FUNDAÇÃO PRESIDENTE ANTÔNIO CARLOS DE UBÁ

FACULDADE DE DIREITO

2019

CRIMES PRATICADOS E AUXILIADOS PELO ANONIMATO DA DEEP WEB: FORMAS DE AMPLIAR O MEIO INVESTIGATIVO

Matheus Almada Venâncio – *matheusvenancio07@yahoo.com.br*

Galvão Rabelo – *galvaorabelo@yahoo.com.br*

RESUMO

O desenvolvimento deste trabalho tem como objetivo demonstrar a atuação brasileira contra crimes praticados no meio virtual, apresentado crimes que são praticados na vida real e eventualmente, com o avanço tecnológico passaram a serem praticados através de meios profundos da internet. Discute-se, os meios investigativos atualmente utilizados pela polícia nacional, bem como os que são utilizados fora do país, a fim de buscar uma melhor solução, mesmo que temporária, para este problema mundial.
Palavras-chaves: Deep Web. Dark Web. Crimes virtuais. Internet. Investigação.

ABSTRACT

The development of this work aims to demonstrate the Brazilian action against crimes committed in the virtual environment, presented crimes that are committed in real life and eventually, with the technological advance began to be practiced through deep means of the internet. It is discussed the investigative means currently used by the national police, as well as those used outside the country, in order to seek a better, even temporary, solution to this worldwide problem.
Keywords: Deep Web. Dark Web. Virtual Crimes. Internet. Investigation.

INTRODUÇÃO

O desenvolvimento tecnológico e a internet passaram a fazer parte do cotidiano das pessoas permitindo uma maior facilidade em suas tarefas diárias.

Contudo, não só benesses foram trazidas para nossas vidas com seu desenvolvimento. Podemos dizer que o fato de encurtar fronteiras, trazer tantas facilidades, é também, uma oportunidade de praticar delitos, comuns na vida real, também no meio virtual. A facilidade proporcionada a seus usuários é a mesma que se apresenta para aqueles que visam praticar delitos, já que a internet é uma rede de transmissão de dados, ficando o agente acobertado pelo anonimato, dificultando a identificação e sua localização.

O desdobramento deste trabalho tem como objetivo o estudo das formas de investigação utilizadas em âmbito nacional, bem como dos métodos adotados para com as condutas praticadas na *Deep Web*. Para tanto, serão examinados a legislação específica existente para combater este tipo de crime, assim como estudo de alguns crimes específicos praticados no ambiente mais profundo da internet, ressaltando a dificuldade existente na investigação e na identificação do agente causador do dano.

Ainda, será discutido o método investigativo adotado pela Polícia Federal, no combate à pornografia infantil, assim como o método investigativo e punitivo adotado em outros países, a fim de buscar uma solução para a falta de penalização de eventuais crimes no meio virtual.

1. CONSIDERAÇÕES INICIAIS

É sabido que nos últimos anos a tecnologia e a internet passaram a fazer parte do nosso cotidiano, proporcionando muitos benefícios para as pessoas, tanto na forma econômica (avanço do empreendedorismo, propagação da informação), como no entretenimento das pessoas.

Ainda que tenha trazido tantos benefícios para melhora da qualidade de vida das pessoas, pode-se dizer que, ao encurtar as fronteiras, permitiu que as pessoas usassem desse meio para praticar delitos, já que podem estar em vários lugares ao mesmo tempo, dando amplitude para a prática de vários crimes, sem sair da frente do computador.

Em meados da década de sessenta começaram a ser descobertos os primeiros casos de crimes informáticos, tais como infiltrações ilícitas, furto de informações sigilosas. Com o passar do tempo, foram aumentando as modalidades de crimes. À medida que a tecnologia foi evoluindo, a mente criminosa “evoluiu” junto, servindo para provar que a nossa legislação, bem como a mundial não estava preparada para solucionar esse tipo de problema, de forma a

provar a vulnerabilidade da sistemática jurídica, no que se refere a punição de quem cometesse crimes nesse meio.

A facilidade que a internet proporciona aos seus usuários é a mesma apresentada para aqueles que visam o mal, já que é uma rede relacionada à transmissão de dados, e o criminoso, em sua grande maioria, fica acobertado pelo anonimato, dificultando a sua identificação, bem como sua localização, atuando de forma clandestina, oculta, bastando o conhecimento técnico e a utilização da máquina para conseguir concretizar seu objetivo. Torna-se, portanto, um dos meios mais eficazes para realização de inúmeros atos delituosos que violam bens da sociedade.

Assim, há uma grande dificuldade para investigadores e para operadores do direito punir os infratores, uma vez que, no direito penal, deve ser respeitado o princípio da reserva legal, legalidade penal e não pode ser aplicado analogia *in malam partem*[1].

Diante de tanta vulnerabilidade do meio cibernético, mais se amplia o leque de crimes, ficando nítido o risco potencial que tem a internet, cabendo ao Estado, a busca de meios para aprimorar as formas de prevenção e combate aos delitos praticados nesse ambiente. Logicamente, é quase impossível que o ordenamento jurídico preveja todas as formas de condutas ilícitas. Contudo, deve haver maior eficiência na repressão dos casos que ocorrem com frequência no ambiente virtual e, partindo dessa premissa, elaborar barreiras que visam a contenção de novas condutas.

Nos dias atuais, existem basicamente no ordenamento jurídico brasileiro, duas leis. A Lei 12.735/2012 e a Lei 12.737/2012, a primeira, tipificando as condutas realizadas usando o sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados. Esta última ficou conhecida nacionalmente com “Lei Carolina Dieckman”, criada após vazamento de fotos pessoais da atriz do seu computador pessoal, esta norma visa penalizar as invasões a computadores, roubo de senha e arquivos.

Contudo, apesar dessas duas leis específicas, é notável que o ordenamento jurídico brasileiro não acompanhou a evolução dos crimes cibernéticos, objetivando coibir eventuais crimes que fossem cometidos nesse meio. Se faz necessário ter uma mentalidade preventiva, a fim de buscar a criação de meios que identifiquem e punam com mais rigor os infratores.

1.1 O que são crimes virtuais?

[1] É aquela em que nos casos de omissão na lei, se adota a lei em for prejudicial ao réu, não sendo permitido no Brasil.

A partir do conceito analítico finalista de crime, podemos chegar à conclusão de que crimes virtuais são todas as condutas típicas, ilícitas e culpáveis, que sejam praticadas com auxílio dos sistemas de informática.

Contudo, as denominações dadas aos crimes praticados neste meio são diversas, não havendo uma definição sobre qual seria o melhor conceito para os delitos cometidos com auxílio da tecnologia no meio virtual.

Dito isso, necessário se faz trazer conceitos de estudiosos diversos no assunto.

Para Ramalho Terceiro,

> Os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo; por isso, ficaram usualmente definidos como sendo crimes virtuais. Ou seja, os delitos praticados por meio da Internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas (TERCEIRO, 2006; s/p).

Augusto Rossini, por seu turno, sustenta que:

> 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 e a confidencialidade (ROSSINI, 2004; s/p).

O conceito trazido por Rossini abrange todas as condutas praticadas no meio da internet e que tenham relação com os sistemas informáticos, o que inclui os delitos em que o computador consiste apenas em objeto de auxílio para o cometimento do crime, ainda que este não esteja conectado no ambiente virtual, ou qualquer ambiente telemático. Para o autor, "delito informático" é gênero, do qual "delito telemático" é espécie.

Já Guilherme Guimarães Feliciano, apresenta um conceito mais amplo sobre crimes virtuais:

> 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 (FELICIANO, 2000, p. 42.).

Perspicaz trazer, ainda, o conceito de "crime de informática" disposto pela Organização para Cooperação Econômica e Desenvolvimento da ONU: "crime de informática é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento de dados e/ou transmissão de dados".

Logo, percebe-se que não há um conceito definido sobre o que é crimes virtuais, tão menos há uma denominação aceita pela maioria.

Alguns doutrinadores classificam os crimes virtuais em duas espécies diferentes, quais sejam os crimes virtuais puros ou próprios e crimes impuros ou impróprios.

Para que um delito seja considerado crime virtual e chegar nesta distinção de espécies levou-se em consideração o bem jurídico por ele protegido.

As condutas típicas onde houve a inviolabilidade de informação automatizada através do computador serão chamados de crimes virtuais próprios. Por conseguinte, os crimes nas quais o computador serviu como instrumento de execução, mas não houve ofensa ao bem jurídico informático (inviolabilidade da informação de dados), denominam-se crimes virtuais impróprios.

1.1.1. Crimes virtuais próprios

Os crimes virtuais próprios consistem naqueles em que o bem jurídico tutelado pela norma penal é a inviolabilidade de informações de dados e sistemas. O objeto é especificamente o computador e seus sistemas de informática e dados que por ele são utilizados, por isso a denominação delitos virtuais próprios.

Neste contexto, entram os atos praticados por hackers – no que se refere à invasão de sistemas –, quanto os atos de modificar, alterar, inserir dados falsos, visando atingir diretamente o software ou hardware do computador e só podem ser concretizados pelo computador ou contra ele.

Dentre os crimes virtuais próprios, é de ressaltar o crime previsto no artigo 154-A, § 1º, do Código Penal Brasileiro, que se refere à criação de programas de computadores destrutivos, tendo como principal representante o vírus informático.

1.1.2 Crimes virtuais impróprios

Crimes virtuais impróprios são aqueles em que o agente se utiliza do computador para produzir um resultado naturalístico, visando produzir prejuízo no mundo físico, como, por exemplo, lesando bens diversos aos da informática, sem que exista, contudo, ofensa ao bem jurídico da informação automatizada (dados).

Portanto, existem crimes impróprios, nos quais se admite a sua pratica no meio virtual, como, por exemplo, os crimes previstos nos artigos 241 e 241-A da Lei n. 8.069 de

1990, em que o agente comercializa fotos ou vídeos de criança e adolescentes através do computador, utilizando-se da rede, sem, no entanto, utilizar-se de dados do computador para cometer o referido crime.

Logo, o computador é usado apenas como um instrumento para que o crime possa ser executado, não havendo ofensa a um bem jurídico, como sistemas de dados, por exemplo.

2. DAS FORMAS DE ACESSO À FACILIDADE DE SE COMETER CRIMES VIRTUAIS

A *internet*, que é um conjunto de redes interligadas espalhadas em todo o planeta, onde os usuários conseguem se comunicar e trocar dados através do protocolo TCP/IP, pode ser dividida em três partes, quais sejam: a *surface*, a *Deep Web* e a *Dark Web*, que serão explicadas no tópico abaixo.

2.1 *Surface, Deep Web* e *Dark Web*

A internet comum, também conhecida como *Surface* ou superfície da web, é qualquer coisa que pode ser acessada por um buscador comum como o Google. Na internet comum os computadores dos usuários são facilmente rastreados, desde que tenham os IP (*Internet Protocol*) das máquinas.

Deep Web, também conhecida como *deep net*, *invisible web* e *hidden web*, traduzindo para o português, internet profunda ou web invisível, refere-se a um conteúdo da internet de difícil acesso, ao qual não se pode ser encontrado por mecanismos de busca, tais como Google, Bing, Yahoo. É o contrário da *Surface*. Sua estrutura possibilita ao usuário certo anonimato, uma vez que o acesso a este ambiente virtual carece de links próprios para acessar seus conteúdos.

Uma vez sendo restrito o acesso aos conteúdos na *Deep Web*, seus usuários utilizam-se de redes criptografadas, que ocultam sua identidade, como *Tor*, o *i2p*, escondendo as informações de IP e dados de quem os usam. Contudo, a maioria das pessoas que acessam a este ambiente da internet não procura se envolver em situações ilegais, apenas não desejam serem encontradas. Existem todos os tipos de informações neste meio, tanto boas, como ruins e muito ruins.

A *Dark Web* é uma ramificação da *Deep Web*, sendo também conhecida como uma zona escura, criptografada de forma altamente complexa, onde somente pessoas com conhecimento avançado de informática conseguem ter acesso.

A diferença é que na *Dark Web* ocorrem todas as situações ilícitas e vazamentos de informações ilegais, comercialização de drogas, fraude de informática através de hackers, pornografia infantil, induzimento ao suicídio (como, por exemplo, o jogo da baleia azul), sendo os *Bitcoins*[2] a forma de pagamento nesse meio.

Em suma, é como se fosse um iceberg, a internet comum (*Surface*) a ponta, onde a pessoa consegue enxergar, a *Deep Web* o meio do iceberg, logo abaixo da água, e a *Dark Web*, o final do iceberg, no escuro, onde se é quase impossível o acesso.

2.2 Crimes praticados na *Dark Web*

Por ser um meio com acessibilidade limitada, o criminoso se aproveita da camuflagem que o ambiente virtual lhe fornece, a fim de potencializar os crimes para o ambiente sistêmico, uma que vez existe uma grande dificuldade de identificar o agente.

2.2.1 Tráfico de Drogas

É sabido que cada vez mais se intensifica o combate ao tráfico de drogas, incluindo o combate a venda. Contudo, claramente ainda não se obteve êxito nesta operação, pelo contrário, o número de comercialização da droga só aumenta, e agora se expande para o ambiente virtual.

Neste meio virtual, existem sites especializados de venda destas substâncias ilícitas que cada vez mais atraem mais pessoas para comprar. Funciona como se fosse um *e-commerce*, premiando os melhores vendedores com uma estrela, com fóruns de debates, esclarecendo qualquer dúvida, garantindo ao cliente a sua venda e tendo o pagamento sendo realizado através de *bitcoins*.

Bitcoins (criptomoeda) é a moeda usada não só *Dark web*, mas na internet de modo geral, podendo ser comprada com dinheiro real, mas só podendo ser trocada no ambiente

[2] *Bitcoin*, também conhecida pela sigla BTC, é uma criptomoeda, moeda digital descentralizada, ela permite transações financeiras eletrônicas sem intermediários, onde apenas os usuários da rede tem acesso. Foi criada no ano de 2008 fazendo ressurgir o sistema bancário livre, onde os usuários podem negociar entre si, independentes de qualquer instituição financeira.

virtual. Seu preço varia de acordo com a lei da oferta e procura, uma vez que nenhuma intuição financeira controla a *bitcoin*. Assim, quanto maior a busca, maior seu preço.

Em pesquisa feita pela Trend Micro, empresa especializada em proteção de computador contra ameaças virtuais, a droga mais procurada neste ambiente é a maconha, seguida de remédios tarja preta, que necessitam de receitas, e o ecstasy.

2.2.2 Pornografia infantil

Outra forma de crime cometido na *Dark Web* é se valer do mercado negro da pornografia infantil, onde os agentes se aproveitam da dificuldade de serem rastreados, para reproduzirem fotos e vídeos desse conteúdo.

Este mercado movimenta, no mundo, mais de 4 bilhões de reais por ano, dados gerados pela Interpol, mostrando, ainda, que o Brasil é um dos países que mais exploram este tipo de conteúdo, ocupando a quarta colocação.

Para penalização da conduta de expor imagens de crianças e adolescentes em cenas de sexo no Brasil, temos a Lei 8.069/90, em seu artigo 240, recentemente alterado pela Lei 11.829/08, conforme segue:

> **Art. 240**. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
> **§ 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.
> **§ 2º** Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:
> **I** – no exercício de cargo ou função pública ou a pretexto de exercê-la;
> **II** – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou
> **III** – prevalecendo-se de relações de parentesco consangüíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento.

Mesmo estas condutas sendo tipificadas na legislação brasileira, quando estes crimes são cometidos no meio da *Dark Web*, tem-se muita dificuldade de identificar o agente que praticou o delito, tendo em vista que este infrator está camuflado por vários IPs, dificultando assim o rastreamento pela polícia.

Não obstante toda dificuldade já relatada, as investigações esbarram, ainda, em questões de territorialidade, uma vez que, na maioria das vezes, os sites que estão hospedados em um provedor estrangeiro podem impedir a retirada deste tipo de conteúdo, em razão da liberdade de manifestação exercida dentro do seu território o que é um preceito fundamental.

Apesar disso, com a Operação *Dark Net*, da Polícia Federal, em 2018, o Brasil conseguiu um avanço nas investigações contra estes crimes, desenvolvendo metodologia para investigar e identificar usuários na *Deep Web* e, consequentemente, na *Dark Web*. Esta Operação já cumpriu mais de 100 mandados de busca e apreensão, além de diversas prisões, comprovando o desenvolvimento das investigações, contudo, com muito trabalho ainda a ser feito.

3. FORMAS DE AMPLIAR O MEIO INVESTIGATIVO

Atualmente o Brasil possui algumas formas de prevenção, ação e punição no que concerne aos crimes cibernéticos. Dentre as formas de prevenção e ação podemos citar o monitoramento de redes de computadores em que há suspeita de práticas ilegais, porém só é possível mediante autorização judicial, o que dificulta o trabalho, aquisição de ferramentas que possam executar exames periciais ou até mesmo o desenvolvimento delas, de acordo com a necessidade, podendo adotar, também, a implantação de tecnologias de segurança da informação, com a intenção de prevenir a ação de criminosos digitais.

Atualmente a legislação brasileira versa no que diz respeito às condutas ilícitas praticadas no meio cibernético através da Lei 12.737/2012, popularmente conhecida como Lei Carolina Dieckman, e pela Lei 11.829/08, na qual penaliza as práticas de expor imagens de crianças e adolescentes em cenas de sexo no Brasil (Lei n. 8.069/90, em seu artigo 240, recentemente alterado pela Lei 11.829/08).

Estima-se que os crimes cometidos neste meio arrecada cerca de 1,5 trilhões anualmente no mundo, e vem crescendo, sendo esta uma das maiores preocupações da ONU e suas agências, não sendo, portanto, um problema apenas nacional.

Nesse sentido, visando combater as ações de criminosos virtuais, no ano de 2001, foi aprovado pelo Conselho da Europa a Convenção de Budapeste sobre cibercrime, hoje considerada uma referencia legislativa mundial no que diz respeito aos crimes praticados no meio virtual. A Convenção conta com a assinatura de 64 países, tendo sido ratificada por 21 nações signatárias, incluindo países da União Europeia, tais como: Espanha, Itália, Portugal e França, contando ainda com países como Canadá, Japão, Estados Unidos, Chile, dentre outros.

A convenção surgiu da necessidade de intensificar a cooperação entre os Estados signatários, com a finalidade de proteger a sociedade contra a criminalidade no âmbito virtual, além disso, a convenção afirma o quão é importante uma cooperação que vai além das

relações internacionais, sendo possível utilizar dos dados obtidos pelas indústrias privadas que possuam dados eletrônicos que possam ajudar na localização e identificação de criminosos virtuais, mesmo sendo localizadas em outros países.

No ano de 2008, na CPI da pedofilia, presidida pelo parlamentar Magno Malta, foi colocado em pauta um caso em que uma grande empresa de tecnologia se recusou a fornecer dados e suspeitos de pedofilia, alegando que os usuários se cadastram seguros em que há sigilo nas informações e as mesmas não serão repassadas a terceiros. Somente após a intervenção do Ministério Público Federal, através de negociações e depoimentos é que a empresa cooperou, o que ocasionou muita demora pois, apesar de o crime envolver brasileiros, o local em que os dados foram armazenados se encontrava em outo Estado, sendo assim em outra jurisdição, fora do alcance das leis brasileiras. Tal problema poderia ter sido resolvido de forma mais célere, se, por exemplo, o Brasil fosse membro da Convenção de Budapeste, pois o principal objetivo, já anteriormente mencionado, é a cooperação entre os Estados.

Como o Brasil não foi signatário do Tratado, para adesão o Comitê dos Ministros do Conselho Europeu é quem deve convidar o Brasil a fazer parte. Para que o convite ocorra, a aprovação deve ser unânime entre os países membros, o que não seria impossível, tendo em vista a boa relação do Brasil com os países Europeus. O fato é que, com a adesão ao tratado, facilitaria, e muito, o combate aos crimes virtuais.

Apesar de o tratado ser uma hipótese solutiva, o Brasil possui, ainda, alguns meios de investigação, como por exemplo a infiltração de agentes da polícia com a finalidade de investigação de crimes contra a dignidade sexual de crianças e adolescentes, prevista na Lei 13.441 de 2017, desde que sejam preenchidos os requisitos constantes da referida lei, mediante autorização judicial e também a demonstração de necessidade do delegado de polícia ou do Ministério Público, dentre outros requisitos constantes no artigo 190 – A incisos I ao III. Através da autorização judicial é que se pode realizar monitoramento de redes, através de denúncias ou até mesmo suspeitas de que algum crime está sendo cometido. Porém existe uma grande defasagem na polícia e nos softwares utilizados na busca pela identidade do agente, sendo necessária a capacitação dos agentes envolvidos nas investigações, além de um investimento na infraestrutura dos meios investigativos.

Não menos importante, a devida conscientização dos internautas se faz infinitamente necessária, uma vez que a maioria dos usuários comuns não tem conhecimento dos riscos que estão escondidos ao acessar a internet, sendo um site de caráter duvidoso, o perigo de se abrir um e-mail que contenha vírus ou até mesmo ao instalar um programa em seu computador.

CONCLUSÃO

O presente trabalho demonstrou que os meios de investigação e até mesmo de punição brasileiras ainda tem muito a melhoras, mesmo possuindo formas de investigação, ainda há muita dificuldade na hora de agir. No que se refere aos procedimentos e equipamentos utilizados pelas autoridades na busca pelo agente, necessitamos a urgente evolução, tanto na polícia quanto em relação a população.

Os crimes virtuais não são uma preocupação somente do Brasil e sim mundial, e uma solução não permanente, mas iminente, momentânea, eficaz, por assim dizer, seria uma união entre Estados. Logo, a Convenção de Budapeste, que tem como objetivo combater os crimes virtuais, tipificando-os como infrações contra sistemas e dados informáticos, delitos relacionados com computadores ou seu conteúdo, pornografia infantil e seus adjacentes, aparece como melhor opção.

Impossível será encontrar uma solução definitiva para um problema em evolução. Todas as ideias são para resolver problemas momentâneos, uma vez que logo depois surgirão outros problemas. A contenção será sempre um fator a ser explorado, devendo ser assegurado que a segurança neste ambiente nunca é garantida.

Ainda que as autoridades busquem as soluções, a segurança na internet não está apenas sob suas responsabilidades, mas também da mudança da conscientização da sociedade, sendo um conjunto entre adesão ao tratado, conscientização da população através de campanhas publicitárias e educação digital, além de melhorar a capacitação dos agentes envolvidos nas investigações. Os problemas trazidos no mundo obscuro da *Deep Web* e *Dark Web* são os mesmos que existem no mundo real, cabe à sociedade adotar o comportamento correto para afastar-se da utilização deste meio.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAUJO, Felipe de Senna Silva. Sancionadas leis que tratam de crimes cibernéticos. **Migalhas**, 2012. Disponível em: https://www.migalhas.com.br/Quentes/17,MI168701,51045-Sancionadas+leis+que+tratam+de+crimes+ciberneticos. Acesso em: 19 de Out. de 2019.

ANDRADE, Leonardo. *Cybercrimes* na *deep web*: as dificuldades jurídicas de determinação de autoria nos crimes virtuais. **Jus.com.br**, 2015. Disponível em: https://jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicas-de-determinacao-de-autoria-nos-crimes-virtuais/2. Acesso em: 26 de Out. de 2019.

BARROS, Evilin. Saiba a diferença entre *surface web*, *Dark Web* e *Deep Web*, e entenda o lado obscuro da internet. **Blog Maxi Educa**, 2018. Disponível em: https://blog.maxieduca.com.br/saiba-a-diferenca-entre-surface-web-dark-web-e-deep-web-e-entenda-o-lado-obscuro-da-internet/. Acesso em: 05 de Out. de 2019.

BRAGA, Diego Campos Salgado. Métodos de investigação no âmbito cibernético. Jus.com.br, 2019. Disponível em: https://jus.com.br/artigos/71463/metodos-de-investigacoes-no-ambito-cibernetico. Acesso em: 04 de Nov. de 2019.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Rio de Janeiro, 31 Dez. 1940.

BRASIL. Decreto-Lei 13.441, de 08 de Maio de 2017. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13441.htm. Acesso em: 26 de Out. de 2019.

BRASIL. Decreto-Lei 11.829, de 25 de Novembro de 2008. Altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm. Acesso em 27 de Out. de 2019.

CARIES, Gustavo Mattos de. Responsabilidade jurídica na *deep web*: Formas de diminuição da impunidade. **Unitoledo**, 2018. Disponível em: http://www.unitoledo.br/repositorio/handle/7574/2079. Acesso em: 06 de Out. de 2019.

CONVENÇÃO SOBRE O 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 Out. 2019.

DUARTE, David; MEALHA, Thiago. Introdução à *Deep Web*. **Universidade Nova de Lisboa**, 2016. Disponível em: http://hdl.handle.net/10362/18052. Acesso em: 05 de Out. de 2019.

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.

FREITAS, Laura Campos de. Dos crimes virtuais cometidos se utilizando do anonimato da *deep web*. **Toledo Prudente**, 2019. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7789. Acesso em: 13 de Out. de 2019.

GIMENES, Emanuel Alberto Sperandio Garcia. Crimes Virtuais. **Revista doutrina TRF4**, 2013. Disponível em: http://www.revistadoutrina.trf4.jus.br/index.htm?http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html. Acesso em: 01 de Out. de 2019.

HAJE, Lara. Saiba como os crimes na internet são tratados em outros países. Câmara dos Deputados, 2011. Disponível em: https://www.camara.leg.br/noticias/217913-saiba-como-os-crimes-na-internet-sao-tratados-em-outros-paises/. Acesso em 05 de Nov. de 2019.

LINS, Luiz Fernando; VILELA, Felipe; AZEVEDO, Vitor de. *Deep Web*. Universidade Federal do Rio de Janeiro, 2018. Disponível em: https://www.gta.ufrj.br/ensino/eel878/redes1-2018-1/trabalhos-v1/deepweb/definicao.html. Acesso em: 13 de Out. de 2019.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. Crimes Virtuais. Advogado Criminalista, 2005. Disponível em: https://www.advogadocriminalista.com.br. Acesso em: 14 de Out. de 2019.

ROSSINI, Augusto Eduardo de Souza. Informática, telemática e Direito Penal. São Paulo: Memória Jurídica, 2004.

SENNA, Tel. Crimes virtuais: uma análise jurídica no Brasil. **Jus.com.br**, 2014. Disponível em: https://jus.com.br/artigos/32331/crimes-virtuais-uma-analise-juridica-no-brasil. Acesso em: 20 de Out. de 2019.

SERIBELI, Eduardo. Crime cibernético: estupro virtual e embasamento à infiltração virtual com o advento da lei 13.441/ 17. **Toledo Prudente**, 2018. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/Direito/article/view/7470. Acesso em: 12 de Out. de 2019.

SCHMIDT, Guilherme. Crimes cibernéticos. **Jusbrasil**, 2014. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. Acesso em: 06 de Out. de 2019.

SILVA, Gleice Kelly Paixão. Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na *deep web* e *dark web*. **Uni-Anhanguera**, 2019. Disponível em: http://repositorio.anhanguera.edu.br:8080/jspui/handle/123456789/227. Acesso em: 05 de Out. de 2019.

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013.