UNIVERSIDADE ESTADUAL DA PARAÍBA

CAMPUS DE CAMPINA GRANDE

CENTRO DE CIÊNCIAS JURÍDICAS

CURSO DE DIREITO

JESSYCA BELCHIOR BAZANTE DE ANDRADE

OS CRIMES COMETIDOS NA *DEEP WEB* E SEU ENQUADRAMENTO NO DIREITO PENAL BRASILEIRO

CAMPINA GRANDE - PARAÍBA

2019

JESSYCA BELCHIOR BAZANTE DE ANDRADE

OS CRIMES COMETIDOS NA *DEEP WEB* E SEU ENQUADRAMENTO NO DIREITO PENAL BRASILEIRO

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Direito, da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção de grau de Bacharel.

Orientadora: Prof.ª Dra. Ana Alice Ramos Tejo Salgado.

CAMPINA GRANDE - PARAÍBA

2019

JESSYCA BELCHIOR BAZANTE DE ANDRADE

OS CRIMES COMETIDOS NA *DEEP WEB* E SEU ENQUADRAMENTO NO DIREITO PENAL BRASILEIRO

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação de Direito da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção de grau de Bacharel.

Nota: (9,5) nove, cinco

Data da Aprovação: 08 / 03 / 2019

BANCA EXAMINADORA

Ana Alice Ramos Tejo Salgado

Prof.ª Dra. Ana Alice Ramos Tejo Salgado (Orientadora)
Universidade Estadual da Paraíba (UEPB)

Aureci Gonzaga Farias

Prof.ª Dra. Aureci Gonzaga Farias
Universidade Estadual da Paraíba (UEPB)

Rosimeire Ventura Leite

Prof.ª Dra. Rosimeire Ventura Leite
Universidade Estadual da Paraíba (UEPB)

A554c Andrade, Jessyca Belchior Bazante de.

Os crimes cometidos na Deep Web e seu enquadramento no Direito Penal Brasileiro [manuscrito] / Jessyca Belchior Bazante de Andrade. - 2019.

28 p. : il. colorido.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas , 2019.

"Orientação : Profa. Dra. Ana Alice Ramos Tejo Salgado , Coordenação do Curso de Direito - CCJ."

1. Deep Web. 2. Crimes Virtuais. 3. Direito Penal. I. Título

21. ed. CDD 345

Elaborada por Fernanda M. de A. Silva - CRB - 15/483 BSCCJ/UEPB

Dedico esta conquista primeiramente à **Deus,** pois Ele tem se mostrado presente em todos os momentos dessa longa trajetória. Tenho visto Seu agir até nos menores detalhes. Ele tem sido minha provisão, força e fortaleza. Dele sou eternamente dependente.

Dedico também aos meus amados pais, **Adriana e Nilson**, ao meu esposo **Wellington** e a nossa querida filha, **Jolye Vitória**; aos meus irmãos, **Joyce**, **Jonas** e **Jamily**, por todo apoio e estima.

AGRADECIMENTOS

A **Deus**, pois sem Ele eu nada poderia fazer, sequer existiria, o agradeço pela vida, pelo cuidado e por seu amor inigualável, rendo-lhe graças pois a conclusão desse curso é fruto do cumprimento de suas promessas em minha vida. Obrigada Senhor, por ter me dado força para vencer todos os desafios dessa jornada! Tenho visto Seu agir até nos menores detalhes.

Agradeço aos meus pais, **Adriana Belchior Lima Bazante** e **José Nilson Silva Bazante**, que apesar de muitos sacrifícios e dificuldades não mediram esforços para formar a cidadã, que hoje sou. Agradeço-lhes por sempre acreditarem em meu potencial e por instigarem o meu crescimento.

Mãe, seu cuidado e dedicação sempre me deram a esperança para prosseguir. Pai, sua presença significou a certeza e segurança de um ombro amigo.

Meus amados pais, todo carinho e esmero por vós oferecido, fizeram-me convicta de que nunca estive só nessa caminhada.

Agradeço, aos meus bisavós (IN MEMORIAN), **Josefa de Barros Lima** e **João Barros de Lima**, pois contribuíram efetivamente para construção de meu caráter, desde a mais tenra idade.

Ao meu amado esposo, **Wellington Diniz de Andrade**, que tem sido meu ajudador, meu companheiro, o ombro amigo que está sempre pronto a me oferecer consolo, carinho e cuidado. Você tem sido um exemplo de compreensão e amor, pois nunca mediu esforços para que eu pudesse concluir mais esta etapa.

A minha filha**, Jolye Vitória Belchior Bazante de Andrade**, que me fez compreender o real sentido da vida, me fez crescer como pessoa. Encontrei em ti, minha amada menina, a motivação para continuar lutando pelos meus sonhos.

Aos meus irmãos de sangue, de fé e de alma: **Joyce**, **Jonas** e **Jamily**, por todo apoio e força. Que este trabalho vos sirva como um exemplo de que coisas boas se seguem após o trabalho árduo.

À **Micaelle Faustino**, minha companheira de curso, que pacientemente me ajudou, seja como amiga, dando palavras de conforto quando necessário, seja como auxiliadora, no suporte acadêmico; sem você nada disso seria possível.

À professora, **Dra. Aureci Gonzaga Farias,** com quem partilhei momentos ímpares. Nossas conversas, durante e para além dos grupos de estudo do PIBIC, foram fundamentais. No decurso desta graduação, sua história de vida me serviu como modelo inspirador. A ti, minha sincera gratidão.

A minha orientadora, **Dra. Ana Alice Ramos Tejo Salgado**, que durante a graduação despertou meu amor pelo Direito Penal e que, com imensa paciência corrigiu minhas produções destinadas à composição deste trabalho. Sua ajuda foi fundamental para a realização do meu sonho.

Às professoras doutoras, **Ana Alice Ramos Tejo Salgado**, **Aureci Gonzaga Farias** e **Rosimeire Ventura Leite**, que de bom grado aceitaram meu convite para compor a banca examinadora, e a todos que contribuíram para a conclusão desta etapa, meu muitíssimo obrigada!

“Não to mandei eu? Esforça-te, e tem bom ânimo; não temas, nem te espantes; porque o SENHOR teu Deus é contigo, por onde quer que andares.”

Josué 1:9 (BÍBLIA SAGRADA)

OS CRIMES COMETIDOS NA *DEEP WEB* E SEU ENQUADRAMENTO NO DIREITO PENAL BRASILEIRO

Jessyca Belchior Bazante de Andrade

RESUMO

O presente artigo tem como objetivo central analisar a adequação típica de condutas praticadas na *Deep Web*, dando ênfase aos casos "*Skil Road*" e "Canibal de Rotemburgo", a partir da legislação penal brasileira. Tratando-se do tipo de pesquisa, adotou-se a qualificação que relaciona dois aspectos: os meios e os fins. Quanto aos fins, a pesquisa desenvolveu-se como exploratória e quanto aos meios, a pesquisa foi bibliográfica, sendo realizadas investigação em livros, textos normativos e artigos científicos extraídos das bases eletrônicas LILACS e SciELO. Considerando que a *Deep Web*, subcamada da internet, tem se destacado dentre as práticas criminosas, por possuir uma configuração de rede que permite o anonimato entre os usuários, questionou-se: Como tem evoluído o direito penal brasileiro a fim de reprimir a criminalidade na internet? Por fim, os resultados da pesquisa evidenciaram que o direito penal brasileiro tem caminhado a passos lentos, no que concerne à repressão dos crimes virtuais próprios, pois, ainda subsistem diversas lacunas no ordenamento nacional.

Palavras-Chave**:** *Deep Web*. Crimes Virtuais. Direito Penal. Brasil.

THE CRIMES COMMITTED TO DEEP WEB AND ITS FRAMEWORK IN BRAZILIAN CRIMINAL LAW

ABSTRACT

The main objective of this article is to analyze the typical adequacy of the behaviors practiced in the Deep Web, emphasizing the cases "Skil Road" and "Canibal de Rotemburgo", from the Brazilian penal legislation. As for the type of research, the qualification was adopted which relates two aspects: means and ends. As for the ends, the research was developed as exploratory and as for the means, the research was bibliographical, being carried out investigation in books, normative texts and scientific articles extracted from the electronic bases LILACS and SciELO. Considering that Deep Web, a sub-layer of the Internet, has stood out among the criminal practices, because it has a network configuration that allows anonymity among users, it was questioned: How has Brazilian criminal law evolved to repress criminality in Internet? Finally, the results of the research showed that Brazilian criminal law has been slow to tread in relation to the repression of its own virtual crimes, since there are still several gaps in national law.

Key words: Deep Web. Virtual Crimes. Criminal Law. Brazil.

1 INTRODUÇÃO

O presente trabalho de conclusão de curso, intitulado "OS CRIMES COMETIDOS NA *DEEP WEB* E SEU ENQUADRAMENTO NO DIREITO PENAL BRASILEIRO", tem como objetivo central analisar a adequação típica de condutas praticadas na *Deep Web*, dando ênfase aos casos "*Skil Road*" e "Canibal de Rotemburgo", a partir da legislação penal brasileira.

Os índices de criminalidade e violência têm crescido descomedidamente no seio social, ressaltando a necessidade de urgentes intervenções frente a problemática. Essa realidade também tem se propagado nos meios informacionais, sobretudo na internet, pelo fato de que, até pouco tempo ela ainda era conhecida como "território sem lei".

Hodiernamente, a *Deep Web*, subcamada da internet, tem se destacado dentre as práticas criminosas, por possuir uma configuração de rede que permite o anonimato entre os usuários. Neste desiderato, questionou-se: Como tem evoluído o direito penal brasileiro a fim de reprimir a criminalidade na internet?

Para responder tal questionamento, levantou-se a seguinte hipótese: o direito penal brasileiro tem caminhado a passos lentos, no que diz respeito à repressão dos crimes na internet; e que, portanto, esta seria a principal causa da perpetuação e da proliferação da criminalidade cibernética em território nacional.

Necessário se faz justificar a razão da escolha do tema como objeto de estudo, assim, é relevante destacar que a autora cursou a disciplina de Direito da Tecnologia e da Informação, constante na grade do curso. Por esse motivo, incrementou-se o desejo por estudar a fundo os crimes virtuais e suas consequências ao seio social. Entretanto, no decurso das pesquisas foram identificados casos de pedofilia e de tráfico de mulheres, ambos imbuídos na camada mais profunda da internet, a *Deep Web*. Nesse panorama, a *Deep Web,* enquanto meio de propagação de práticas criminosas, passou a ser concebida como novo objeto de estudos. Por conseguinte, pode-se afirmar que a pesquisa desenvolvida apresenta relevância científica e social. Esta, se inscreve nos elementos norteadores, oferecidos através dos resultados do estudo, que permitem ao público uma melhor compreensão da problemática. E aquela pois auxilia os operadores do direito e os estudiosos do ramo da informática a ampliarem seus conhecimentos.

Para tanto o trabalho foi estruturado em seis capítulos. No primeiro, "A EVOLUÇÃO TECNOLÓGICA E AS BENESSES À VIDA HUMANA", objetivou-se definir o conceito de internet, explorando sua concepção, subdivisão e evolução histórica, perpassando inclusive, por aspectos do desenvolvimento tecnológico. A segunda parte, "OS CRIMES VIRTUAIS", conceitua os crimes informáticos e classifica-os em crimes virtuais puros e impuros.

Na terceira parte, "A DEEP WEB E O ANONIMATO", teve-se como âmago conceituar o termo *Deep web* e assim destacar seu papel no *cyberespaço*. No quarto capítulo, "OS CRIMES DE MAIOR REPERCUSSÃO NA *DEEP WEB",* buscou-se destacar as adequações típicas e as cominações legais dentro do ordenamento jurídico brasileiro, para os dois casos de maior destaque na *Deep Web*: "*Skil Road*" e "Canibal de Rotemburgo".

No quinto capítulo, "OS CRIMES COMETIDOS NA INTERNET E A EVOLUÇÃO DA NORMATIVIDADE PENAL BRASILEIRA" fora realizada uma explanação demonstrando os avanços do ordenamento penal brasileiro, no que tange aos crimes virtuais próprios e impróprios. Por fim, na sexta parte, são feitas as considerações finais.

A pesquisa teve início em junho de 2018, com duração de seis meses e subdivisão em seis etapas de trabalho, quais sejam: pesquisa bibliográfica, revisão de literatura, coleta de dados; análise, discussão e interpretação dos dados coletados, procedimento exploratório e descritivo e revisão final.

Quanto ao aspecto metodológico, seguiu-se o entendimento defendido por Gil (1999, p. 26), que compreende como método todo o caminho do conhecimento científico, necessário a identificar operações mentais e técnicas que possibilitam chegar a determinado fim; e como método científico o conjunto de procedimentos intelectuais e técnicos adotados para se atingir o conhecimento. Assim, fora escolhido o método indutivo, que segundo Gil (1999, p. 28), trata-se de um procedimento que parte da observação de fatos ou fenômenos, cujas causas deseja-se conhecer, buscando-lhes peculiaridades comuns, para por fim proceder-se a generalização.

Tratando-se do tipo de pesquisa, adotou-se a taxionomia apresentada por Vergara (2016, p.41), que a qualifica em relação a dois aspectos básicos: quanto aos meios e quanto aos fins. Quanto aos fins, a pesquisa desenvolveu-se como exploratória, pois objetivou familiarizar-se com o fenômeno investigado, de modo que a pesquisa subsequente pudesse ser concebida com maior compreensão, entendimento e precisão.

Quanto aos meios, a pesquisa foi bibliográfica, tendo em vista que para a fundamentação teórico-metodológica do estudo foi realizado investigação em livros, textos normativos e artigos científicos extraídos das bases eletrônicas LILACS e SciELO. A busca eletrônica teve como alvo os artigos indexados no período de 2001 a 2018 e os seguintes descritores: "*Deep Web*", "Crimes" e "Direito Penal". Foram encontrados 18 (dezoito) artigos sobre a temática, entretanto 7 (sete) foram excluídos, pois não atendiam fidedignamente a proposta. A amostra foi composta por 10 (dez) artigos em português (na íntegra) e 13 (treze) livros e 19 (dezenove) textos normativos.

2 A EVOLUÇÃO TECNOLÓGICA E AS BENESSES À VIDA HUMANA

Desde os tempos mais remotos o ser humano tem buscado desenvolver tecnologias a fim de facilitar sua existência, perpassando pelo descobrimento e domínio do fogo, manuseio de metais, fabricação de armas, criação de medicamentos e tantas outras inovações.

Segundo Pinto (2005, p. 220) o conceito de tecnologia pode ser entendido como o conjunto de todas as técnicas de que uma sociedade dispõe, em qualquer fase histórica de seu desenvolvimento.

Para Chao (2005, p. 17), durante a trajetória evolutiva, o ser humano aprendeu a utilizar os recursos disponíveis no meio ambiente, a fim de garantir sua sobrevivência. Com o aprimoramento das práticas de domínio e com a especialização das formas de utilização dos meios existentes, o ser humano passou a compreender e apropriar-se das forças da natureza, criando assim a cultura. O autor também destaca, que as evidências científicas apontam para o fato de que, o ser humano surgiu no mundo a pouquíssimo tempo, e que mesmo assim, é o único ser vivo que teve a capacidade de dominar tecnologias capazes de transformar toda a paisagem natural, inclusive para as próprias benesses.

Dentre estas, surge a internet, como um claro sinal à necessidade de comunicação; tonando-se também uma indispensável ferramenta de pesquisa. Ela possibilita a conexão e o compartilhamento fácil e rápido de informações entre diversos dispositivos ao redor do mundo, tudo isso de modo instantâneo.

2.1 A SOCIEDADE DA INFORMAÇÃO

Durante a década de 1980, surge a chamada "Era da Informação", caracterizada por uma grande efervescência nos meios tecnológicos e no ramo de pesquisas. Paulatinamente, seus efeitos colaterais começaram a remodelar a base material da nossa sociedade, provocando transformações progressivas no modo de viver; particularmente visíveis nos avanços biotecnológicos, telecomunicacionais, industriais, nos transportes e até mesmo na área de saúde.

> É inegável que a globalização proporcionou profundas modificações na sociedade contemporânea. Este processo, iniciado na segunda metade do século XX, é fator no rompimento de barreiras econômicas entre países, integrando sociedades. Vive-se em uma aldeia global, expressão criada por Herbert Marshall McLuhan (1964). Da globalização, surge a sociedade do conhecimento, ou a nova economia, ou, ainda, a sociedade da informação. Vivemos uma economia global e informacional. (JESUS; MILAGRE, 2016, p. 14).

Para Castells (1999), essa "Sociedade Informacional" concebe uma organização social específica, pautada no processamento e na transmissão de informações, corroborando para o incremento na produtividade e no poder.

Segundo Lima (2006), esse novo padrão comportamental abre caminhos às relações em rede e à interatividade, tendendo a expandir os recursos de multimídia e ampliar a capacidade de armazenar e de gerir dados. Destarte, sem a imposição de limites geográficos ou culturais, a Era da Informação criou cidadãos ativos e conectados, tudo isso através de sua maior ferramenta: a internet.

2.2 O SURGIMENTO DA INTERNET E SUAS IMPLICAÇÕES SOCIAIS

Segundo Loveluck (2018, p. 45), as origens da internet denotam dos resultados da Agência Arpa (*Advanced Research Projects Agency*), concebida em 1958 pelo Departamento de Defesa dos Estados Unidos, a fim de coordenar pesquisas que correspondessem à altura, o disparate russo de lançar seu primeiro satélite, Sputnik. A audácia da Rússia, inflou nos Estados Unidos um sentimento de atraso, incentivando-o a desencadear um processo de remobilização da pesquisa norte-americana e de suas ligações com a defesa, especialmente no que tange a implementação de um programa espacial.

Diante dos entraves da Guerra Fria, pode-se inferir que, trata-se, portanto, de uma clara disputa pela hegemonia do poderio bélico e tecnológico, em outras palavras, uma literal corrida armamentista.

Para Zittrain (2008, p. 70), durante os processos de aperfeiçoamento, a rede informatizada recebe novas configurações, concebendo assim os ideais de generatividade da internet. Nessa sistemática a rede depara-se com numerosos desafios políticos, culturais e econômicos, perpassando pelos ideais de liberdade de expressão, de concorrência, de monopólios comerciais e de possibilidades e condicionantes de criação.

Considerando que o lapso temporal entre a concepção da internet e sua massificação fora extremamente curto, seu crescimento descomedido permitiu que diversos segmentos do conhecimento humano, fossem permeados pelo tecido cibernético. Destarte, bens jurídicos tutelados encontram-se vulneráveis nesse ambiente virtual, atraindo cada vez mais *cybercriminosos*.

3 OS CRIMES VIRTUAIS

Segundo Jesus e Milagres, (2016, p. 54), o Direito da Informática pode ser subdividido em Direito Civil da Informática e Direito Penal da Informática. Sendo importante destacar que o Direito Civil da Informática é aquele que atrai as normas, regulamentações e entendimentos jurídicos atinentes às relações privadas oriundas ou realizadas por intermédio da tecnologia da informação. Já o Direito Penal da Informática é o complexo de normas, regulamentos e entendimentos jurídicos concebidos no escopo de repreender fatos criminosos que atentem contra bens informáticos.

Os delitos informáticos, também denominados crimes virtuais correspondem aos atos infracionais reproduzidos em ambiente virtual, geralmente, onde um computador ou uma rede de computadores é utilizada como meio para a prática criminosa.

Esse epíteto engloba crimes e contravenções penais, alcançando não somente condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, sejam eles meios ou fins. Isto significa dizer, que estão inclusos também os delitos em que o computador é utilizado como meio, pois impreterivelmente estarão conectados à rede e, portanto, terão um endereçamento específico.

> [...] 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. (ROSSINI, 2004, p. 110).

Ademais, os crimes virtuais são subdivididos em próprios (puros) e impróprios (impuros).

3.1 CRIMES VIRTUAIS PRÓPRIOS

Denominam-se crimes virtuais próprios, aqueles cuja a utilização dos sistemas informacionais tornam-se imprescindíveis para a consumação do fato. Neste ensejo, essa tipologia decorre em prejuízos à segurança de sistemas, à integridade de dados e à titularidade de informações.

Para Viana (2003, p. 40-41), os crimes virtuais próprios são:

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

Já o doutrinador Jesus entende-os como:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado. (JESUS, 2003, p.77).

Assim, diante dessas convicções, temos como exemplo de crimes virtuais próprios, os acessos não autorizados (*hacker* ou *cracker*), a disseminação de vírus, o embaraçamento ao funcionamento de sistemas e as condutas tipificadas nos artigos 313-A e 313-B do Código Penal.

Neste ponto, é necessário que se faça um adendo, pois socialmente os termos *hacker* e *cracker* são usados como sinônimos, enquanto que na realidade há uma nítida diferença entre os conceitos.

Define-se como hackers aqueles que modificam softwares, desenvolvendo funcionalidades, encontrando falhas em sistemas e ajudando a corrigi-las. Estes operadores cibernéticos também são conhecidos com *White-hats* (chapéus brancos), pois utilizam de seus conhecimentos para legalmente melhorar a segurança de sistemas. Em contrapartida, os crackers, também denominados *Black-hats* (chapéus negros), são indivíduos que invadem computadores ou sistemas a fim de concretizar propósitos ilícitos.

> Os hackers direcionam seu potencial para construir, não destroem ou roubam dados de forma intencional, compartilham informações deixando rastros de passagem abertas para que administradores de rede possam fazer correções; eles têm como objetivo aprender mais, pois são autodidatas e gostam de desafios. Já os Crackers são os indivíduos que utilizam suas habilidades em benefício próprio, não importando quantos ou quais prejuízos causem; são elementos perigosos e prepotentes, deixam mensagens do tipo: "Eu sou o melhor! Apaguei e escapei!". (ANONYMOUS, 1998).

Destarte, é importante ressaltar que o próprio governo brasileiro já foi vítima da ação de crackers. No ano de 2011, os sites do Instituto Brasileiro de Geografia e Estatística (IBGE) e da Empresa Brasileira de Infraestrutura Aeroportuária (INFRAERO) foram invadidos, gerando grandes transtornos à coletividade.

Neste cerne, hodiernamente, a melhor adequação típica faz-se presente nos artigos 154-a e 226 do Decreto Lei nº 2.848/40, que prevêm punição específica para quem invadir dispositivo informático alheio, tendo como âmago a adulteração ou destruição de dados ou informações; ou mesmo para quem interrompa, impeça ou dificulte o reestabelecimento de serviço telemático ou de informação de utilidade pública.

No Brasil, outro importante avanço legal no combate aos crimes virtuais próprios, diz respeito a Lei 9.983/ 2000, que propiciou atualização no Código Penal, ensejando sobre a proteção aos bancos de dados e aos sistemas de informações governamentais. Desde então, os artigos 313-A e 313-B do Código Penal passaram a criminalizar a violação de informações contidas nas bases de dados da Administração Pública, encetadas por seus próprios funcionários.

Destarte, os artigos supracitados tratam de duas modalidades dos crimes funcionais, a inserção de dados falsos em sistemas de informações e a modificação ou alteração não autorizada de sistema de informações. Esses delitos também são conhecidos como crimes próprios, pois a condição de funcionário público é um elemento essencial para a configuração do crime.

Segundo o artigo 327 do Código Penal, considera-se funcionário público todo indivíduo legalmente investido, que exerce cargo, emprego ou função pública, mesmo que de forma transitória e sem remuneração.

Especificamente, o artigo 313-A constitui-se em um peculato eletrônico, pois o agente altera dados, exclui-os indevidamente, insere-os ou facilita a inserção, em sistemas ou bancos de dados da Administração pública, objetivando o alcance de vantagem indevida, seja para si ou para terceiros. Já no artigo 313-B, o agente modifica ou altera sistema ou programa informático sem a devida autorização ou solicitação de autoridade competente. Esses crimes recebem respectivamente as seguintes penas: reclusão de 2 a 12 anos, e multa; e detenção de 3 meses a 2 anos, e multa.

3.2 CRIMES VIRTUAIS IMPRÓPRIOS

Define-se como crimes impróprios aqueles onde o agente se utiliza de um equipamento com conexão à internet, para através dele produzir resultado naturalístico.

> Os crimes impróprios consistem em uma nova forma de praticar crimes já existentes, no qual o computador e a internet são utilizados como instrumentos para a realização de um delito já tipificado pela legislação brasileira, como o caso dos crimes contra a honra que são injuria, calúnia e difamação. (LIRA, 2010, p. 4).

Como exemplo de crimes virtuais impróprios, em que se admite a sua prática por meio da internet temos: a pedofilia (artigos 241 e 241-A da Lei 8.069/90) e a divulgação de cenas de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia (artigo 218-C da Lei nº 13.718/ 2018).

Ademais, podem-se citar tantos outros crimes virtuais impróprios já cometidos através da *Deep Web*: extorsão (artigo 158 do CP), formação de grupos para fins ilícitos (artigo 2º da Lei 12.850/ 2013), terrorismo (artigo 20 da Lei nº 7.170/1983), contrabando de mercadorias e de materiais radioativos (artigos 334 e 334-A da Lei nº 13.008/ 2014), prostituição adulta e infanto-juvenil (artigos 229 e 230, § 1º do Código Penal), tráfico de drogas (artigo 33 da Lei nº 11.343/2006), tráfico de pessoas (artigo 149-A do CP) e de órgãos humanos (artigo 14, § 1º da Lei 9.434/1997), assassinato por aluguel (artigo 121, §v 2º, I do CP), sequestro (artigo 148 do CP), falsificação de moedas em curso, de cartões de crédito e identidades civis (artigos 297 e 298 do CP). Por conseguinte, qualquer ação tipificada nas leis supracitadas, ainda que cometida por meio virtual, desencadeará prejuízos a(s) vítima(s) no mundo físico.

4 A *DEEP WEB* E O ANONIMATO

Hodiernamente, o conceito de *Deep web* permanece até então, como uma temática pouco explorada pela doutrina nacional e até mesmo internacional, mas que demanda extrema atenção, tendo em vista que ela tem se destacado como um instrumento facilitador para o cometimento de inúmeros crimes.

Vulgarmente conhecida como *Deepnet*, *Undernet*, Web Oculta ou mesmo Web Invisível, a *Deep Web* figura como um conjunto de páginas e serviços inacessíveis ao grande público, ema outras palavras, trata-se de uma espécie de ambiente de navegação que não sofre, até os dias de hoje, nenhum tipo de regulamentação ou controle. Sua arquitetura diferenciada permite que usuários acessem a rede de maneira anônima, tendo em vista que os mecanismos de busca convencionais, não conseguem se conectar às páginas requisitadas, mesmo que contenham expressão ou conteúdo chave.

Ressalta-se ainda, que a *Deep Web* é um ambiente amplo, chegando a ser quinhentas vezes maior do que a "surface" (internet convencional). Ela também é conhecida por subdividir-se em camadas, ou seja, quanto mais profundo o acesso, mais sigiloso e perigoso pode ser o conteúdo encontrado.

Segundo Abreu e Nicolau (2014, p. 120), a *Deep Web* funciona como um universo paralelo, composto por sistemas que trabalham com redes anônimas, fornecedoras de conteúdos escondidos. Por conseguinte, nenhuma de suas páginas é localizada através dos tradicionais mecanismos de busca; entretanto, o fator mais alarmante diz respeito ao fato de que esta subcamada ocupa uma área bastante significante no campo da internet.

Os autores também sustentam a ideia de que, os processos criptográficos são o aparato fundamental para a ostensível invisibilidade dos dados em rede, pois oferecem o subsídio do anonimato aos usuários mal intencionados.

Diante da complexidade de seus mecanismos e de sua robusta capacidade emancipatória, a subcamada tem se apresentado como um monstro em potencial às polícias de todo mundo, preocupando governos e a própria sociedade.

Diversas denúncias cerceiam a *Deep Web*, principalmente por envolverem esquemas de prostituição adulta e infanto-juvenil, formação de grupos para fins ilícitos, terrorismo, contrabando de mercadorias e de materiais radioativos, extorsão; tráfico de drogas, pessoas e órgãos humanos, grupos de canibalismo, assassinato por aluguel, sequestro, falsificação nos diversos âmbitos, incluindo a de moedas em curso, cartões de crédito e identidades civis.

Assim, imersa nas profundezas da rede, essa subcamada é muitas vezes um local propício a diversas ações delituosas, impondo grandes riscos à coletividade. Para tanto, reivindica-se que sejam tomadas medidas para resguardar as tutelas individuais e coletivas.

5 OS CRIMES DE MAIOR REPERCUSSÃO NA *DEEP WEB*

Dentre os crimes praticados na *Deep Web*, os que alcançaram maior notoriedade foram: *Silk Road* e Canibal de Rotemburgo, ambos interligados pelo alto grau de reprovabilidade social.

5.1 *SKIL ROAD*

O termo *Skil Road* foi concebido para denominar um *website*, que funcionava através do sistema de *marketplace*, também conhecido como *ecommerce*. Sua diagramação era idealizada para oferecer comodidade e segurança de dados aos usuários, portanto, o acesso ao seu endereço de rede só era possível através de um navegador específico, o Tor.

O *website* dispunha de uma interface subdividida em tópicos e categorias expansíveis, facilitando o acesso e a identificação dos produtos; oferecendo também carrinhos de compras virtuais e serviços de pagamento com moedas digitais criptografadas, como o *bitcoin* e o *litecoin.*

> O Silk Road não é, em si, uma loja. Em vez disso, ele fornece a infraestrutura para que os vendedores e compradores realizem transações em um ambiente online que preza pelo anonimato dos interagentes. O acesso à página só é

> possível através do navegador Tor e o único meio de pagamento aceito pelo site é o Bitcoin. (HOFFMANN, 2014, p. 12).

Entretanto, a principal problemática está centrada no fato de que esta página se voltava para a comercialização de substâncias controladas e de narcóticos.

Segundo Christin (2013), o site também comercializava bens de conteúdo pornográfico, armamentos, bens digitais, e moedas virtuais. Geralmente, esses itens ficavam disponíveis por apenas três semanas, em seguida, eram retirados da plataforma. Ainda de acordo com o autor, outra estratégia para preservar a identidade de seus usuários, diz respeito ao fato de que, a maioria dos vendedores, simplesmente desaparecia, em média, depois de três meses com o cadastro ativo.

As vendas no website funcionavam da seguinte forma: uma vez realizada a compra, o produto deveria ser enviado ao destinatário via correio, entretanto, no momento das transações, orientava-se para que o comprador enviasse um endereço físico diferente do residencial. Uma vez entregue, o comprador tinha por obrigação avisar à Silk Road, para que só então ela liberasse os fundos ao fornecedor. Após este processo, todos os endereços e dados eram apagados do sistema.

Neste desiderato, após longas investigações, em 2013, Ross William Ulbricht, suspeito de ser o dono e principal administrador da *Silk Road*, foi preso pelo *Federal Bureau of Investigation* - (FBI) e o website teve suas atividades encerradas.

De acordo com Ciancagline (2013, p. 11), o FBI apurou que em quase dois anos de existência, o comércio desenvolvido na *Silk Road* levantou uma quantia aproximada de 9 milhões e meios de bitcoins, além de colecionar outros 600 mil oriundos da coleta de comissões em vendas. Esse montante, à época, era equivalente a aproximadamente 12 bilhões de dólares em vendas e 80 milhões em comissões.

5.2 ADEQUAÇÕES TÍPICAS E COMINAÇÕES LEGAIS NO ORDENAMENTO BRASILEIRO PARA O CASO "SKIL ROAD"

Por conseguinte, considerando que as práticas supracitadas fossem adequadas ao ordenamento brasileiro, teríamos a seguinte cominação legal: Tráfico internacional de drogas (Lei nº 11.343), e tráfico internacional de armas de fogo (Lei 10.826/03).

No que concerne ao tráfico internacional de drogas, encontramos respaldo na Lei nº 11.343, que define em seu artigo 1º, parágrafo único, o conceito de drogas: "Para fins desta Lei, consideram-se como drogas as substâncias ou os produtos capazes de causar dependência,

assim especificados em lei ou relacionados em listas atualizadas periodicamente pelo Poder Executivo da União."

Com relação aos delitos, encontramos perfeita tipificação nos artigos 33 e 40 do mesmo instrumento legal, tendo em vista que Ross William Ulbricht vendia internacionalmente substâncias controladas e narcóticos, portanto, importava, exportava e fornecia drogas transnacionalmente.

Ademais, é necessário ressaltar que o tráfico de drogas trata-se de crime contra a saúde pública, sendo pois classificado como: crime comum (pode ser praticado por qualquer pessoa), de perigo abstrato (não exige a ocorrência do dano, bastando a realização da conduta proibida para que se presuma o perigo ao bem tutelado), de mera conduta (a conduta do agente, por si só, configura o crime), de ação múltipla (o crime que descreve várias condutas no mesmo artigo, ou seja, descreve uma variedade de verbos como núcleos do tipo), unissubjetivo (mesmo que o agente pratique, em um mesmo contexto fático, mais de uma ação típica, responderá por crime único, haja vista o princípio da alternatividade), e plurisubsistente (não admite a tentativa, tendo em vista que qualquer início de execução já caracterizaria um das condutas alternativas).

Logo, como se trata de crime de perigo abstrato contra a saúde pública, o sujeito passivo é a coletividade. Por conseguinte, a ação penal pública será incondicionada à representação, cabendo ao Ministério Público o oferecimento da denúncia.

Já no que se refere ao tráfico internacional de armas de fogo, temos como embasamento os artigos 18, 19 e 21 da Lei 10.826/03, pois Ulbricht favorecia a saída de armas de fogo de variado calibre, incluindo as de uso proibido ou restrito, além de suas munições e acessórios. Portanto, é necessário salientar que o tráfico internacional de armas de fogo, caracteriza-se como crime comum, de perigo e de mera conduta.

Destarte, no que tange ao tráfico de drogas, segundo os artigos 33 e 40, I, do Código Penal, a cominação adequada estaria entre cinco e quinze anos de reclusão, com um aumento de pena entre um sexto e dois terços, mais multa de quinhentos a mil e quinhentos dias-multa**.** Já no caso do tráfico internacional de armas de fogo, segundo os artigos 18, 19 e 21 do Código Penal, teríamos uma pena de reclusão variável entre quatro e oito anos, aumentada de metade e multa. Sendo-lhe insuscetível a liberdade provisória.

Dessa maneira, considerando que o caso em tela apresenta concurso material de crimes, as penas serão dosadas separadamente e posteriormente somadas. Assim, a título exemplificativo teríamos um mínimo de onze anos e dez meses de reclusão; sendo cinco anos e dez meses = cinco anos mais um sexto da pena, referentes ao crime de tráfico de drogas e seis anos = quatro anos mais metade da pena para o tráfico internacional de armas de fogo; e multa.

Já como máximo, teríamos a seguinte pena: trinta e sete anos de reclusão, sendo vinte e cinco anos = quinze anos mais dois terços da pena referentes ao crime de tráfico de drogas e doze anos = oito anos mais metade da pena para o tráfico internacional de armas de fogo; e multa.

5.3 CANIBAL DE ROTEMBURGO

O caso narrado corresponde aos fatos criminosos praticados pelo alemão Armin Meiwes, no ano de 2001, com o intermédio da *Deep Web*.

Segundo pesquisa realizada e registrada nos autos processuais, Armin Meiwes, também conhecido como Canibal de Rotemburgo, passou a realizar buscas voltadas à temática canibalesca a partir do ano de 1999. Suas pesquisas também versavam sobre "instruções para estripamento" do corpo humano. Neste decurso temporal, Meiwes montou em sua residência um quarto específico para a execução e só então passou a sondar possíveis vítimas na *Deep Web*.

Os autos também afirmam que Armin passou a identificar-se na internet como "Antropófago" e a usar o seguinte descritor: "homem gay procura homem forte 18-30 anos para abater".[1] Considerando que suas exigências eram rigorosíssimas, o Canibal de Rotemburgo manteve contato com mais quatrocentos homens, entretanto, apenas em janeiro de 2001, encontrou sua vítima, Bernd Jürgen Armando Brandes, um berlinense de 42 anos.

No dia nove de março de 2001, Bernd, que também possuía alguns distúrbios sexuais, permitiu que Meiwes decepasse seu pênis; logo em seguida, o membro foi frito e ambos o consumiram.

Todavia, apenas em momento posteriormente, Armin Meiwes decidiu posicionar uma câmera e então dar cabo à vida de sua vítima. Primeiramente, desferiu-lhe dois golpes com instrumento perfurocortante, à altura do pescoço. Após tal fato, seguindo instruções da internet, dissecou e congelou cerca de vinte e quatro quilogramas de carne, a qual consumiu pela primeira vez em 12 de março de 2001.

Após este desfecho, o canibal voltou a procurar por vítimas em potencial, onde finalmente um jovem com o qual mantinha contato, alertou a polícia, o que acabou culminando em uma série de investigações e em sua prisão.

---

[1] Tradução livre da Sentença do Tribunal que apreciou o recurso da decisão de primeira instância. BUNDESGERICHTSHOF. Urteil des 2. Strafsenats vom 22.4.2005 - 2 StR 310/04. Disponível em: < http://juris.bundesgerichtshof.de/cgibin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=0c1607e20879c6d690a67d0cbcb2b243&nr=3267 5&pos=0&anz=1>. Acesso em 12 de janeiro de 2019.

5.4 ADEQUAÇÃO TÍPICA E COMINAÇÕES LEGAIS NO ORDENAMENTO BRASILEIRO PARA O CASO "CANIBAL DE ROTEMBURGO"

Considerando que as práticas supracitadas fossem adequadas ao ordenamento brasileiro, teríamos a seguinte adequação típica: Lesão corporal de natureza grave (artigo 129, § 2, III, do Código Penal), homicídio duplamente qualificado (artigo 121, § 2°, II e III do Código Penal) e destruição, subtração ou ocultação de cadáver (artigo 211 do CP). Sendo importante ressaltar que, no caso em tela, a lesão corporal grave configura-se como um crime autônomo, pois apenas em momento posterior o agente decide pela prática do homicídio, ensejando em uma nova conduta criminosa.

A lesão corporal de natureza grave decorre da perda do membro, que neste caso, seria o pênis da vítima. Neste ponto, deve-se ressaltar que o consentimento da vítima não tem relevância jurídica, haja vista que o artigo 13 do Código Civil veda a disposição do próprio corpo se ela resultar em diminuição permamente da integridade física – "Art. 13. Salvo por exigência médica, é defeso o ato de disposição do próprio corpo, quando importar diminuição permanente da integridade física, ou contrariar os bons costumes.". Logo, Bernd Jürgen jamais poderia legalmente assentir que Armin Meiwes decepasse seu pênis.

Tendo como ponto de partida a informação de que Meiwes, matou Bernd Jürgen para obter satisfação sexual, constatamos então a primeira qualificadora: o homicídio por motivo fútil (artigo 121, § 2°, II, do Código Penal). Percebe-se também que o agente amputou o pênis da vítima e que somente em momento posterior, decidiu desferir-lhe golpes à altura do pescoço, ceifando-lhe a vida. Concebendo assim, mais uma qualificadora, o homicídio cometido através de meio cruel. (artigo 121, § 2°, III, do CP).

Ainda nesse caso, podemos verificar que Armin Meiwes dissecou, congelou e consumiu o corpo da vítima, e que por isso cometeu o crime previsto no artigo 211 do Código Penal, a destruição, subtração ou ocultação de cadáver.

Logo, no que tange à lesão corporal de natureza grave, teríamos como cominação uma pena de reclusão, de dois a oito anos. No caso do homicídio duplamente qualificado, por motivo fútil e meio cruel seria estabelecido uma pena de reclusão, de doze a trinta anos; e se tratando da destruição e ocultação do cadáver, teríamos uma pena de reclusão, variando de um a três anos, e multa.

Portanto, considerando que o caso em tela apresenta concurso material de crimes, as penas serão dosadas separadamente e posteriormente somadas. Assim, a título exemplificativo teríamos um mínimo de quinze anos, e multa; sendo dois anos referentes à lesão corporal grave,

doze anos pelo homicídio duplamente qualificado e um ano pela destruição e ocultação de cadáver.

Em contrapartida, como pena máxima teríamos um total de quarenta e um anos de reclusão, e multa. Sendo oito referentes à lesão corporal grave, trinta anos pelo homicídio duplamente qualificado e três anos pela destruição e ocultação de cadáver.

6 OS CRIMES COMETIDOS NA INTERNET E A EVOLUÇÃO DA NORMATIVIDADE PENAL BRASILEIRA

A expansão tecnológica à nível mundial é um processo notório e factual, portanto, não seria diferente em território brasileiro. Com a popularização da internet, dos computadores, *smartphones* e *tablets*, novos caminhos têm sido abertos às práticas criminosas, todavia, infelizmente, nosso ordenamento jurídico não tem conseguido acompanhar a evolução desses delitos cibernéticos.

Como afirma Ivette Senise Ferreira (2001, p. 208), o crescimento da informatização trouxe às mãos dos criminosos novos instrumentos para perpetuar suas práticas, corroborando assim com o surgimento das mais variadas modalidades de lesões, seja a bens ou a interesses; incumbindo, portanto, o Estado desta tutela. Entretanto, apenas nas últimas décadas o Brasil passou a preocupar-se efetivamente com a temática. Segundo os dados apresentados pelo Colégio Notarial do Brasil (CNB), o número de crimes virtuais no país aumentou em setenta por cento entre 2012 e 2013. (KURTZ, 2014, p. 1). Tais números, meramente exemplificativos, demonstram a urgente necessidade de esforços para que o Direito Penal possa proteger os cidadãos dos riscos da sociedade da informação.

Até o início do século XXI, não havia nenhum instrumento legal para punir os crimes cibernéticos próprios, existindo leis apenas para o combate aos crimes impróprios. Por esse motivo, no ano de 2000, fora promulgada a Lei 9.983, que ensejou na criação dos artigos 313-A e 313-B do Código Penal. Esses versam sobre a proteção aos bancos de dados e aos sistemas de informações governamentais.

Ulteriormente, em virtude de alguns ataques a sites do governo e à divulgação de fotos íntimas da atriz Carolina Dieckmann, dois instrumentos normativos foram sancionados com maior urgência, quais sejam, a Lei 12.735/2012, mais conhecida como "Lei Azeredo", e a Lei 12.737/2012, também denominada "Lei Carolina Dieckmann".

Fruto do Projeto de Lei 84/99, a "Lei Azeredo", alterou o inciso II do § 3° do artigo 20 da Lei n° 7.716/1989, denominada Lei do Crime Racial, a fim de permitir que qualquer juiz

solicite a retirada de conteúdo discriminatório dos mais diversos meios comunicativos, inclusive em rádio, TV ou internet. A lei em cerne, também determina que os órgãos da polícia judiciária criem delegacias especializadas no combate aos crimes virtuais.

Já a Lei 12.737/12, apelidada "Carolina Dieckmann" criou o tipo penal "invasão de dispositivo informático", hoje previsto no artigo 154-A do Código Penal Brasileiro. Além da incorporação desse dispositivo, a composição dos delitos previstos no artigo 266, do mesmo diploma legal, foi ampliada. O tipo penal de indisponibilização passou a englobar serviços telemáticos ou de informação de utilidade pública. Já no caso de falsificação de documentos, a nova lei passou a equiparar os cartões de crédito ou débito a documento particular.

Entretanto, a Lei Dieckmann também apresenta grandes falhas, primeiramente por não considerar como crime a indisponibilidade de sistemas de informação de entidades privadas; assim como não usou de tecnicidade. Ao apropriar-se do termo "dispositivo informático" deixou especificamente de abranger grande parte dos *smartphones* e *smath tvs*, que na realidade são dispositivos eletrônicos. Ademais, a harmonização de termos técnicos é imprescindível para a efetiva abrangência de um tipo penal, tanto próprio, quanto impróprio.

Outra lacuna diz respeito ao fato de que no artigo 154-A do Código Penal, o legislador não se ateve ao simples ato de "vasculhar" o dispositivo eletrônico, firmando-se apenas a "obter, adulterar ou destruir".

Outrossim, no ano de 2014, o ordenamento pátrio foi enriquecido com a Lei 12.965/2014, oficialmente qualificada como Marco Civil da Internet, que por sua vez, passou a estabelecer aos usuários e ao Estado, princípios, garantias, direitos e deveres no uso da internet. Entretanto, por mais que pareça eficaz, algumas lacunas podem ser apontadas, uma delas diz respeito ao ato de introduzir ferramentas judiciais físicas ao contexto virtual, como a obtenção de ordem judicial. Este fato remonta em contra produtividade, pois há uma clara divergência entre as velocidades dos dois mundos, o primeiro é eivado pela morosidade, enquanto que o segundo pela celeridade.

Todavia, além legislações supracitadas, ainda tem-se a Lei nº 11.829/2008, que combate a pornografia infantil na internet; a Lei nº 9.609/1998, que trata da proteção da propriedade intelectual do programa de computador; a Lei nº 9.296/1996 que disciplinou a interceptação de comunicação telemática ou informática; e a Lei nº 12.034/2009, que delimita os direitos e deveres dentro da rede mundial, durante as campanhas eleitorais.

Destarte, é necessário ressaltar à nível penal não houveram modificações significativas no que tange aos crimes cometidos por meio da internet. Os chamados crimes virtuais impróprios, seguem punidos com a previsão constante no Código Penal brasileiro.

7 CONSIDERAÇÕES FINAIS

Acalorado pelas urgentes demandas sociais, o ordenamento jurídico brasileiro, até então defasado, passa a fazer frente a algumas condutas ilícitas na seara da informática. Para tanto, após longas discussões, emergem as Leis 9.983/2000, 12.735/2012 (Lei Carolina Dieckman), 12.737/2012 (Lei Azeredo) e 12.965/2014 (Marco Civil), buscando mitigar tal problemática.

Neste cerne, é necessário destacar que a ausência de legislação especifica mostra-se como um retrocesso no processo de combate ao *cybercrime,* tendo em vista que ela poderia fornecer elementos contundentes para a erradicação dos delitos de tal natureza.

Ademais, diante da manifesta conjuntura pode-se concluir que o direito penal brasileiro tem caminhado a passos lentos, no que concerne à repressão dos crimes virtuais próprios, pois, ainda subsistem diversas lacunas no ordenamento nacional.

Não obstante, embora exprimam um avanço significativo no combate à criminalidade na internet brasileira, as leis pátrias deixaram a desejar em vários aspectos, restando muito a ser feito quanto a criminalidade digital; por exemplo, a Lei 12.737/2012 (Carolina Dieckmann), deve sofrer reformulação e assim passar a considerar como crime a indisponibilidade dos sistemas de informação de entidades privadas. Nesse mesmo diploma legal, torna-se imperiosa a trocar do termo "dispositivo informático" por "dispositivo eletrônico", a fim de que todos os dispositivos tecnológicos que disponham de conexão com a internet, sejam abrangidos.

No que tange ao artigo 154-A do Código Penal, torna-se imprescindível que os verbos núcleo do tipo penal sejam reorganizados, de modo que se inclua o termo "sondar", entre os já previstos ("obter, adulterar ou destruir"), tudo isso a fim de extinguir possíveis lacunas. Já em relação à Lei 12.965/2014 (Marco Civil da Internet), torna-se necessária a desvinculação da obtenção de ordens judiciais, através da criação de ferramentas próprias ao contexto virtual, a fim de garantir a celeridade e a plena produtividade.

Destarte, torna-se sine qua non que leis específicas sejam instituídas, buscando acompanhar as constantes transformações socias, tudo isso a fim de resguardar fidedignamente a segurança social e sobretudo os direitos fundamentais da pessoa humana, proporcionando assim o fortalecimento da sociedade, em plena "Era da Informação".

REFERÊNCIAS

ABREU, Giovanna; NICOLAU, Marcos. A estética do anonimato na deep web: a metáfora das máscaras e do homem invisível aplicada ao "submundo" da internet. **Revista Culturas Midiáticas**. João Pessoa, ano VII, n. 12, p. 119-134, jan./jun. 2014.

ANONYMOUS. **Maximum Security**: a hacker's guide to protecting your internet site and network. Indianapolis: SAMS Publishing, 1998.

BRASIL. Código Penal. Decreto-lei nº 2.848, de 7 de dezembro de 1940. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei nº 7.170, de 14 de dezembro de 1983. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei nº 7.716, de 5 de janeiro de 1989. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Estatuto da criança e do adolescente. Lei nº 8.069, de 13 de julho de 1990. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei nº 9.296, de 24 de julho de 1996. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei nº 9.434, de 4 de fevereiro de 1997. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei nº 9.609, de 19 de fevereiro de 1998. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei no 9.983, de 14 de julho de 2000. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Código Civil. Lei nº 10.406, de 10 de janeiro de 2002. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Estatuto do Desarmamento. Decreto-lei n. 10.826, de 22 de dezembro de 2003. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei nº 11.343, de 23 de agosto de 2006. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei nº 11.829, de 25 de novembro de 2008. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei nº 12.034, de 29 de setembro de 2009. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei nº 12.735, de 30 de novembro de 2012. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei nº 12.737, de 30 de novembro de 2012. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei nº 12.850, de 2 de agosto de 2013. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei nº 12.965, de 23 de abril de 2014. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei nº 13.008, de 26 de junho de 2014. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

_____. Lei nº 13.718, de 24 de setembro de 2018. ***Vade mecum***. São Paulo: Revista dos Tribunais, 2018.

CALDERON, Barbara Idaerla Santos. **Em que medida a deep web aumenta a difusão de poder.** 59f. Monografia (Bacharelado em Relações Internacionais) – Universidade Federal de Santa Catarina, Florianópolis, 2014. Disponível em :< https://repositorio.ufsc.br/xmlui/handle/123456789/128072>. Acesso em: 14 out. 2018.

CARNEIRO, Daniele Soares (Coord.). **Manual de normalização de documentos científicos de acordo com as normas da ABNT**. Curitiba: UFPR, 2015. – (Normas para apresentação de documentos científicos).

CARVALHO, Ivan Lira de. **Crimes na Internet. Há como puni-los**. Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: <http://jus.com.br/revista/texto/2081>. Acesso em: 03 maio. 2014

CASTELLS, Manuel. **A sociedade em rede**. A era da informação: economia, sociedade e cultura; v.1. São Paulo: Paz e Terra, 1996.

CHAO, Cheng Hsin Nery. **Universidade e educação ambiental**. 230f. Tese (Doutorado em Educação) - Universidade Federal do Rio Grande do Norte, Natal, 2005.

CHRISTIN, Nicolas. **Traveling the Silk Road**: a measurement analysis of a large anonymous online marketplace. Disponível em:< https://arxiv.org/abs/1207.7139>. Acesso em: 22 dez. 2018.

FERREIRA, Ivette Senise. A Criminalidade Informática. In: LUCCA, Newton; SIMÃO FILHO, Adalberto. **Direito & Internet**: Aspectos Jurídicos Relevantes. São Paulo: Quartier Latin, 2001.

HOFFMANN, Thayse Vasconcelos. **SILK ROAD ANONYMOUS MARKET**: um estudo de caso sobre o comércio anônimo na deep web. 94f. Trabalho de Conclusão de Curso (Bacharelado em Relações Públicas) – Faculdade de Economia e Comunicação, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

JESUS, Damásio de. **Tráfico Internacional de Mulheres e Crianças** – Brasil. São Paulo: Saraiva, 2003.

KURTZ, João. **Registros de ocorrências de crimes virtuais aumentam 70% no país em 1 ano**. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2014/10/registros-de-ocorrencias-decrimes-virtuais-aumentam-70-no-pais-em-1-ano.html>. Acesso em: 07 jan. 2019.

LIMA, Joaquim Manuel Martins do Vale. **As Novas Tecnologias no Ensino**. Disponível em: <http://www.airpower.au.af.mil/apjinternational/apj-p/2006/2tri06/lima.html>. Acesso em 18 dez. 2018.

LIRA, Kalliane Wilma Cavalcante. CAVALCANTI, Jose Ivalmir Neves. **Crimes praticados via internet e suas conseqüências jurídicas**. 2010.

LOVELUCK, Benjamin. **Redes, liberdades e controle**: uma genealogia política da internet. Petrópolis: Vozes, 2018.

MAURYA, Shivam. **What is deep web? How you can access deep web, is it legal?** Disponível em: <http://stuffboxnews.com/what-is-deep-web-how-you-can-access-deep-web-is-it-legal/>. Acesso em: 09 fev. 2019.

PINTO, Álvaro Vieira. **O conceito de tecnologia**. Rio de Janeiro. Contraponto, 2005.

RAMALHO, David Silva. A investigação criminal na dark web. **Revista de Concorrência e Circulação**, Lisboa, ano IV, n 14/15, p. 383-429, abr./set. 2013.

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

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet:** construção e aplicação Juiz de Fora. Editar Editora Associada Ltda, 2016.

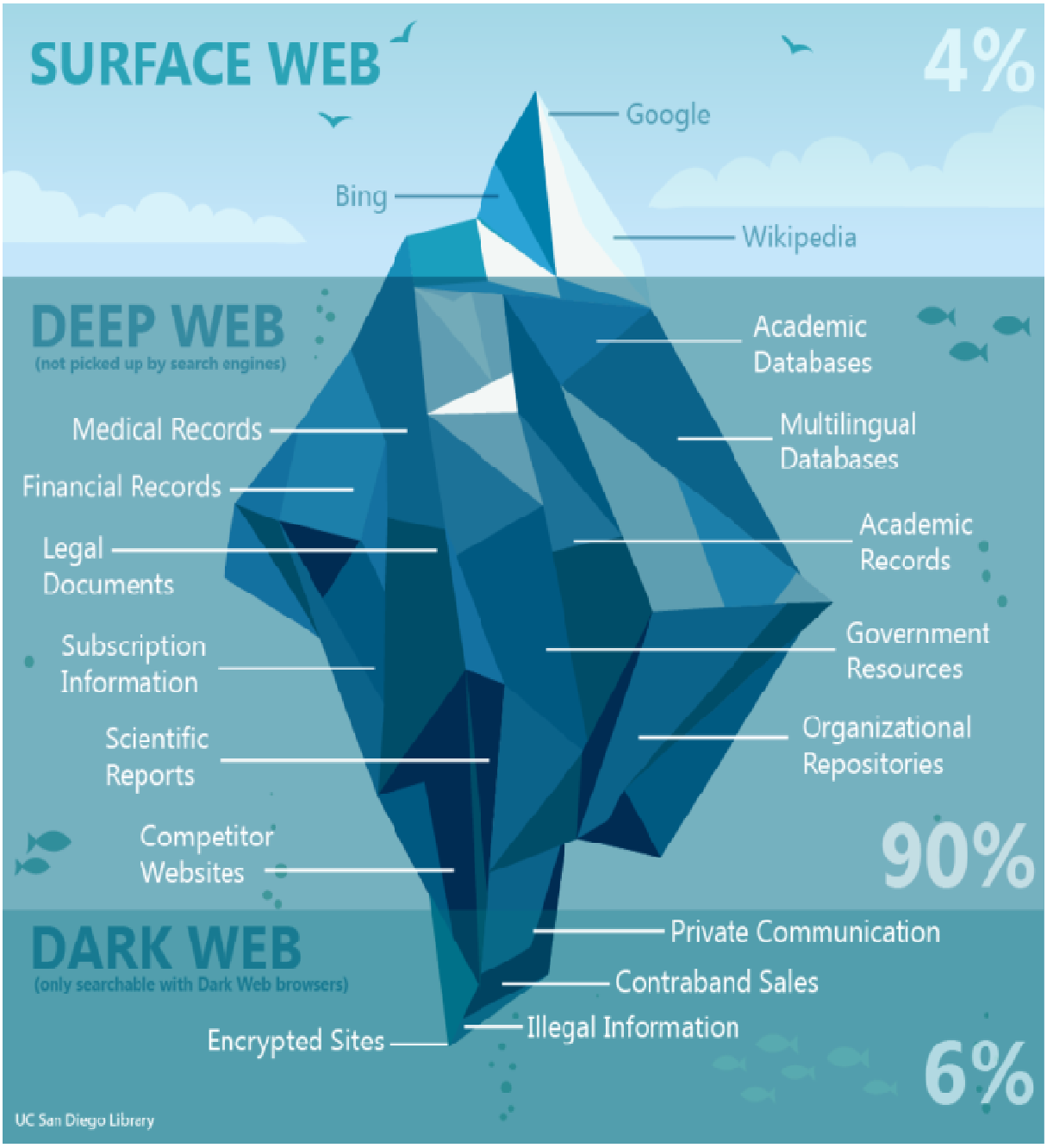
VERGARA. Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. 16. ed. São Paulo: Atlas, 2016.

VIANA, Túlio. **Fundamentos de direito penal informático**. Do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003, p. 40-41.

ZITTRAIN, Jonathan. **The future of the internet**: and how to stop it. New Haven; London: Yale University Press, 2008.

ANEXO 1

FIGURA 1 – CAMADAS DA INTERNET



FONTE: MAURYA, Shivam. Disponível em:< http://stuffboxnews.com/what-is-deep-web-how-you-can-access-deep-web-is-it-legal/>. (2017).

ANEXO 2

FIGURA 2 – PÁGINA FRONTAL DO WEBSITE *SKIL ROAD*

FONTE: CHRISTIN, Nicolas. **Traveling the Silk Road**: a measurement analysis of a large anonymous online marketplace. (2012)