ao computador. Na verdade, a maior parte dos ataques ocorre para prejudicar o usuário. Notável que, com o avanço tecnológico, o homem tornou-se mais frágil e mais suscetível a práticas de delitos. Difamar, caluniar e denegrir a imagem das pessoas também pode ser caracterizado como crime virtual, uma vez que ocorre com o auxílio do computador, conforme já

explanado anteriormente. Os crimes contra a honra já estão previsto no capítulo V, Parte Especial do Código Penal.

Caracteriza-se a honra em objetiva e subjetiva. A honra objetiva é aquele juízo que os outros fazem de alguém, portanto, ao atacar a honra objetiva de uma pessoa interfere-se na maneira como o mundo verá aquele alguém. Já honra subjetiva é a maneira como cada um vê a si mesmo, ou seja, elemento que, através de seus valores, traz sentimentos de grandeza a cada um. Ao ferir a honra subjetiva, interfere-se na maneira como a pessoa enxerga a si mesma.

É muito comum encontrar casos de divulgação de fotos ou vídeos particulares de usuários sem a permissão deste, no intuito de constranger e expor determinada pessoa por vingança – por exemplo nos casos conhecidos como a vingança do *mouse*, em que geralmente ex-namorados divulgam vídeos com conteúdo sexual do ex-parceiro -, ou por questões de ódio e preconceito.

3.3.6 *Cyberbullying*

O *Cyberbullying* nada mais é do que a prática do *bullying* (atos de violência física ou psicológica que ocorrem de maneira repetida e intencional) pelo meio virtual, através de computadores, *tablets* e celulares. De acordo com Cassanti, *cyberbullying* é definido como:

> A ação intencional de alguém fazer uso das tecnologias de informação e comunicação para hostilizar, denegrir, diminuir a honra ou reprimir consecutivamente uma pessoa. Contrário do tradicional e não menos preocupante bullying, que é presencial, ou seja, as ações do agressor têm lugar certo, no cyberbullying o agressor não consegue presenciar de forma imediata

> os resultados da sua ação, minimizando um possível arrependimento ou remorso.[12]

Uma vez que o criminoso está geralmente acobertado pelo anonimato, isso permite e incentiva condutas que normalmente não seriam praticadas pessoalmente. O principal aspecto do *bullying* virtual, assim como os demais crimes contra a honra praticados na internet e talvez um dos mais preocupantes, é o fato de que uma vez praticado, tal informação não poderá ser facilmente apagada. Na verdade, na maioria das vezes, isto é praticamente quimérico já que não se pode ter dimensão de por onde tais informações foram compartilhadas.

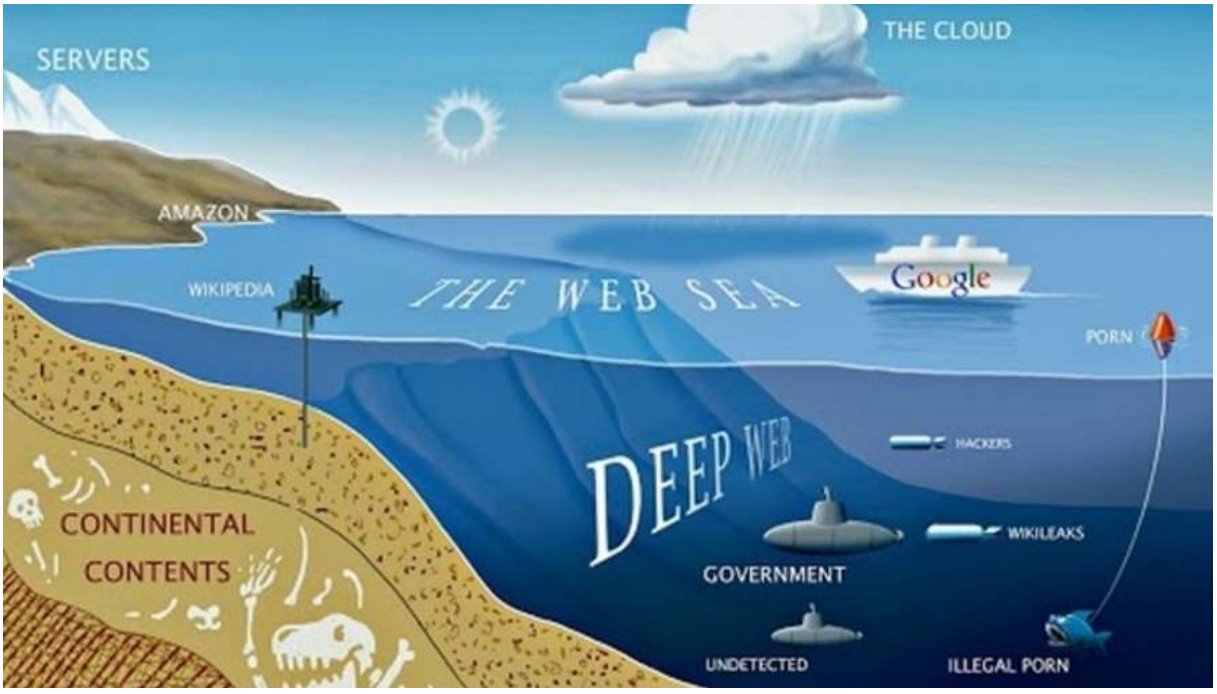
Outro aspecto sobre o *cyberbullying* é que, diferentemente do *bullying*, este não está limitado apenas aos momentos em que o agressor está diante da vítima, ou seja, ele pode acontecer o tempo todo. Devido a facilidade de compartilhar e expor a vítima com um alcance muito superior e a maior dificuldade em identificar os agressores, isto acaba por aumentar a sensação de impotência da pessoa que sofre com este tipo de crime.

---

[12] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas reais.** Rio de Janeiro: Brasport, 2014, pg. 35.

4. A *DEEPWEB* – FERRAMENTE SEGURA PARA A PRÁTICA CRIMINOSA

O paralelo criado entre a internet e o oceano trouxe expressões como “surfar” e “navegar”, que são utilizadas para compreender a complexidade do sistema tecnológico da internet e a cataloga em camadas, dentre as quais a grande maioria da população só acessa a superfície, como se fosse um *iceberg* do qual só enxerga-se a ponta. Porém, existem outras camadas mais profundas que são conhecidas como *“dark web”* ou *“deep web”*, que significa “a internet escura ou profunda”. A internet, como é conhecida pela maioria das pessoas, também chamada de *Surface Web,* representa apenas uma pequena porcentagem do real tamanho que a deep web pode alcançar. A maioria dos internautas não possui acesso a essas camadas mais profundas da internet. Geralmente, a população limita-se a acessar a *Surface Web* visto que ela já supre suas necessidades. Porém, é verdade que existe muito mais além daquilo que é possível enxergar da internet, são partes criadas com intuitos diferenciados.



A deep web teve origem em 1996, quando Paul Syverson desenvolveu um software livre de rede aberta capaz de resistir a ataques e análises dos pacotes de dados trafegados para que não se pudesse identificar a origem do acesso, que utiliza diversos servidores denominados *nós.* Assim, para cada novo salto de conexão criado, automaticamente surgirá novos *nós* até que se chegue ao destino pretendido. Dessa forma surge o anonimato, visto a complexidade do funcionamento de sua conexão que torna a identificação do usuário deveras dificultosa.[13]

Para muitos usuários é difícil e até mesmo arriscado tentar o acesso nesse mundo subterrâneo da deep web. Porém, para muitos que já trafegam e conhecem os meios de acessá-la, é fácil obter o anonimato[14]. Essas pessoas ficam sem nenhuma identificação perante à rede e sem o controle de nenhuma autoridade governamental. É nesse "esgoto da internet" que os pedófilos, exploradores sexuais, assassinos de aluguel e até mesmo organizações criminosas terroristas ou que traficam pessoas, drogas e armas costumam se esconder.

Devido ao certo grau de anonimato que o usuário que acessa a *deep web* obtém, esta é muito utilizada para a troca e arquivo de informações sigilosas que não podem estar expostas aos olhos da população. Assim, militares, cientistas e jornalistas são exemplos de categorias que se utilizam da *deep web* para guardar dados. Porém, também é fácil a proliferação de crimes e atrocidades cometidas pelo ser humano como tráfico de drogas, armas, tráfico de pessoas, encomendas de assassinatos, disseminação da pornografia infantil, entre outros.

Nesse submundo ocorrem, por dia, milhares de compartilhamentos e acessos a conteúdos pornográficos (em sua maioria fotos e vídeos de abusos cometidos contra crianças), sites de vendas de armamento pesado, prestação de serviços para homicídios encomendados onde é cobrado em torno de $40 mil dólares por morte.

---

[13] BARRETO, Alessandro Gonçalves. **Investigação Digital em fontes abertas**. Rio de Janeiro. Brasport,2017,pg. 210.

[14] ROHR ,ALTIERES. **Deep web: o que é e como funciona.** Disponível em: < http://g1.globo.com/tecnologia/blog/seguranca-digital/post/deep-web-o-que-e-e-como-funciona-g1-explica.html> . Acesso em 5 de março de 2018.

Esse mercado negro existente na *deep web* utiliza a moeda virtual para suas transações. A *bitcoin* é uma moeda virtual muito utilizada na *dark web*, que permite que os usuários conduzam transações de forma anônima, muitas vezes atrelada ao tráfico de drogas[15]. Essa é uma ferramenta que prejudica muito a identificação das atividades criminosas que ocorrem na *deep web* uma vez que tal produto - *bitcoin* - é mundialmente aceito e não regulamentado, portanto não fiscalizado. Atualmente, o valor de 1 *bitcoin* equivale a aproximadamente R$ 24.521,98 (vinte e quatro mil quinhentos e vinte e um reais e noventa e oito centavos)[16], e é um mercado que movimenta milhões de dólares por ano no Brasil. A Receita Federal, em 2014, tentou tributar a *bitcoin* e cobrar a declaração no imposto de renda de quem possuísse mais de R$ 1.000,00 (mil reais) em moedas virtuais. Dessa forma, tentou sugerir a declaração e tributação voluntária. Contudo, por ser uma moeda criptografada, ela não é regulamentada por nenhum banco central e, a menos que o usuário utilize uma corretora nacional - a qual irá exigir o cadastro por CPF - não existe maneira de controlar os valores que são transacionados por *bitcoins*. Essa é a maior vantagem das moedas virtuais[17].

A utilização da moeda digital favorece e muito outra prática ilícita no meio virtual: a lavagem de dinheiro. O termo “lavar” dinheiro é utilizado para o ato de mascarar a origem ilícita do dinheiro, dando uma cara nova a ele, a fim de não levantar suspeitas. Segundo pesquisa publicada na *Thomson Reuters* [18] - uma empresa multinacional canadense, fornecedora de serviços de comunicação especializada que atende a vários setores da economia mundial, abrangendo cerca de 140 países - foi descoberto que cerca de 95% de toda a lavagem de dinheiro praticada no mundo não é descoberta pelas instituições financeiras devido a dificuldade de rastreamento.

---

[15] ***DEEP WEB*** **ABRIGA ILEGALIDADES COMO ESPIONAGEM, TRÁFICO E PEDOFILIA** – Fantástico. Disponível em : <http://g1.globo.com/fantastico/noticia/2015/10/deep-web-abriga-ilegalidades-como-espionagem-trafico-e-pedofilia.html>. Acesso em: de janeiro de 2018.

[16] Disponível em: <http://www.quantocusta1bitcoin.com.br/>. Acesso em: 31 de março de 2018.

[17] **RECEITA FEDERAL QUER TRIBUTAR ATÉ BITCOIN**. Disponível em : <https://www.conta-corrente.com/criptomoedas/bitcoin/receita-federal-quer-tributar-ate-bitcoin/>. Acesso em: de janeiro de 2018.

[18] Disponível em:< https://www.thomsonreuters.com.br> .Acesso em: 30 de outubro de 2017.

Esses criminosos se valem de mecanismos como o uso de *shell corporations (*organizações que operam sem possuir ativos relevantes), cartões pré-pagos e tipos de sistemas bancários paralelos - como o *Shadow Banking* - para tentar legitimar esse dinheiro. Barbara Calderon, em sua obra *Deep & Dark Web*[19], explica como essas lavagens ocorrem:

> ‘’Se você deseja lavar o seu dinheiro, você precisa trocar o dinheiro que possui (que pode ser em dólar, real, peso argentino, euro, libra esterlina, etc.) por uma moeda que existe apenas no ambiente virtual - como uma espécie de câmbio do novo milênio. Você troca os dólares que possui “comprando” a moeda digital em questão, como, por exemplo, a *Bitcoin*. Agora você tem uma carteira online recheada de moedas *Bitcoins* para comprar produtos e serviços na web escura ou, se desejar, trocar por serviços reais como hospedagens em hotéis.’’

Dentre os crimes praticados na *Deep Web*, a pedofilia é o que causa maior impacto. A grande quantidade dos acessos - aproximadamente 80% - ocorridos nesse subterrâneo da internet é o fator que gera maior preocupação entre as autoridades. Ao acessar a *deep web*, é possível encontrar sites que promovem a pedofilia em forma de competição, ou seja, os pedófilos possuem um *ranking* de pontuação, no qual aquele que compartilhar maior quantidade de conteúdos permanecerá em maior colocação, como uma espécie de jogo.[20]

Essa não é a única atrocidade que acontece na *dark web*. Embora esta não seja um lugar apenas para cometimento de crimes, e muitos usuários acessem legalmente para encontrar arquivos que não estejam disponíveis na *Surface web*, se você acessá-la correrá o risco de encontrar conteúdos desagradáveis e perversos. Por exemplo, é possível encontrar grupos extremistas que agem através de fóruns bloqueados disseminando os piores tipos de preconceito. Nesses fóruns, o acesso só é permitido após o usuário passar por diversos testes até que adquira o direito de acessar tal

[19] CALDERON, Bárbara. **Deep & Dark Web**. Rio de Janeiro. Alta Books, 2017.

[20] **OS PERIGOS DA DEEP WEB**. Repórter Record Investigação - Linha de Frente. Televisão Rede Record, transmitido em 16/03/2015.

conteúdo e, em um deles, os *crackers* inclusive acessam todo tipo de informação a respeito daquele que pretende entrar. Ali são compartilhados conteúdos como vídeos e fotos de ataques a pessoas que fazem parte de um grupo específico ao qual o ódio e preconceito daquele fórum é direcionado. Também são compartilhadas teses que fulminam e incentivam o preconceito e os atos brutais cometidos.

Os assassinos de aluguel são encontrados nas “camadas” mais profundas da *deep web*, oferecendo os mais variados tipos de serviço, e os valores a serem cobrados são de acordo com o mérito e o alvo. Mérito diz respeito à quantidade e resultados dos homicídios já praticados por aquele sujeito, e o alvo, pelo grau de dificuldade que a vítima implica para a realização do serviço, ou seja, quanto mais conhecido, por exemplo, mais alto será o valor cobrado. Geralmente, os melhores assassinos são extremamente difíceis de encontrar, sendo que para fazê-lo é necessário indicação de outros que já foram clientes.

Além da prática desses assassinatos encomendados, existem também os fóruns que compartilham os *videos snuffs*, que nada mais são do que vídeos gravados de homicídios premeditados, em que o agente filma todo o ato exibindo a crueldade praticada contra a vítima.

Os usuários relatam atrocidades ainda mais doentias, como vídeos compartilhados de experimentos científicos realizados com animais e até mesmo seres humanos. A maioria deles são experimentos em que são arrancados os membros e emparedados com membros de animais com o objetivo de constatar quantos dias permanecerão vivos. Alguns dos responsáveis por tais atrocidades são pessoas ligadas à área da ciência ou que possuem muita influência, já que tais fóruns são tão supervisionados que ao menor indício de que algum “intruso” acessou aqueles conteúdos, estes são imediatamente apagados. Eis uma das maiores dificuldades para encontrar tais criminosos.

Dentro dos fóruns existe também o canibalismo. Lá são partilhados imagens e até mesmo receitas de como se prepara carne humana. Muitos casos já vieram a

público de canibais que admitiram ter comido carne humana e, em algumas circunstâncias, a pedido da própria vítima.

Alguns casos foram descobertos de sequestro de pessoas, principalmente crianças, que eram mandadas para sofrer tortura até a morte satisfazendo os desejos sádicos do comprador. Isso acontece em países em que a lei é muito mais branda, como a Tailândia, e o nível de pobreza é muito grande. Muitos casos identificados eram de crianças vendidas para essas e outras atividades pelas próprias famílias, que vivem em extrema pobreza e aceitam qualquer quantia para entregar os filhos.[21]

Essas e tantas outras brutalidades evidenciam o quão delicado é para as autoridades tratarem desse tipo de crime. Inicialmente, pela complexidade dos procedimentos adotados por esses criminosos, pode-se concluir que são pessoas que possuem muita influência e muito dinheiro já que, se não fosse assim, não conseguiriam manter a "segurança" que possuem, o alto nível de vigilância e nem mesmo as práticas deturpadas que exigem grandes investimentos. Todo aquele que possui poder e influência, influencia e exerce poder sobre alguém, e é por isso que muito além de ter uma equipe de profissionais bem preparados ou uma polícia especializada, escancarar tais práticas é acima de tudo uma afronta a muitos poderosos, o que resultaria em muitos prejuízos para outros que dependem ou tenham interesses particulares com esses criminosos. É uma situação semelhante à corrupção. Quando alguém tenta "desmascarar" um político corrupto, se depara com muitas adversidades, visto o grande poder que ele exerce sobre as mídias sociais, os grandes empresários e os demais criminosos e políticos. De igual forma, desmascarar um *cibercriminoso* como esse é, além de uma luta constante para combater e identificar essas pessoas, uma guerra de interesses.

Há ainda uma camada mais profunda e obscura chamada *Mariana's Web* - conhecida assim devido às fossas marianas, o lugar mais profundo dos oceanos,

---

[21] **OS 8 PIORES CASOS DA *DEEPWEB* QUE FORAM ENCONTRADOS PELOS INTERNAUTAS NA *SURFACE* .** Disonível em: < https://maringapost.com.br/ahduvido/os-8-piores-casos-da-deepweb-que-foram-descobertos-por-internautas-da-surface/4/>. Acesso em: 14 de outubro de 2017.

localizado no Pacífico, a leste das ilhas Mariana -, sendo o local mais difícil de acessar, onde se escondem os *cibercriminosos* mais perigosos. Esse é o local em que a polícia tem maiores dificuldades de acesso, afinal, quanto mais profunda a camada em que pretende penetrar, maior a dificuldade.

Um problema legislativo que podemos identificar no Direito Brasileiro é que pela falta de legislação específica, em alguns casos, um crime acaba sendo punido como outro. Muitas vezes o ato praticado é tão raro que não existe tipo penal que o preveja, como no caso do canibalismo. Atualmente, o canibalismo por si só não é crime, pois não se enquadra em nenhum tipo penal. Porém, quando são descobertos casos como esses no país, esses canibais acabam sendo processados apenas por homicídio, ou seja, por terem matado a vítima antes do ato canibal, portanto, se alguém come a carne humana, sem ter matado, não terá cometido crime algum. Ao depender do entendimento do juiz, poderão no máximo, ser condenados por homicídio qualificado. A discrepância jurídica existente nesse caso é tão ilógica que não se pode compreender como uma atitude com um grau de reprovabilidade social tão alta, pode ser abrandada a um homicídio, enquanto que para outros crimes mais comuns a norma penal é extremamente cuidadosa para tratar de punir de forma mais severa as condutas reprováveis.

Outro aspecto que pode ser considerado é a própria questão de a mídia mundial não divulgar os casos mais extremos em redes de comunicação, pelo grande impacto e comoção social que geraria, além de despertar sentimentos de indignação na população que seriam difíceis de controlar, como a sensação de impunidade e de falta de credibilidade na proteção Estatal. Outro motivo também é que, ao evitar a divulgação de tais práticas, busca-se manter um certo controle de que a informação não será disseminada e não resultará por incentivar outras pessoas a praticarem o mesmo.

O Direito acompanha a mesma lógica da conduta de sigilo por parte da mídia, que evita falar do que ocorre no submundo do mercado negro. Visto que o direito deve responder ao clamor social e midiático, se a sociedade desconhece os fatos, ela não clama por justiça, portanto, não existem leis que punem tais condutas.

5. DA INVESTIGAÇÃO POLICIAL

Inicialmente, para se obter resultados na investigação desses crimes ocorridos virtualmente, é essencial que se identifique qual forma o usuário utilizou, ou seja, quais ferramentas foram mecanismos para as prática delituosas. Por isso a importância de compreender como funciona a internet e as formas maliciosas existentes nela.

Para se entender o grau de dificuldade existente na investigação policial nos crimes virtuais, cumpre ressaltar alguns aspectos básicos quanto aos procedimentos na execução dos crimes. Uma vez que na década de 1950, período no qual não existia internet, uma organização criminosa se dividia em funções para o cumprimento das práticas ilegais, uma delas envolvia o contato físico do criminoso com o cliente. Assim, a organização promoveria o encontro com o cliente-criminoso para a obtenção do "produto", efetivando o contato em local físico, consumando o crime. Caso a polícia não tomasse conhecimento, os membros da organização e o cliente se dispersariam na sociedade. Porém, se a polícia conseguisse intervir, ela desmancharia parte da organização, identificaria alguns dos membros dela, seus meios de operação, algumas das práticas corriqueiras da organização, bem como os locais habituais de encontro e também o consumidor final.[22] Agora, se esta mesma organização fosse formada atualmente, seria impossível que esta não se valesse dos recursos tecnológicos para efetivar a prática do crime. Utilizaria, por exemplo, a internet para comunicação interna entre os integrantes em diversos locais.

Ocorre também a facilitação da divulgação e compartilhamento de conteúdos ilícitos como vídeos sexuais através do meio virtual, uma vez que não se faria mais necessário a presença física do consumidor para a obtenção do material. Sem o local físico, a perspectiva de uma eventual apreensão dos produtos ilícitos, da identificação dos criminosos e dos consumidores, e até mesmo um possível resgate de vítimas é deteriorada.

---

[22] CALDERON, Barbara. ***Deep & Dark Web***. Rio de Janeiro. Alta Books, 2017.

Em uma análise feita por Luís Eduardo Soares[23], as estatísticas criminais brasileiras indicam que o foco da repressão policial se concentra principalmente nas prisões em flagrante, as quais são mais fáceis de investigar. Porém, grande parte dos delitos não são sequer denunciados, por vários motivos como a opressão sócio-cultural ou os interesses particulares existentes no protecionismo político de esquemas criminosos sofisticados. Visto que esses crimes estão longe de serem de conhecimento público, é notório que a população e o Estado não possuem estatísticas que se aproximem à realidade fática criminosa. Uma vez que não são conhecidos, impossível criar mecanismos que solucionem esses problemas.

Outra grande dificuldade de se obter provas no mundo virtual é a instabilidade, ou seja, ela pode ser facilmente apagada, alterada, editada, excluída ou perdida. Isso se diferencia enormemente das investigações policiais em crimes do mundo real, uma vez que no mundo físico é muito mais difícil de exterminar por completo evidências das ações humanas. Já no mundo virtual, com essa possibilidade, o acesso aos vestígios criminosos são impalpáveis e demandam mais esforço da análise criminal. Além disso, devido a globalização, se torna muito mais simples a prática dos crimes virtuais uma vez que se pode acessar a internet de qualquer lugar do mundo, o que torna o ato criminoso muito mais fácil e rápido do que a identificação dele. Sobre isso, Gustavo Testa Corrêa discorre:

> "O grande problema relacionado aos "crimes" digitais é a quase ausência de evidências que provem contra o autor, a inexistência da arma no local do crime. Uma gloriosa invasão a sistema alheio não deixaria nenhum vestígio, arquivos seriam alterados e copiados, e nenhum dano seria prontamente identificado. Um crime perfeito, sem traços, e portanto sem evidências. Justamente por essa qualidade da perfeição há a dificuldade em presumir o provável número desses "crimes"."[24]

[23] SOARES, Luís Eduardo. PEC - 51: revolução na arquitetura institucional da segurança pública. In: Boletim do IBCCrim, ano 21, nº 252, novembro de 2013. São Paulo.
[24] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** 5 ed**.** São Paulo, Saraiva, 2010.

Enquanto no mundo real o dano causado à vítima é quase que imediato, no mundo virtual ela talvez demore muito tempo até perceber que seu computador foi infectado, ou suas informações roubadas, fazendo com que muitas das evidências relacionadas ao fato criminoso se percam. Até mesmo as grandes empresas, quando identificam a invasão em contas particulares de seus clientes, geralmente não informam a polícia a fim de inibir que se torne de conhecimento público a falha no sistema de segurança, colocando em situação delicada sua imagem perante os clientes. Dessa forma, é comum que os crackers se encaminhem em maior quantidade para esta finalidade.

Antigamente, o conceito do *cibercriminoso* estava diretamente relacionado com o *cracker,* porém isso foi modificado com o tempo. Hoje em dia, os crimes cibernéticos muitas vezes ocorrem devido a ignorância dos usuários, que praticam delitos como o *cyberbullying*, e também pela incapacidade e dificuldade que a polícia investigativa encontra para lidar com tais delitos.

Outro fator é a banalização e divulgação de informações que ensinam usuários comuns a terem acesso a documentos privados por invadir sistemas e até contas pessoais de outras pessoas. Tornou-se muito comum, inclusive, pessoas que obtiveram informações sobre como *hackear* redes sociais de outros, realizarem chantagens, dizendo que irão divulgar informações pessoais da vítima, ou que até mesmo cobram para devolver o acesso à rede. Nesses casos, o crime exige muito menos conhecimento técnico de informática do que daquele sujeito que acessa o sistema bancário de alguém, ou invade o sistema de segurança de uma grande loja. Assim, aumenta cada vez mais o número de denúncias envolvendo esse tipo de crime virtual, e pela instável situação das redes sociais, é praticamente impossível de se identificar o agressor, restando como alternativa aos usuários que se protejam cada vez mais desse tipo de ataque.

As redes sociais também se tornaram alvos dos crimes virtuais conforme foram se tornando cada vez mais populares entre os brasileiros e ao redor do mundo, sendo utilizadas para buscar relacionamentos, diversão, passatempo, divulgar informações, anunciar produtos e serviços, além de muitas outras funções. Com o crescimento

dessas redes sociais, consequentemente a criminalidade se introduziu neste meio. A maioria dos usuários não se preocupa com um possível ataque de *hacker*, ou um *stalker* (termo utilizado no meio virtual advindo do inglês que significa perseguidor) mal intencionado buscando informações sobre a rotina da vítima, nem mesmo se protegem contra agressores que agem por preconceito ou ódio para ofender ou discriminar. Por consequência, isso facilita e muito a atividade desses agressores e criminosos. Visto a facilidade de criar perfis falsos, acessando as contas virtuais por qualquer computador ou dispositivo em qualquer lugar, é muito difícil, para não dizer quase impossível que as autoridades consigam alcançar o autor da prática. Todas essas características tornam a identificação do agressor muito complexa, exige muito tempo da polícia, e ainda a incerteza de sucesso é muito grande.

Pode-se dizer que a internet é abrangente, no sentido que ela alcança democraticamente todos os países do globo. Porém, não são todos os países que estão conectados à rede mundial. Em comparação com os crimes que ocorriam antes da Internet, em que a abrangência dos crimes e das organizações criminosas se limitava a possibilidade de estar fisicamente em vários locais diferentes, os crimes cibernéticos abrem oportunidade para todos os países que estejam conectados na rede.

Em crimes como a pedofilia existente na *dark web,* a maior dificuldade encontrada pela polícia na identificação e no combate aos compartilhamentos de conteúdos sexuais é que os criminosos fazem as informações serem transmitidas e salvas por diversos servidores. Então, enquanto um servidor é identificado, outros muitos já possuem e continuam divulgando aquele conteúdo. Este fator torna a ação da polícia quase que inexistente, visto que ela praticamente não causa nenhum incômodo à prática criminosa.

Além disso, defronta-se com outro problema: o da competência territorial. O combate a esses crimes ocorre pelas autoridades capacitadas em território nacional, porém, quando estes agentes estão em outros países, os procedimentos são outros. Acerca dessa dificuldade, constata Pinheiro:

> "O problema é que na internet fica muito difícil estabelecer uma demarcação de território, as relações jurídicas que existem podem ser entre pessoas de um país e outro, e entre diferentes culturas, as quais se comunicam o tempo todo, e o direito deve intervir para proteger os litígios que eventualmente vierem a acontecer".[25]

Uma das ferramentas mais importantes para a investigação digital é a utilização do IP (*Internet Protocol*), formado por uma sequência numérica, separada por pontos, com números variáveis entre 0 e 255, que nada mais é do que o endereço único de cada conexão que é estabelecida na internet. Ou seja, são as informações de acesso que, se rastreadas, são capazes de identificar qual máquina ou aparelho está conectado. Dessa forma, torna-se mais próxima a identificação do usuário que praticou tal conduta.

Na maioria dos casos, as grandes empresas e órgãos públicos possuem endereços de IP estáticos, enquanto que os usuários domésticos utilizam de IPs dinâmicos, ou seja, cada vez que é estabelecida uma conexão é gerado um número diferente de IP. Portanto, para se identificar quem utilizou o IP, é necessário solicitar à concessionária do serviço a quebra do sigilo da informação de quem estava conectado naquele dia.

Para se identificar quem esteve conectado naquele determinado momento, é essencial que se obtenha não somente o endereço de IP que foi utilizado, mas também a data e o horário. Ao acessar o site *www.meuip.com.br* através do seu dispositivo, é possível verificar qual o endereço de IP no qual está conectado, ou seja, neste determinado dia e hora, seu dispositivo é quem utiliza este IP específico. Porém, se acessá-lo novamente daqui a uma semana, é possível que este já tenha mudado, ou não, não existe regra de quanto tempo o IP pode mudar. Isto significa que, para identificar a pessoa que esteve conectada, não se pode buscá-la apenas pelo endereço

[25] PINHEIRO, Patrícia Peck. **Direito Digital**. 4°. Ed. São Paulo: Saraiva, 2010.p.80.

de IP, pois este provavelmente estará identificando outro usuário. Portanto, é necessário que ao buscar essa informação, indique o IP, a data e o horário em que o crime foi cometido.

Outra ferramenta muito útil é o reconhecimento através do domínio utilizado. Para se criar um *website* é necessário registrar o seu domínio na internet, sendo que este deverá estar disponível, ou seja, não poderá haver dois domínios iguais. Portanto, para identificar o dono do domínio, é preciso saber em nome de quem foi realizado o registro. Porém, a identificação do responsável se torna complexa visto que não são exigidos documentos para o registro, o que facilita fraudes. Através do site da IANA[26] (*Internet Assigned Numbers Authority*) que no português significa Autoridade para Atribuição de Números da Internet, podem ser solicitados dados aos gestores de cada país, solicitando informações sobre o responsável pelo site. E no Brasil, através do site *www.registro.br.*

Assim, obtendo o endereço IP e os dados do responsável pelo domínio, é possível chegar até os autores do crime. É importante que o investigador esteja atento a todo tipo de conteúdo exposto no site, uma vez que por meio deste pode-se conseguir informações como *e-mail*, endereço, telefone, que podem beneficiar o trabalho da polícia.

Além disso, deverão as autoridades competentes registrar essas informações para que não sejam perdidas por meio de impressão, *print screens* e até mesmo através do *download* dos conteúdos que servirão como prova, mantendo a originalidade dos documentos para que possam servir de base de localização dos criminosos, e também para que se evite possíveis questionamentos durante o curso do processo penal sobre a veracidade das informações utilizadas.

Ao entrevistar o advogado especializado em crimes digitais, Dr. Fernando Peres, foi questionado quais seriam as principais dificuldades na obtenção de provas nos crimes cibernéticos, em que se pode verificar:

---

[26] Disponível em:< www.iana.org/domains/root/db>. Acesso em: 16 de outubro de 2017.

> O grande problema se encontra na produção de provas e na identificação do agente. A produção de provas em si, depende muito mais da sua existência e disponibilidade. Por exemplo, se alguém faz um comentário na internet, ou publica um site falso, se este ainda estiver no ar eu posso facilmente produzir a prova, por meio de *print screens*, impressões ou até mesmo por meio de prova testemunhal. Agora, quanto a identificação do agente, [...] cada aparelho registra as informações de acesso, que corresponde a conexão daquele momento [...] e a partir dessas informações vamos pedir a quebra de sigilo no processo judicial e ir até a operadora de internet, e lá, com o número de IP, data e hora, obrigatoriamente, eles devem fornecer os dados cadastrais do responsável por aquela conexão. Mas por exemplo, se o sujeito está na casa de outra pessoa, será identificado o nome dessa outra pessoa, nesse caso na investigação policial ou cível, pode ser realizado uma busca e apreensão de equipamento para que se faça uma perícia. Essa é uma situação padrão, mas não quer dizer que seja a mais fácil. Por exemplo, quando se trata de locais como hotéis, shoppings, mercados e etc, durante a investigação ao questionar o responsável muitas vezes eles diz não saber. Nesse caso será responsabilizado na esfera cível mas não na criminal, o que resulta na perda de oportunidade de identificar essas pessoas.[...] Outro problema é quanto aos procedimentos tomados pela vítima, visto que muitas vezes ela demora muito na produção de provas. Por exemplo, o Marco Civil da Internet prevê que os provedores de aplicação devem guardar os registros de IP com data e hora pelo período de 6 meses. Assim, se a vítima demora muito a descobrir o crime ou a solicitar a informação, eles não serão obrigados a fornecer. [...] Podemos registrar essas provas por meio do próprio boletim de ocorrência, que possui fé pública, por meio da ata notarial e se não houver tempo para isso um *print screen* poderá ser utilizado. Esta prova se tornará válida a partir do momento em que não for contestada, pois um simples *print screen* pode ser adulterado, então esta poderá ser contestada no processo judicial. Mas se não for questionada pela outra parte, se tornará legítima. [...] Falta muitas vezes conhecimento do próprio juiz, promotores e advogados na produção da própria técnica, como por exemplo, compreender que é obrigatória a informação não só do IP como da data e hora, para que essa prova não seja inútil, o que acaba dificultando na obtenção dessas informações.[27]

A lei será sempre mecanismo essencial para conter e inibir as práticas criminosas no meio virtual. Dessa forma, é necessário compreender qual a legislação vigente ao tema no Brasil. Para Hans Kelsen:

[27] PERES, Fernando. Entrevista concedida a Isadora Marina C. de Almeida Pagnozzi. Curitiba, 1 de novembro de 2017.

> (...) o Direito é uma ordem normativa da conduta humana, ou seja, um sistema de normas que regulam o comportamento humano. Com o termo 'norma' se quer significar que algo deve ser ou acontecer, especialmente que um homem se deve conduzir de determinada maneira. É este o sentido que possuem determinados atos humanos que intencionalmente se dirigem à conduta de outrem."[28]

Dessa forma, constata-se que a ordem normativa é indispensável na regulamentação dos atos da vida comum. Gustavo Têsta Correa identifica três categorias básicas de leis relevantes para serem analisadas, que se dividem entre: as leis que já foram promulgadas, que serão utilizadas para tipificar os crimes virtuais, como com a aplicação do Código Penal para enquadrar o autor ao crime, sendo este princípio aplicável principalmente aos bens tangíveis, porém podem ser aplicados aos intangíveis; as leis que seriam aplicadas em segundo plano, conjuntamente, para atingir de forma mais eficaz os seus objetivos; e por fim, as leis específicas que regulamentem condutas ilícitas, que visam normatizar o "novo"[29]. O problema da legislação que normatiza o "novo" é que muitas vezes resultam na criação de leis vagas e esparsas, que não alcançam de maneira eficaz a evolução da sociedade, visto que os crimes têm se tornado cada vez menos óbvios, sendo difícil prever todas as possibilidades.

Pode-se dizer que a grande maioria dos crimes virtuais já estão tipificados no ordenamento jurídico brasileiro, contudo, o grande problema é que geralmente os crimes virtuais não se limitam a tipificação já existente, sendo cada vez mais complexos, exigindo mais atenção do legislador para detalhar cada vez mais, através de legislações específicas as condutas praticadas, principalmente, facilitando a possibilidade de punir civil e penalmente o sujeito que as pratica.

Um aspecto que gera discussão é quanto a competência territorial dos crimes cibernéticos, sendo que muitos questionam sobre a responsabilidade de determinado

---

[28] KELSEN, Hans. **Teoria pura do direito**. Tradução de João Baptista Machado. 7. ed. São Paulo: Martins Fontes, 2006

[29] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** 5 ed**.** São Paulo, Saraiva, 2010.

país por um crime, e quanto a competência da polícia de exercer o seu poder de polícia.

A internet como meio de comunicação já possui regulamentação. Visto que se trata de serviço público, segue regulamentação da ANATEL (Agência Nacional de Telecomunicações). Em tese, a competência seria da União desde que este fosse considerado um serviço de telecomunicação segundo previsto na Carta Magna no artigo 21, XI, que compete à União a exploração, a concessão ou permissão, e os serviços de telecomunicações, e dispor sobre a organização dos serviços, a criação de um órgão regulador e outros aspectos institucionais. Mas a União não possui previsão na regulamentação para tratar de crimes cibernéticos, servindo para amparar apenas os serviços de cunho público, não podendo considerar a competência de tal órgão. Dessa forma, cabe analisar as decisões proferidas pelo Supremo Tribunal de Justiça relativa a essas questões. De acordo com o Tribunal da Cidadania, esta competência é territorial.

Em relação à competência quanto à territorialidade, em âmbito penal, o Código Penal Brasileiro determina em seus artigos 5º e 6º que:

> Art. 5º-Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.
>
> Art. 6º- Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado. [30]

Portanto, ao se tratar de crimes cometidos em território nacional, a legislação é clara ao determinar que a lei brasileira continuará prevalecendo sobre os tratados e convenções internacionais, segundo o princípio da ubiquidade.

Em 2016, em uma operação coordenada pela *Europol,* foram encontrados mais de 200 mil arquivos de abusos sexuais contra bebês e crianças de até 16 anos. Essa

[30] **VADEMECUM**, Código Penal, 24ª edição. São Paulo. Saraiva, 2017.

operação teve início quando a Interpol, através de trocas de informações com a ONG NECMEC (*Nacional Center for Missing and Exploited Children*) tomou conhecimento que um usuário da província de Múrcia, na Espanha, estaria distribuindo conteúdo pedófilo pela internet. A ação resultou na prisão de 13 pessoas. Ao investigar o caso, foi identificado que esses vídeos foram encaminhados para diferentes países (Espanha, Irlanda, Brasil, Reino Unido, Sérvia, Argentina, México e Chile), em cerca de 551 direções de *emails* e mais de 8 mil arquivos de conteúdo explícito. A investigação teve auxílio da Europol juntamente com as polícias dos Estados Unidos, Canadá, Irlanda, Letônia, França, Grécia, Suécia, Suíça, Alemanha, Reino Unido, Dinamarca, Austrália, Sérvia, Argentina, Indonésia, Israel, Japão, Quênia, Nicarágua, Paquistão, África do Sul, Sri Lanka, Ucrânia, México, Brasil e Chile.[31]

Em países como Estados Unidos existem serviços secretos (FBI, *Air Force OSI)* responsáveis por investigar crimes que saiam das fronteiras do país. Já na Europa, esses crimes são investigados por meio de cooperação mútua, que permitem tratados assinados por diversos países, e por meio da *Interpol,* que é responsável pela organização dessas investigações em outros países.

Ao se falar em crimes transnacionais, é necessário entender como age a polícia em casos como o mencionado anteriormente. Quando se identifica que determinado crime está ocorrendo parcialmente em território nacional, para que se possa investigar é fundamental a colaboração internacional. Esta ocorre por meio de tratados internacionais de investigação que permitem que a polícia nacional, juntamente com as autoridades do país no qual se pretende investigar, trabalhem conjuntamente para alcançar o resultado em comum, por exemplo, perseguindo criminosos em território estrangeiro.

[31]Disponível em: <http://g1.globo.com/mundo/noticia/2016/05/operacao-de-9-paises-contra-pedofilia-na-internet-termina-com-13-detidos.html>. Acesso em: 5 de novembro de 2017.

6. LEGISLAÇÃO NACIONAL APLICÁVEL

Por si só, podemos dizer que a legislação vigente no Brasil atualmente já abrange os principais crimes virtuais. Mesmo que não os exemplifique separadamente, os artigos do Código Penal já tipificam as mesmas condutas, portanto, podemos analogicamente aplicá-las ao caso concreto. Por exemplo, o artigo 139 do Código Penal prevê pena de detenção de três meses a um ano e multa pelo crime de difamação, que consiste em imputar a alguém fato ofensivo a sua reputação. O crime, cometido em âmbito virtual ou real, será punido de igual forma.

Todavia, era de extrema importância que existisse lei específica que garantisse maior efetividade do judiciário no combate aos crimes cibernéticos. Então, em 2012, com a entrada em vigor das Leis 12.735 e 12.737, a possibilidade de responsabilização do agente e daqueles que invadem dispositivos para roubar dados se tornou mais concreta.

A Lei 12.735 veio a regulamentar a ação da polícia judiciária, em que se pode ler:

> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.
>
> Art. 5º O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação: "Art. 20. II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;[32]

[32] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.html>. Acesso em: 1 de novembro de 2017.

Houve muitas críticas a essa lei devido a um evidente retrocesso legislativo em comparação à Convenção de Budapeste, que será tratada mais adiante. Visto que esta pretendia um vigilantismo exacerbado das práticas na Internet, ficou claro que de forma alguma os *cibercriminosos* seriam prejudicados pela nova lei, e sim os próprios usuários que, acabando com a navegação anônima, estariam completamente expostos às corporações que rastreiam dados dos internautas, aos governos de países autoritários e os próprios criminosos que teriam ainda mais facilidade de obter informações. Daí surgiu uma urgência constitucional na criação do Marco Civil da Internet.

Já na Lei 12.737, durante sua criação ocorreu o incidente com a atriz Carolina Dieckmann, que teve seu dispositivo invadido e fotos íntimas de seu computador divulgadas, portanto, a lei ficou conhecida carregando seu nome. Esta lei visa tipificar os delitos informáticos tratando das invasões a dispositivos informáticos, da interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública e da falsificação de documento particular e cartão. E, além disso, tipifica condutas que não eram até então tratadas como infração penal.

Porém, houve descontentamento por parte de muitos com relação a baixas penas atribuídas a esse tipo de infração, não servindo necessariamente para coibir tais condutas. Também, tais leis não esgotaram toda a necessidade de especificar as diversas possíveis formas de delitos. Repara-se:

> Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
>
> "Invasão de dispositivo informático Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.[33]

[33] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.html>. Acesso em: 2 de novembro de 2017.

Como podemos notar, a lei prevê que a invasão a dispositivos com o intuito de obter, adulterar ou destruir dados é infração penal punível de três meses a um ano, mas não prevê os casos de bisbilhotagem, por exemplo, em que o agente tem por intuito apenas acessar dados para proveito próprio ou para chantagear a vítima, ou nos casos em que o criminoso distribui esses arquivos roubados. Então, se o agente não violar nenhum dispositivo de segurança, não terá cometido nenhum crime.

Segundo Fernando Peres, quando questionado a respeito dos problemas do legislativo na hora de criar leis:

> Eu tenho um medo muito grande no processo de criação de leis. Vejo ainda que leis que tratam de áreas específicas como a tecnologia, acabam recebendo muita influência de empresas que possuem algum tipo de interesse. E grandes provedores de internet no Brasil, possuem representantes de relações governamentais, que visam impedir que algumas leis sejam aprovadas junto ao Congresso. Agora, na hora de se criarem leis técnicas, apesar de muitas colaborações que recebem , acabam criando previsões que não são inúteis ou são impossíveis de ser realizadas. Como por exemplo, a Lei Carolina Dieckmann, que possui artigos tão específicos, que muitos crimes podem não ser enquadrar. [...] Quando se trata de questão criminal, temos que ser pontuais, não podemos fazer analogias e interpretações em desfavor do réu. [34]

Em 2014, foi sancionada a Lei 12.965, também conhecida como Marco Civil da Internet que visa regulamentar o uso da Internet por meio de princípios, garantias, direitos e deveres para os usuários. A ideia do projeto surgiu com a resistência à Lei de Azeredo (12.735/12), como uma proposta do Poder Executivo a Câmara dos Deputados e aprovada em 23 de abril de 2014. Ela serve para regular a utilização, garantir a privacidade, a inviolabilidade da vida privada, bem como para garantir que a Internet cumpra a função social devida. É regida a partir de princípios como os da neutralidade, da reserva jurisdicional, da responsabilidade dos provedores, dentre outros. Foi de

[34] PERES, Fernando. Entrevista concedida a Isadora Marina C. de Almeida Pagnozzi. Curitiba, 1 de novembro de 2017.

extrema importância para impor principalmente obrigações de responsabilidade civil aos usuários e provedores.

7. LEGISLAÇÃO INTERNACIONAL E TRATADOS

Nesse âmbito, podemos citar a Convenção de Budapeste, também conhecida como Convenção do *Cybercrime*, que trata-se de um tratado internacional de direito penal e processual emergido na União Européia em 2001 e aderido por diversos países desde então que, segundo seu preâmbulo, visam criar uma política criminal comum com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço através de legislação e cooperação internacional.

Em síntese, podemos identificar que ela trata de tipificar: os crimes virtuais como infrações de sistemas; as infrações relacionadas aos crimes com computadores; os crimes que envolvem pedofilia; e também tipificar violações de direitos autorais. Ela trata também da competência e cooperação internacional, deixando a critério das partes decidirem quem será a jurisdição mais apropriada para o procedimento legal.

> Artigo 22º - Competência
>
> 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infração penal definida em conformidade com os artigos 2º a 11º da presente Convenção, sempre que a infracção seja cometida: a) No seu território; ou b) A bordo de um navio arvorando o pavilhão dessa Parte; c) A bordo de uma aeronave matriculada nessa Parte e segundo as suas Leis; ou d) Por um dos seus cidadãos nacionais, se a infração for punível criminalmente onde foi cometida ou se a infração não for da competência territorial de nenhum Estado.[35]

Para aprofundar o entendimento a respeito, é proveitoso compreender como funciona a Cooperação Internacional.

A ONU (Organização das Nações Unidas) utiliza instrumentos multilaterais que implicam em harmonizar as políticas de colaboração entre os países em âmbito penal,

[35]Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf>. Acesso em 10 de outubro de 2017.

de forma que estabelece regras e responsabilidades para o combate aos crimes transnacionais. Tem por objetivo incentivar os países a criar tratados bilaterais e multilaterais para aumentar a eficácia dessas cooperações por ampliar as bases jurídicas preenchendo as lacunas legais em que os países podem contar.

Outro aspecto importante é quanto à resposta ao pedido de cooperação internacional, isso quer dizer que é necessário por parte dos países que atendem as solicitações de outros países para investigar e tomar as providências cabíveis em casos de crimes transnacionais. Para isso, depende muito da infraestrutura, dos profissionais e das possibilidades que o país possui para atendê-las. Isso ocorre basicamente com preparação de autoridades que desempenhem essas funções, coordenando, recebendo e processando os pedidos. Geralmente as autoridades mais comumente designadas para essas atividades são os ministérios da Justiça, procuradorias-gerais e ministérios de Relações Internacionais.[36]

[36] Disponível em: <https://nacoesunidas.org/crime2015/cooperacao-internacional/>. Acesso em: 10 de outubro de 2017.

CONCLUSÃO

Ao fim da pesquisa pode-se compreender a relevância do tema visto que a evolução tecnológica tem se expandido mais e mais a cada dia, surgindo diversos tipos de delitos cibernéticos. Tais crimes exigem atenção uma vez que a internet tornou-se parte essencial da vida em sociedade, necessitando de normas que regulamentem as ações humanas no ambiente virtual.

No primeiro capítulo nota-se que o surgimento desses primeiros delitos acarretou na necessidade do Direito em direcionar seu olhar para a *internet* originando, junto com a Constituição Federal, as primeiras menções a normas informáticas e questões de competência.

No segundo capítulo conceitua-se o crime virtual para compreender quem são os *cibercriminosos* e de que maneira ocorre esse tipo de crime. Desconceitua também o paradigma social de que o *cibercriminoso* é necessariamente alguém com conhecimento técnico, mas que pode ser também um usuário comum que utiliza a *internet* e pratica condutas tipificadas no Código Penal.

O terceiro capítulo aborda parte do universo da *deepweb*, que se mostrou um espaço vasto e muito complexo no combate à criminalidade visto a dificuldade em identificar os agentes transgressores e a facilidade com que as informações são compartilhadas, fugindo da alçada da polícia em cessar a transmissão de informações.

Aborda também a utilização da moeda virtual – *Bitcoin* – para transações no mercado negro e lavagem de dinheiro. Fato este que evidencia a necessidade de regulamentação e fiscalização por parte do Estado, a fim de inibir práticas ilícitas, não podendo mais manter-se omisso diante dessa situação fática.

A falta de legislação também se mostra um problema, como no exemplo do canibalismo citado anteriormente neste trabalho. Não se admite a falta de norma que proíba tal prática apenas porque o fato é esporádico. Nota-se que a falta de informação

é um dos motivos para que a sociedade permaneça inerte às brutalidades que são comandadas e organizadas através da *deepweb*.

No quarto capítulo aborda-se a dificuldade na obtenção de provas que possam identificar o agente e instruir um processo penal. A fragilidade e instabilidade da *internet* se mostra fato gerador da causa, sendo essencial a criação e divulgação de políticas de prevenção contra crimes cibernéticos, visto que essa é melhor opção para o combate à criminalidade. Nesse óbice, empresas provedoras de *internet* e as empresas que fornecem o acesso à ela precisam criar mecanismos de controle e identificação dos usuários.

Se faz necessária também a criação de normas específicas que englobem de maneira mais eficaz os atos cometidos na esfera virtual, afinal, por mais que o legislador tenha criado leis para tanto, observa-se deficiências quanto a efetividade da norma.

Os quintos e sextos capítulos analisam a maneira como as legislações nacionais e internacionais se posicionam a fim de repelir condutas criminosas. Evidencia-se que a promulgação do marco civil da internet mostrou-se de papel fundamental para regular a utilização da *internet*, juntamente à Convenção de Budapeste.

Conclui-se também que a Cooperação Internacional é essencial no combate aos *cybercrimes*, assim como as convenções entre países que visam harmonizar a atividade e os seus ordenamentos jurídicos.

Cabe ressaltar que a reflexão acerca do tema visa que o Direito Penal alcance de forma mais plena as mudanças que a sociedade vem sofrendo frente à evolução das ciências tecnológicas, a fim de torná-lo concomitante com a realidade fática social.

REFERÊNCIAS

BARRETO, Alessandro Gonçalves. **Investigação Digital em fontes abertas**. Rio de Janeiro. Brasport, 2017.

BRASIL. LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012 altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. **Diário Oficial da República Federativa do Brasil,** Brasília, 30 de novembro de 2012.

BRASIL, LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012 dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da República Federativa do Brasil,** Brasília, 30 de novembro de 2012.

CALDERON, Bárbara. **Deep & Dark Web**. Rio de Janeiro. Alta Books, 2017.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas reais**. Rio de Janeiro: Brasport, 2014.

COLLI, Maciel. ***Cibercrimes*: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos**. Curitiba: Juruá Editora, 2010.

CONVENÇÃO SOBRE CIBERCRIME. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf >. Acesso em 10 de outubro de 2017.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 5 ed. São Paulo, Saraiva, 2010.

***DEEP WEB* ABRIGA ILEGALIDADES COMO ESPIONAGEM, TRÁFICO E PEDOFILIA –** Fantástico. Disponível em : <http://g1.globo.com/fantastico/noticia/2015/10/deep-web-abriga-ilegalidades-como-espionagem-trafico-e-pedofilia.html>. Acesso em: de janeiro de 2018.

FERREIRA, Ivette Senise. **Direito & Internet: Aspectos Jurídicos Relevantes**. 2 ed. São Paulo: Quartier Latin, 2005.

FOXBIT. Disponível em: <http://www.quantocusta1bitcoin.com.br/>. Acesso em: 31/03/2018.

G1. **Operação de 9 países contra pedofilia na internet termina com 13 detidos.** Disponível em: <http://g1.globo.com/mundo/noticia/2016/05/operacao-de-9-paises-

contra-pedofilia-na-internet-termina-com-13-detidos.html> Acesso em: 5 de novembro de 2017.

INTERNET ASSIGNED NUMBERS AUTHORITY. Disponível em: <www.iana.org/domains/root/db>. Acesso em: 16 de outubro de 2017.

JESUS, Damásio de; MILAGRE, José Antonio. **MANUAL DE CRIMES INFORMÁTICOS**. São Paulo: Saraiva, 2016.

KELSEN, Hans. **Teoria pura do direito.** Tradução de João Baptista Machado. 7. ed. São Paulo: Martins Fontes, 2006.

KRONE, Tony. ***High Tech Crime Brief. Australian Institute of Criminology***. Canberra, Australia. ISSN 1832-3413. 2005.

ONU. Brasil. **Combatendo o crime organizado transnacional através de uma melhor cooperação internacional.** Disponível em: https://nacoesunidas.org/crime2015/cooperacao-internacional/. Acesso em: 10 de outubro de 2017.

OS PERIGOS DA DEEP WEB. Repórter *Record* Investigação - Linha de Frente. Televisão Rede Record, transmitido em 16/03/2015.

OS 8 PIORES CASOS DA *DEEPWEB* QUE FORAM ENCONTRADOS PELOS INTERNAUTAS NA *SURFACE* . Disonível em: < https://maringapost.com.br/ahduvido/os-8-piores-casos-da-deepweb-que-foram-descobertos-por-internautas-da-surface/4/>. Acesso em: 14 de outubro de 2017.

PERES, Fernando. **Entrevista concedida a Isadora Marina C. de Almeida Pagnozzi**. Curitiba, 1 de novembro de 2017.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4°. Ed. São Paulo: Saraiva, 2010.p.80.

RECEITA FEDERAL QUER TRIBUTAR ATÉ BITCOIN. Disponível em : <https://www.conta-corrente.com/criptomoedas/bitcoin/receita-federal-quer-tributar-ate-bitcoin/>. Acesso em: de janeiro de 2018.

ROHR ,ALTIERES. **Deep web: o que é e como funciona.** Disponível em: < http://g1.globo.com/tecnologia/blog/seguranca-digital/post/deep-web-o-que-e-e-como-funciona-g1-explica.html> . Acesso em 5 de março de 2018.

SCHJOLBERG, Stein. ***The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva***. Disponível em: <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>. Acesso em 11 de outubro de 2017.

SOARES, Luís Eduardo. **PEC - 51: revolução na arquitetura institucional da segurança pública**. In: Boletim do IBCCrim, ano 21, nº 252, novembro de 2013. São Paulo ZEVIAR-GEESE, G. **The State of the Law on Cyberjurisdiction and**

Cybercrime on the Internet. California Pacific School of Law. Gonzaga Journal of International Law. Volume 1. 1997-1998.

THOMSON REUTERS. Disponível em: <https://www.thomsonreuters.com.br>. Acesso em: 5 de novembro de 2017.

UM MUNDO INVISÍVEL: VOCÊ SABE O QUE É A FAMOSA DEEP WEB? Disponível em: < https://tecnologia.uol.com.br/noticias/redacao/2017/11/12/um-mundo-invisivel-o-que-e-a-deep-web.html>. Acesso em: 7 de março de 2018.

VADEMECUM, Código Penal, 24ª edição. São Paulo. Saraiva, 2017.