LUCIANO SEBASTIÃO DE SOUZA SILVA

CYBER ESPAÇO E OS DESAFIOS DO ANONIMATO

Uma análise do sistema de camadas da WEB e seus reflexos na legislação brasileira

São Lourenço/MG

2022

LUCIANO SEBASTIÃO DE SOUZA SILVA

CYBER ESPAÇO E OS DESAFIOS DO ANONIMATO

Uma análise do sistema de camadas da WEB e seus reflexos na legislação brasileira

Trabalho de Conclusão de Curso apresentado pelo aluno Luciano Sebastião de Souza Silva como requisito para obtenção do título de Bacharel, do Curso de Direito, da Faculdade de São Lourenço.
Orientador: Professor Me Renato A. de A. Philippini

São Lourenço/MG

2022

340.0285
S729c Souza, Luciano Sebastião de

Cyber espaço e os desafios do anonimato: uma análise do sistema de camadas da web e seus reflexos na legislação brasileira / Luciano Sebastião de Souza. - - São Lourenço: Faculdade de São Lourenço, 2022.

26 f.

Orientador: Renato Augusto de Alcântara Philippini

Artigo científico (Graduação) – UNISEPE / Faculdade de São Lourenço / Bacharel em Direito.

1. Direito – processamento de dados. 2. Crime virtual. 3. Cyberespaço. I. Philippini, Renato Augusto de Alcântara, orient. II. Título.

Catalogação na fonte
Bibliotecária responsável: Fernanda Pereira de Castro - CRB-6/2175

CYBER ESPAÇO E OS DESAFIOS DO ANONIMATO
Uma análise do sistema de camadas da WEB e seus reflexos na legislação brasileira

Luciano Sebastião de Souza Silva[1]
Renato A. de A. Philippini [2]

RESUMO

O presente trabalho apresenta um estudo em relação ao sistema de camadas da web, cyber espaço, suas fragilidades e organização perante as leis brasileiras vigentes. O objetivo é analisar a sistemática técnica, entendê-la em seu contexto no dia a dia e vislumbrar as fragilidades e desafios das leis brasileiras, uma vez que a tecnologia não para de avançar. Para tanto, foi realizado um estudo abordando a pratica cotidiana, mecanismos que o Estado tem para combate indireto com usuários, que muitas vezes são desconhecidos/anônimos em um ambiente complexo, o trabalho da ênfase em uma busca morosa contra um sistema dinâmico, e se perfaz com base em pesquisa bibliográfica, documental e amparo legal vigente. Por meio deste estudo foi possível verificar que o referido sistema legislativo tenta se adequar as mudanças do ambiente virtual, porém diante da complexidade e expressiva dificuldade técnica não logra total êxito, reflexo este que se destaca com as últimas atualizações promovidas pelas Leis nº 12.737/2012 , 12.965/14, 14131/21 e 14.155/21 com vistas a combater os crimes cibernéticos e suas possíveis variantes em ambiente virtual, seja on-line e/ou off-line. Desse modo entende-se que a problemática na morosidade e falta de atualização da legislação pátria oportunamente abre precedente para eventuais crimes, estabelecendo um desequilíbrio entre particulares, seja mercadológicas e/ou até mesmo com o ente público, culminando em implicações sobre as garantias constitucionais inerentes e eventual responsabilidade dos indivíduos, fazendo-se valer da limitação e controle estatal.
Palavras-Chave: Cyberespaço. Dark Web. Deep Web. Crimes Virtuais. Dificuldades na investigação.

ABSTRACT

This paper presents a study in relation to the system of layers of the web, cyberspace, its fragilities and organization before the current Brazilian laws. The objective is to analyze the systematic technique, understand it in its everyday context and glimpse the weaknesses and challenges of Brazilian laws, since technology does not stop advancing. To this end, a study was carried out addressing everyday practice, mechanisms that the State has for indirectly combating users, who are often unknown/anonymous in a complex environment, the work of emphasis on a time-consuming search against a dynamic system, and whether makes up based on bibliographical and documentary research and current legal support. Through this study, it was possible to verify that the aforementioned legislative system tries to adapt to changes in the virtual environment, but in view of the complexity and significant technical difficulty, it does not achieve complete success, a reflection that stands out with the latest updates promoted by Laws nº 12.737/2012 , 12.965/14, 14131/21 and 14.155/21 with a view to combating cybercrime and its possible variants in a virtual environment, whether online and/or offline. In this way, it is understood that the problem of slowness and lack of updating

[1] Bacharelando em Direito pela Faculdade São Lourenço/UNISEPE. E-mail: lsss.advogado@gmail.com
[2] Mestre em Relações Internacionais e Ciência Política pela Universidade da Força Aérea. Docente e Coordenador do curso de Direito da Faculdade São Lourenço/UNISEPE. E-mail: rphi@uol.com.br

of the national legislation opportunely sets a precedent for possible crimes, establishing an imbalance between individuals, whether market and/or even with the public entity, culminating in implications on the inherent constitutional guarantees and eventual responsibility of individuals, making use of state limitation and control.

1 INTRODUÇÃO

Apesar da imensa informação disponível livremente na *World Wide Web*, conhecida pela sigla WWW ou, somente pelo termo *Web*, que pode ser traduzido como teia mundial, a maior quantidade de informações encontra-se em outras camadas de sua arquitetura.

A internet que milhões de pessoas utilizam diariamente em seus computadores, *tablets*, *smartphones* e outros dispositivos é denominada de *Visible Web* (*Web* Visível), *Surface Web* (*Web* da Superfície) e/ou, ainda, de *Normal Web* (*Web* Normal) (Bergman, 2001). Contudo, entre as camadas mais profundas da *WEB*, estão a *Deep Web* e a *Dark Web*, conceitos distintos, muitas vezes tidos como congêneres, cuja quantidade de dados que guardam dificilmente poderia ser mensurada, uma vez que se caracterizam por serem de acesso restrito.

Apesar de possuírem certas semelhanças, não são, por certo, a mesma *Web*. Em todo caso, a internet, em sua totalidade, tem sido pouco explorada diante de uma literatura nacional que retrata tanto a *Deep* quanto a *Dark Web* de forma escassa.

Nesse sentido, o objetivo do presente trabalho é descrever a arquitetura da *World Wide Web*, examinando suas diversas camadas, e avaliar a relação das leis brasileiras em vigor com essa arquitetura. Objetiva-se, ainda, apreciar as dificuldades de investigação no ambiente da internet.

Para tanto, adotou-se o método dedutivo, utilizando-se de pesquisa bibliográfica e documental.

2 DEEP WEB: ONDE SE ENCONTRAM 90% DOS DADOS NA WEB

A *Deep Web*, ainda muito pouco conhecida, estudada e investigada por trabalhos científicos, representa uma Web difusa e saturada por desconhecimento e estereótipos pejorativos em razão de seu conteúdo e carência de informação. O termo *Deep Web*, traduzido como “Rede Profunda”, foi referenciado em meados de 1994 pela Dra. Jill Ellsworth (Bergman, 2001) comumente conhecido e aceito como *Invisible Web* (*Web* Invisível) (SHERMAN; PRICE, 2001; FULTON; MCGUINNESS, 2016) e/ou *Hidden Web* (*Web* Escondida), conforme prefere Hurlburt (2017).

Todavia, e diante de muitas confusões conceituais, diversos autores como East (2017) popularizam que a *Deep* e *Dark Web* representam a mesma coisa no cyberespaço, ou seja, a mesma *Web*, trazendo equiparação dos dois termos para um mesmo objeto, fato contrário ao que se propõe no presente estudo. Conforme os estudiosos Fulton e McGuinness (2016), não se permite confusão entre a dificuldade de pesquisar assuntos, e/ou não encontrar certas páginas na *Deep Web* com a profundidade e obscuridade do anonimato da *Dark Web*. No mesmo sentido e de forma majoritária, também explicam os estudiosos Finklea (2017) e Zilman (2019).

A *Invisible Web* é significativamente uma parte expressiva do ciberespaço, em sua maioria traz, conteúdos/resultados não indexáveis ou não recuperáveis (não registrados) pelas plataformas e mecanismos de busca, tais como *Google* e *Bing*!. Diante da falta de indexação e não recuperação das informações, ocasionam uma quantidade expressiva de arquivos não transitáveis e, deste modo, não encontrados e acessados por todos no ciberespaço. Para Sherman e Price (2001) a *Deep Web*, identifica que as plataformas de busca em geral, não podem ou não conseguem tecnicamente registrar arquivos e páginas especificas em seus índices, por optações predefinidas e/ou, questões de comercialização e tarifamento que por sí só restringem o acesso, conforme explica Winkler e Gomes (2017). Mike Bergman (2001) esclarece que os sites de busca habituais como Google registram seus índices nas páginas da *surface*, o que reafirma a disposição dos motores em não indexar, demonstrando que essa indexação é deliberadamente superficial. Em analogia aos tradicionais aplicativos de GPS, que permitem, transitar em inúmeras rotas, sendo necessário apenas o endereço a se seguir, mas que, entretanto, não possibilitam mapear dentro de um endereço especifico residencial ou comercial sem o devido acesso.

Afirma Céndon (2001) que indispensáveis bancos de dados não fazem parte do objetivo de resultados apresentados pelas ferramentas de buscas tradicionais. Existem uma diversidade de opções e páginas com conteúdo específicos como materiais de referência, sejam eles, dicionários, catálogos e mostruários *on-line* de bibliotecas e acervos, informações protegidas e "seguras" por banco de dados de assinaturas comerciais (com base em taxas) e *firewalls* (sistema de segurança de rede que restringe o trafego da internet para rede privada) são exemplos encontrados na Deep Web (Rouse, 2019). Contudo, uma relevante e vital constatação da pesquisa e contribuição de Bergman (2001) é a de que 95% dos sites da Deep Web são gratuitos e livres, o que potencializa prejuízos a criadores e propagadores de

informações específicas de cunho comercial ou autoral, submetendo resultados a qualquer pessoa que busque por informações na Web.

Em busca de uma melhor compreensão territorial relacionadas as dimensões visíveis (facilmente acessíveis) vs invisíveis (tecnicamente não acessíveis) da Deep *Web* Bergman (2001) traz dados essenciais, mesmo, sendo considerados antigos, não foram encontrados dados e pesquisas mais recentes com a precisão de Bergman (2001), seja na literatura nacional ou internacional. O autor demonstra que na *Deep Web*: (a) a informação pública, diante de acesso livre e fácil é 400 a 550 vezes maior que a da normal *web ou web* de superfície; b) de forma técnica e dimensional, a *Visible Web* teria aproximadamente à época 19 terabytes, contra 7.500 da *Deep Web* (Rouse, 2019); (c) sendo que a normal *Web* teria 1 bilhão de documentos e, a *Deep Web*, 550 bilhões; (d) existem mais de 200.000 *sites*; (e) o conteúdo da *Deep Web* é de 1 a 2 mil vezes maior do que o da *web* comum.

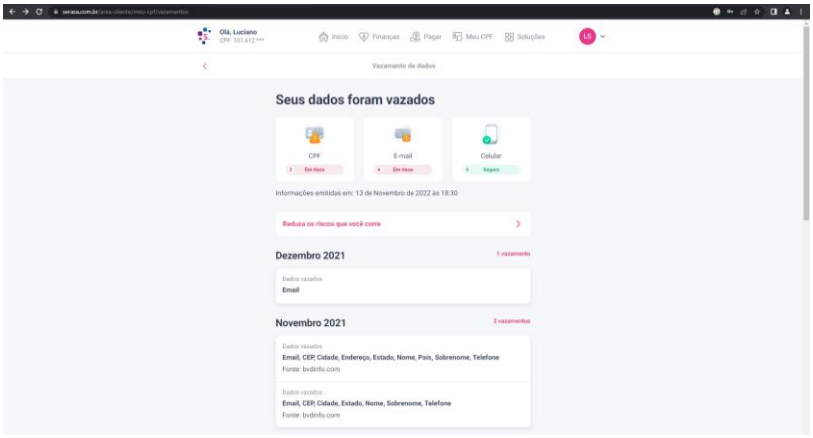
Igualmente, estudiosos como Atwood (2017), East (2017) e Rouse (2019) demonstram que a normal *Web* em sua totalidade disponível, só resulta em apenas 4% de todo o conteúdo da internet. Na tentativa de atualizar os dados expressivos de Bergman (2001), Rouse (2019) traz a seguinte fração da totalidade de conteúdo da internet em suas camadas: (a) *Deep Web* = 90% de todo o conteúdo do ciberespaço, seja ele aberto ou fechado comercialmente; (b) *Dark Web* = 6%; e (c) *Visible Web* = apenas 4%, ou seja, tudo que normalmente conhecemos da internet é meramente superficial e irrisório.

Conforme explica Zilman (2019), a totalidade da Deep *Web* é calculada por incríveis 7.500 *terabytes* de arquivos de conteúdo, assim como já visualizado por Bergman (2001). É necessário evidenciar que a multiplicidade se torna complexa, seja de arquivos ou informações na *Deep Web* tornando-a significativa e promissora. Diversos materiais inapropriados e ilegais no Brasil, tais como pornografia infantil, zoofilia, e demais patologias sexuais, comércio e fabricação de drogas, além de muitos outros tipos de venda ilegal, golpes e tratativas de fraudes em diversos assuntos, lavagem de dinheiro, e até mesmo rituais canibalísticos, são, inquestionavelmente, visualizados na *Deep* (e mais precisamente na *Dark Web* diante da possibilidade de anonimato quase que total) como produtos primários de mérito da *internet* e suas origens, e não como propriedade dessa ou de outra camada do *cyber* espaço. Não é recomendado a exposição de Dados Sensíveis (dados pessoais, tais como, nome completo, CPF, RG, data de nascimento entre outros) por questões de privacidade, ética, segurança e inúmeros outros motivos de responsabilidade legal, seja, para os proprietários/administradores das páginas e fóruns, como para o usuário final, que utiliza,

compra e replica o serviço ou produto. Nesse sentido, deve-se observar a enorme “confiança” de uns e “receio” de outros, ao aceitar os termos de uso de cada página, a depender é claro do nível de familiaridade com a *web*. Nessa perspectiva, por necessidade e carência, foi publicada a Lei Geral de Proteção de Dados Pessoais no Brasil em 2018, com o foco na prevenção e proteção legal aos Dados Pessoais e Sensíveis (BRASIL, 2018).

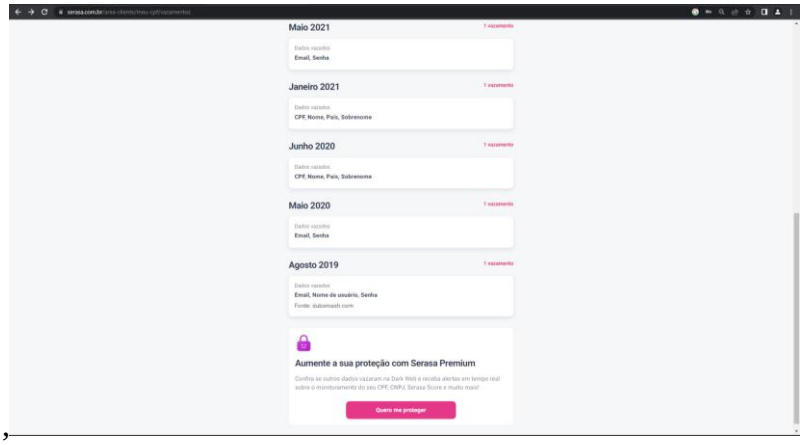
Já em toda União Europeia, as especificidades legais acerca da proteção dos Dados Pessoais e Sensíveis já ocorrem desde 1981 e, independentemente de internet e meios digitais, suprindo uma demanda comercial que posteriormente em 2016 foi atualizada e adaptada para internet e afins, através do Regulamento Geral de Proteção de Dados. No que se refere aos direitos à privacidade, hoje resguardados por leis e até mesmo regimentos nacionais e internacionais, ocorrem nas camadas da *Deep* e *Dark Web*, inúmeros crimes que refletem muito negativamente na manutenção dos direitos dos usuários. Ao passo que inúmeras discussões e instrumentos legais são desenvolvidos e atualizados para uma melhora na proteção dos Dados Pessoais e Sensíveis de forma geral, sejam nas camadas de superfície como nas camadas mais obscuras da internet ainda há uma grande dificuldade na garantia desses direitos, tanto a usuários comuns de relação pessoal ou até mesmo na complexidade de pessoas jurídicas. Inúmeras informações, dados e arquivos de registros públicos de pessoas físicas ou jurídicas (Rouse, 2019) estão entre os mais variados exemplos de dados sensíveis e sigilosos recuperados na *Deep* ou na *Dark Web*, ilustrando o enorme e difícil desafio, até mesmo por que uma vez “compartilhados” indevidamente e associados a interesses escusos, existe uma fragilidade e impossibilidade de alteração e ou manutenção dos dados, vistos de sua própria publicidade e especificidade. É muito comum algumas ferramentas na surface identificarem algum conteúdo pessoal/dados sensíveis expostos, como exemplo, Serasa Experian, onde é possível identificar conteúdos sensíveis que foram vasados, tais como CPF, telefone, nome completo e até mesmo e-mail, tudo coletado na Normal Web, sejam por sites comerciais de pouca ou nenhuma segurança, e até mesmo em sítios governamentais, todos resultados, estão atrelados a um sistema pago de monitoramento e pesquisa aprofundada. Os dados vazados compõe um banco de dados de extremo interesse a pessoas mal intencionadas, sejam para aplicação de golpes, empréstimos, financiamentos entre outros, conforme demonstram as Figuras 1, 2 e 3.

Figura 1. Site exemplificativo em ambiente logado e mediante cadastro Serasa Experian: *Visible Web*.



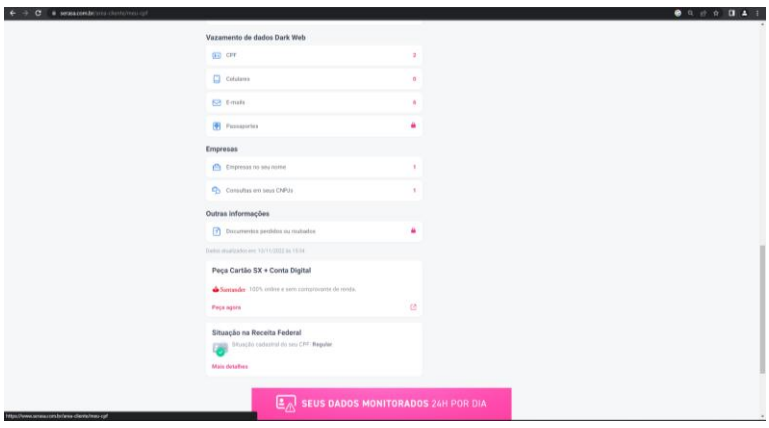
Fonte: www.serasa.com.br (2022).

Figura 2. Site exemplificativo em ambiente logado e mediante cadastro Serasa Experian: *Visible Web*.



Fonte: www.serasa.com.br (2022).

Figura 3. Site exemplificativo em ambiente logado e mediante cadastro Serasa Experian: *Visible Web*.



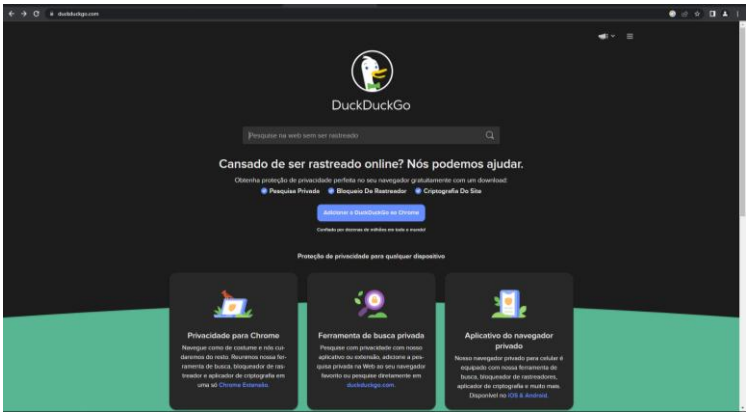
Fonte: www.serasa.com.br (2022).

Tais ferramentas são reflexo de ações e combate diante dos milhares de sítios (*sites*) existentes no *cyber* espaço, destinados especificamente a denúncias e à violação de direitos de privacidade e identidade o que muitas vezes é feito de forma proposital pelo usuário. É possível observar, que a invisibilidade/anonimato na *internet*, somado precisamente de seus conteúdos, dados ou informações, é, sob diversos ângulos, precisamente necessária e privada.

Em sua totalidade a *Deep Web* já demonstra com clareza ser uma camada exponencial de informações acessadas e dados não indexados, coexistindo diante de uma pluralidade de materiais aquém da criminalidade e com qualidade substancial (VIGNOLI, 2014; VIGNOLI; MONTEIRO, 2015A, 2015B; NIEMEIER, 2016; ZILMAN, 2019).

Ocorre, entretanto, que os dados da camada escura permanecem camuflados, mas, uma vez identificados, indexados ou acessados, a invisibilidade é dissipada e conhecida. Ou seja, para "navegar" em conteúdos da *Deep Web*, o usuário necessariamente precisa conhecer e encontrar a URL correta e especifica, cadastrando-se a partir daí ou realizando pagamentos para liberação de acesso, em muitos casos ainda, utilizar de ferramentas especificas dos mecanismos de busca para o ambiente profundo. O *Duck Duck Go* é um mecanismo de busca que retorna resultados, tais como o Google e o *Yahoo Search*, entretanto, no ambiente da *Deep Web* e seus resultados sejam da superfície ou não, são protegidos por uma navegação anônima, vislumbrando especificamente a privacidade do indivíduo que busca informações, conforme ilustra a Figura 4 (DUCK DUCK GO, 2019).

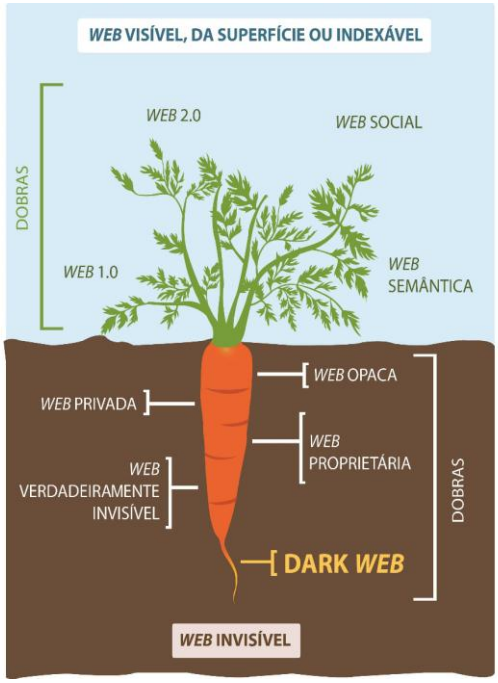
Figura 4. Site exemplificativo *Duck Duck Go: Visible Web*.



Fonte: www.duckduckgo.com (2022).

Diante da não recuperação dos mecanismos de busca tradicionais como *Google* ou *Bing*, a *Deep Web* metaforicamente estaria localizada abaixo da Superfície da *Web* (Figura 5) o que acolheria diversas outras camadas do *cyber* espaço, ainda mais obscuras e profundas, como a *Dark Web*.

Figura 5. Dobras/camadas do ciberespaço: *Visible Web* vs *Invisible Web*.



Fonte: Vignoli (2014).

3 DARK WEB: A REDE PARALELA ANÔNIMA

A internet em geral possui muitos predicados e a *Dark Web* em comparação se torna exponencial, também conhecida como *Web* Escura, se deu início com uma tese de doutorado conhecida como *Distributed Decentralised Information Storage and Retrieval System*, do Dr. Ian Clarke, na Edinburgh University em meados 1995 (BECKETT, 2009). Criada em meados dos anos 2000, surgiu na forma de software, onde foi possível sua replicação e *download*, pioneiramente desenvolvido por Clarke, nomeado de *Freenet* (Freenet, 2019), um sistema grátis de *proxy* com intuito de propiciar o acesso diferenciado à *internet*, sejam eles *sites*, *webchats* e também ao compartilhamento rápido de informações e dados de forma anônima na internet. O poderoso software trabalhava como um mediador entre rede mundial e os computadores, ou seja, de forma mais técnica, entre servidores e usuários. O sistema de *proxy*

viabiliza uma conexão entre usuários locais com sistemas de redes externas que de fato "[...] impede que usuários externos acessem recursos existentes na rede interna ou saibam onde estão localizados." (SAWAYA, 1999, p. 375). Diante da pesquisa cientifica de Clarke, vislumbrou-se a possibilidade da criação de uma paralela rede na internet, para compartilhar e acessar dados, em toda *Web*, ou parte dela, formalizando assim a *Dark Web* na pratica.

Muitos estudiosos como McGuinness (2016) e Hurlburt (2017) vislumbraram inúmeras nomenclaturas para a *Dark Web*, tais como: *Invisible Web* (*Web* invisível); *Dark address space* (Espaço de endereço escuro); *Deep Web* (*Web* Profunda); *Darknet* (*Net* escura); e *Dirty address space* (Espaço de endereço sujo); *Murky address space* (Espaço de endereço sombrio).

Diante de cada nomenclatura encontrada é possível que elas possuam definições próprias conforme cada autor, entre elas as mais comuns são a *Invisible Web* e a *Deep Web* (sinônimos com base na invisibilidade geral da *web*) e a *Darknet*, correspondente a um sinônimo de *Dark Web* e de redes de acesso restrito às camadas profundas.

Conforme explicam Fidencio e Monteiro (2013, p. 692)

> "[...] Dark Web é aquela parte da web que se destina a ser anônima". Por conseguinte, os autores indicam que [...]" "É bastante seguro considerar a *Dark Web* como uma nova ramificação da *Web* Invisível: suas características são próprias; sua filosofia é própria e, além de tudo, seu conteúdo é o mais enigmático e desordenado de todas as ramificações".

Para Lund (2019), a *Web* profunda simboliza um coletivo de sítios da *internet* que só são acessadas com uso de *browser* (programa navegador) específicos (por intermédio de *proxy*). O autor elucida ainda que, seja a *Deep* ou *Dark Web* estão sob as camadas de superfície; todavia, apesar de serem camadas da *Deep Web*, a *Dark Web* é muito mais profunda, restrita e obscura, confirmada pelo anonimato, muitas vezes associado à criminalidade.

Ademais, Hurlburt (2017) esclarece que o mercado obscuro é enorme o suficiente e tem mecanismos de pesquisa próprios, sejam sistemas de classificação e até mesmo fóruns de comunidade, além das bitcoins, sua própria moeda. Aderidos em inúmeras transações comerciais legais no mundo todo, especificamente por ser uma moeda facilitadora para transações ilegais, exclusivamente na *Dark Web*. Por ser uma moeda digital criptografada que dispensa rastreio, burocracia e inúmeras formalidades habituais, entre elas vínculo com contas bancárias ou métodos de pagamento por cartão de credito, facilmente rastreados (BITCOIN, 2020), é um método bem aceito principalmente para compra de serviços e produtos ilegais,

sejam na *Deep* ou *Dark Web*. Este trabalho de pesquisa, defende a hipótese de que o acesso à *Web* profunda mais precisamente a Dark Web, só é possível por meio de programa especifico *proxy*, do contrário, não se falaria da mesma camada da *Web*. O *proxy* acaba por camuflar o *Internet Protocol* (IP) endereço dos diversos dispositivos e permitem acesso a camada.

No ideal de uma compreensão mais clara, Hurlburt (2017) afirma que a *Dark Web* está embutida na *Deep Web*, entretanto só é possível acesso por meio e ajuda de softwares, confirmando uma espécie de hierarquia entre as camadas, conforme bem representado acima, na Figura 5. À vista disso, a *Dark Web* compõe o escopo da *Deep Web* ao mesmo tempo que é a própria *Deep* profunda. Não obstante, diante de sua relevante complexidade e profundeza, seu acesso é realizado diante de conceitos e características diferenciadas, colocando a *Dark Web*, indiscutivelmente, aquém da *Deep Web* em termos técnicos.

O chamariz para a utilização é a falta sistêmica de rastreamento, viabilizando e incentivando a realização de inúmeros delitos, proporcionando também em contra partida, uma navegação tranquila, sem espectadores ou algoritmos de inteligência artificial (AI) em busca do melhor cliente e comercio para a compra e venda de seus produtos, com a tranquilidade ainda de altíssima privacidade. Ou seja, inviabiliza e desencoraja, tanto a espionagem como a invasão de privacidade, muitíssimo recorrente na *Web de* superfície, tal como o reconhecimento por parte do governo e diversas empresas, sobre quem acessa seus sites, esclarece Heaven (2018). Winkler e Gomes (2017) dão destaque para a camuflagem de IP em redes como o *The Onion Router* (TOR), por exemplo, não é ideal, mas aceitável e cumpre a intenção que é ficar invisível na internet.

Portanto, para navegar na *Dark Web*, são indispensáveis programas especializados (softwares) em Redes Anônimas, como, *Anonymity Tools* (AT). As AT mais tradicionais na navegação à *Dark Web* são sem sombra de dúvidas, o *Freenet* e o *Tor*. Existem outras inúmeras opções de AT, até mesmo para dispositivos móveis, com *download* facilitado e de forma muito simples, gratuita e lícita.

Navegar livremente na *internet* e em sua *Web* obscura na forma de dispositivos móveis, como telefone e tablets é uma tendência em crescimento, até mesmo pelo fato de muitas vezes ser desregulamentado percorrendo caminhos onde a lei não prevê ou tipifica diretamente, seja pela falta de conhecimentos, mecanismos possíveis de rastreio e reconhecimento pessoal para responsabilização ou pela dificuldade de identificação.

Como absolutamente nada na *Dark Web* é registrado por meio de indexação (propositalmente), qualquer tipo de formato de arquivos é aceito no compartilhamento dos

conteúdos, gerando inúmeras possibilidades, até mesmo para leitura de mídias e formatos muito específicos dos arquivos. *Hacker, crakers* e muitos outros especialistas da alta tecnologia usam e manipulam formatos de mídias exclusivamente para a camada que utilizam, criando inúmeros outros filtros e até mesmo ostentando novos potenciais produtos.

Conforme explica Monteiro e Fidencio (2013), em sua totalidade a *Dark Web* permanece na invisibilidade, na maioria das vezes, porque se tratar de arquivos e dados judicialmente ilegais. Apesar disso, os crimes não representam o espaço em sua totalidade. Hurlburt (2017) mostra que a *Dark Web* é considerável e que sua maior parcela é um tanto bem-intencionada, contudo, seu destaque é relativo a um espaço onde serviços e bens ilegais são comercializados por e a qualquer usuário disposto a assumir o risco e pagar o preço.

Na literatura vemos outros exemplos como os de Chen (2012) com ideal minoritário e reducionista para a *Dark Web*, defendendo que a *Web* escura se baseia no terrorismo, em vendas e na distribuição de *softwares* piratas, roubo de identidade, ou como mero meio de compartilhamento e base para extremistas que propagam a intolerância e o ódio. Contudo, acredita-se que são sensacionalistas as informações de Chen (2012), haja vista, que todos os crimes descritos pelo autor são somados e presentes na *Visible Web/ Normal Web*. Todavia, não se deve ignorar a in rastreabilidade dos usuários e de seus dispositivos como meio facilitador a pessoas inclinadas a cometer crimes. Vignoli e Monteiro (2015) corroboram e demonstram o que pode ser encontrado na *Dark Web*: em síntese, crimes relacionados a assuntos bancários, tráfico e manipulação de armas de fogo, de drogas e de animais; contrabandos de todos os gêneros; possibilidade para falsificações, tais como, passaporte, identidades, e até mesmo de dinheiro, venda de pesquisa cientifica e diplomas; contratação de assassinos de aluguel; produção de vídeos e contatos para pedofilia e necrofilia (nacional), dentre outras situações ilícitas.

Todavia, é inquestionável a probabilidade de uma navegação livre para outros fins, que não ilegais, como pesquisadores com dados inéditos, jornalistas com suas reportagens secretas, para a discussão em grupos privados diversos e que buscam não ser observados, *etc*.

A camada da *Web* profunda pode e é muito utilizada para burlar a censura e acesso a conteúdos bloqueados, principalmente em países onde imperam a ditadura, no respaldo de sempre manter a privacidade sejam nas comunicações ou mesmo ideias de negócios confidenciais. Acredita-se que a camada da *Dark Web* simboliza uma internet verdadeiramente livre do politicamente correto, e que, apesar do uso indevido, reflete em mais liberdade de navegação, de comunicação e expressão.

A ideologia da *Dark Web* é a liberdade, tendo como norte a certeza de maior liberdade de expressão mediante o técnico anonimato, ilustrando bem o sentimento do usuário, seja em pensamento ou suas atitudes, lidando de forma vítrea com a ética e a moral, seja para o bem ou mal.

4 PANORAMA DA LEGISLAÇÃO BRASILEIRA REFERENTES AOS DELITOS PRATICADOS NO MEIO VIRTUAL

Os crimes praticados no *cyber* espaço são caracterizados como crimes virtuais, crimes digitais, de alta tecnologia, telemáticos, informáticos, delitos por computador, estelionato digital/virtual, crimes cibernéticos, fraude informática ou computacional, delitos transnacionais/computacionais dentre diversos outros exemplos. Existe uma divisão clara entre os chamados crimes próprios (ou puros) aqueles praticados em sentido amplo por meio da informática, onde a computação é o norte jurídico tutelado, assim também como os delitos impróprios (ou impuros) ou seja, o usuário se vale do celular ou computador como artefato para produção resultado específico e naturalístico, ou seja, que de certa forma lese o mundo tangível e espaço real, ofendendo ou ameaçando diversos outros bens além da computação.

Conforme aponta Rossiini (2004) a ideia de "delito informático" conseguiria ser assegurado como uma conduta ilícita e típica, formalizando um delito ou contravenção, culposa ou dolosa, omissiva ou comissiva, produzida pelo usuário, seja ela jurídica ou física, reproduzida a partir da informática e/ou telecomunicações, seja *offline* ou *online*, dentro de uma rede especifica, e que reflita, de forma direta ou indireta, a seguridade digital, que por si só, permeia por referenciais ligados a disponibilidade, confidencialidade e a integridade.

Portanto, o delito por meios tecnológicos abarca todo ideal de conduta delitiva, uma vez que é tipificada e inserida, fazendo-se valer de seus meios, incluindo ou através da web. Explica Nigre (2000, p. 32) que o delito informático: "[...] é um ato lesivo cometido através de um computador ou de um periférico com a intenção de se obter uma vantagem indevida". Posto isto, o entendimento de delito cibernético não incorpora somente os crimes de alteração de dados pessoais e/ou *software*, mais também de roubo e outros crimes como, zoofilia, pedofilia, tortura, tráfico e fabricação de drogas, tráfico de pessoas e órgãos em sentido amplo, pirataria, e até mesmo os mais comuns e corriqueiros nas redes sociais como, calúnia, difamação e a injúria. Dentre estes, destaca-se a insalubre pornografia infantil.

Antes de mais nada, é necessário pontuar que o crime de pornografia infantil não se pode confundir com a Pedofilia, conforme a Organização Mundial da Saúde (OMS) a Pedofilia é uma patologia psiquiátrica, reconhecida como transtorno e perturbação psicológica, em que o indivíduo apresenta anseio sexual por crianças na fase da pré-púberdade. Assim sendo a pessoa na natureza pedófila não é identificada como um criminoso, e sim um paciente, entretanto, no momento em que exterioriza sua doença e está se combina em algum crime com previsão no ordenamento jurídico, o pedófilo torna-se um criminoso infrator. Conforme nossa legislação vigente, a pornografia infantil, se consuma mesmo sem a necessidade eventual de ato sexual, sendo mais que suficiente o consumo pessoal ou comercial e/ou o compartilhamento de fotografias, vídeos pornográficos contendo crianças e adolescentes, o que acaba firmando critérios claros para a tipificação, respaldado na conformidade e como determina o Estatuto da Criança e do Adolescente (BRASIL, 1990).

A difusão de qualquer material na camada profunda da web dificulta extremamente o reconhecimento e rastreio de origem de quem as divulga e replica. Esta realidade criminosa é uma das mais veiculadas e frequentes na Deep Web, camada esta que com mecanismos próprios, torna-se quase impossível a identificação do transgressor, bem como a repercussão viral oferecida pela web e redes sociais, ou mesmo a simples divulgação anônima destes arquivos, incentivando ainda mais tal pratica.

Comumente hoje, com o acesso facilitado, crianças e principalmente adolescentes estão conectados e utilizam algum meio virtual, navegando em diversas redes sociais, jogos *online*, *chats* e *blogs* sem o monitoramento responsável, o que incentiva ainda mais a ocorrência de diversos crimes, tornando-os alvos fáceis e manipuláveis, vítimas reais para estes criminosos.

Outrossim, é a importância da vigilância dos pais, ou da família, seja para o comportamento do menor como também mantendo o diálogo e analise frequente do conteúdo visitado, uma vez uma foto ou vídeo de nudez gravados, tais arquivos podem ser facilmente violados e reutilizados por criminosos, sejam por meio de invasão de dispositivos, e/ou espalhados na web por livre vontade (através de manipulação e promessas) e repassados posteriormente sem quaisquer controles.

Examinando a legislação brasileira, é nítida a carência e defasagem de leis que tipifiquem as condutas criminosas ocorridas no *cyber* espaço; nessa direção Crespo (2011) indica que a confiabilidade dos dados, e a segurança na web, e/ou de comunicação tecnológica, demandam regulamentação do Direito Penal. É claro que ao perceber toda

evolução da informática, em especial os meios de comunicação, reparamos que a legislação penal é insuficiente e em certos momentos não está em conformidade e detrimento da demanda, muito menos diante da relação e tutela jurídica a respeito dos mais elaborados crimes informáticos.

No ambiente *online,* virtual, as pessoas buscam privacidade, segurança e confiabilidade, uma vez que possam expor dados sensíveis, sejam para comercialização ou até mesmo para entretenimento, desfrutando com comodidade e facilidade que a internet e seus benefícios oferecem. Conforme explica Abreu (2011, p.12) as condutas criminosas por sua vez, como o estelionato, roubo e uso criminoso/indevido de dados, entre outros crimes cometidos via web, que com cada vez mais frequência, veem trazendo insegurança e sensação de que as leis e autoridades se encontram impotentes, não acompanhando o progresso tecnológico, ficando inclusive aquém da legalidade, uma vez que é sabido o *modus operandi* utilizado para o combate e controle.

Diante da analise legal disponível, e referenciamento cronológico observa-se uma morosidade enorme e atuante que está sob muita demanda, na pratica visualiza-se também algumas possibilidades "adaptativas" e suas aplicações em ambiente virtual, entre elas, quando o crime se associa a contratos, mesmo virtuais, utiliza-se o Código Civil brasileiro e/ou o Código de Defesa do Consumidor, evidenciando a falta de normas específicas, que muitas vezes são necessárias e extremamente complexas a medida do caso concreto, sejam pela identificação como formalização comercial em suas variações. Já na esfera Penal, também há muita carência, apesar de já existirem normas tipificadas, por exemplo, nos artigos 240 e 241 do Estatuto da Criança e do Adolescente; artigo 12 da Lei nº 9.609/98 que versa sobre crimes contra software/programação; artigos como 138, 139, 140 e 147 do Código Penal, que tipificam respectivamente os crimes de calúnia, difamação, injúria e ameaça, que ocorrem com muita frequência e combatidos de forma adaptativa em alguns casos no ambiente virtual, em sua maioria nas redes sociais.

Inicialmente e sob o prisma do Código Penal brasileiro, originalmente não haviam leis que tratassem de crimes virtuais e afins, até mesmo por conta da época (1940). Observa-se somente e de forma mais especifica em 30 de novembro de 2012, com a publicação da Lei Nº 12.735, que o Código Penal foi atualizado, acrescentado os seguintes artigos 154-A, 154-B, 266 e 298 com foco em uma punição dos crimes cometidos na internet.

Em sequência e no mesmo ano, a tão e popularmente conhecida Lei Carolina Dieckmann, ou seja, Lei n.º 12.737/2012, formulada em consequência do "vazamento" e

publicidade de imagens em sites pornográficos, isto é, após hackers terem invadido o computador pessoal de uma conhecida figura pública, os mesmos, usando subterfúgios técnicos obtiveram acesso a arquivos de mídia, onde perceberam no acervo, fotos da atriz nua seguindo de uma tentativa infrutífera de tirar proveito financeiro por meio de chantagem, com tudo, os dados da atriz global (Rede Globo) foram parar na web uma vez da recusa da vítima à extorsão, não formalizando o pagamento de quantia em dinheiro para que suas fotografias em poses íntimas não fossem amplamente divulgadas.

Conforme explica Brito (2013), a atualização da lei sobre crimes cibernéticos representa um marco histórico para ordenamento jurídico brasileiro, pois por si só trouxe um avanço significativo no que concerne de uma tipificação focada e especifica para criminalidade digital.

A Lei n. 12.737/2012 explora a tipificação de crimes digitais, seja na intenção de atualizar a legislação penal vigente, como sanar vícios específicos, prevista no art. 154-A do Código Penal brasileiro, inserido pelo art. 2º da Lei 12.737, fica claro e expresso que a conduta delituosa de invadir dispositivo informático/tecnológico de outrem, estando ou não conectado à rede mundial de computadores, violando indevidamente mecanismos de segurança para obter, adulterar, ou destruir dados ou arquivos sem previa autorização do proprietário do dispositivo, com vista na obtenção de vantagem ilícita.

Completa neste sentido Cabette (2013, p. 1):

> Não é qualquer dispositivo informático invadido que conta com a proteção legal. Para que haja o crime é necessário que o dispositivo conte com 'mecanismo de segurança' (v.g. antivírus, 'firewall', senhas etc.). Assim sendo, o dispositivo informático despido de mecanismo de segurança não pode ser objeto material das condutas incriminadas, já que o crime exige que haja 'violação indevida de mecanismo de segurança'. Dessa maneira, a invasão ou instalação de vulnerabilidades em sistemas desprotegidos é fato atípico. […] Sinceramente não se compreende essa desproteção legislativa exatamente aos mais desprotegidos. É como se o legislador considerasse não haver violação de domicílio se alguém invadisse uma casa que estive com as portas abertas e ali permanecesse sem a autorização do morador e mesmo contra a sua vontade expressa! Não parece justo nem racional presumir que quem não instala proteções em seu computador está permitindo tacitamente uma invasão, assim como deixar a porta ou o portão de casa abertos ou destrancados não significa de modo algum que se pretenda permitir a entrada de qualquer pessoa em sua moradia. A forma vinculada disposta no tipo penal ('mediante violação indevida de mecanismo de segurança') poderia muito bem não ter sido utilizada pelo legislador que somente deveria chamar a atenção para a invasão ou instalação desautorizadas e/ou sem justa causa. Isso seria feito simplesmente com a locução 'mediante violação indevida' sem necessidade de menção a mecanismos de segurança.

Todavia, mesmo com a confecção das Leis nº 12.735/12 e 12.737/2012 não mudaram muito a realidade cotidiana, visto o "combate efetivo" dos delitos que são cometidos através da internet, principalmente dado o avanço informático e telemático como também pela criativa gama de crimes virtuais e a falta de leis específicas. Ademais, a natureza taxativa do Código Penal inviabiliza, dificultando muitas vezes a tipificação de suas leis por analogia ou costumes aos crimes virtuais.

Posteriormente Vale mencionar, ainda, que em 2014, por intermédio da Lei nº 12.965/14, nasce o Marco Civil da Internet ("MCI") com a missão especifica e mais clara de reagir/combater aos crimes virtuais, dando maior suporte nas investigações destes delitos, buscando ainda, enfrentar teses que estavam em aberto na sociedade, que por consequências implicavam nos mais variados e diretos impactos sob os interesses pessoais e comerciais. O Marco da Internet, popularmente conhecido, busca a manutenção da segurança dos registros e dados sensíveis, trazendo uma maior proteção aos dados pessoais e interações privadas, procurando sempre garantir maior neutralidade na web, inclusive cobrando responsabilidade civil dos provedores em geral, não só diante da guarda de dados e registros, como na possibilidade de requisição judicial de dados, afim de garantir o bom e transparente cumprimento e responsabilização legal, seja pessoal ou comercial (BRASIL, 2014).

Conforme entendimento do o art. 3º do Marco Civil da Internet, fica claro três princípios estabelecidos a internet brasileira, compostos pelos fundamentos que se relacionam entre si, da neutralidade da web, da liberdade de expressão e sobre tudo da privacidade, A ideia de neutralidade da web se desenvolve sobre as garantias comerciais, evitando de que as operadoras não cobrem de forma diferente, a depender do assunto veiculado, exceção apenas quanto às velocidades de transmissão (planos de dados), propiciando a democratização e maior busca, trazendo a facilidade ao acesso à internet no Brasil (BRASIL, 2014).

No tocante ao ideal de privacidade pessoal, a lei tenta garantir maior proteção e atenção na manutenção aos dados sensíveis (dados pessoais) sejam em relação aos provedores de acesso, autorizando apenas em ocasiões excepcionais judicializadas a quebra do sigilo. Como já é sabido, a liberdade de expressão é garantida constitucionalmente, entretanto, recebe destaque no Marco na Internet, reforçando um princípio que condiciona o uso da internet no país e exercício pleno do direito de acesso.

Mais modernamente outras Leis foram promulgadas trazendo melhor manutenção, para os casos concretos e presentes no dia a dia, são elas, Lei 14132/21 e 14.155/21.

A Lei nº 14132/21 acrescentou o artigo 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), prevendo o crime de perseguição (também conhecido como *stalking*) aumentando expressivamente a proteção de vítimas de situações como insistentes comportamentos após por exemplo, o fim de relacionamentos, Perquirindo a obsessão ou perturbação continuada pela internet.

Somente no Estado do Paraná, desde a criação da lei, em abril de 2021, há um ano, foram registradas 4.570 ocorrências destes crimes.

A titular adjunta da Delegacia da Mulher de Curitiba, Emanuele Maria de Oliveira Siqueira, reitera que o stalking se caracteriza diante de atitudes contumazes do perseguidor infrator no cerceamento a privacidade e liberdade da vítima, tais como "[...]"frequentar locais nos mesmos horários da vítima para impor sua presença, rondar a casa, fazer ligações telefônicas insistentes que imponham medo é crime. Mas há pessoas que não sabem que essas atitudes configuram crime" (AGÊNCIA DE NOTÌCAS DO PARANÁ, 2022).

E, por fim, a Lei nº 14.155/21 alterando o crime de invasão de dispositivo informático, melhorando inclusive sua redação e aumentando substancialmente suas penas (art. 154-A do CP). Além disso, finalmente, foram criados os crimes específicos de furto mediante fraude eletrônica (art. 155, § 4º-B do CP) e de fraude eletrônica (art. 171, § 2º-A do CP). A mesma lei ainda definiu o local competente para julgar os crimes de estelionato cometidos por meio de cheque sem fundos, com pagamento frustrado, ou por transferência de valores que passou a ser, nesses casos, o local da residência da vítima (art. 70, § 4º, CP).

5 DIFICULDADES DA INVESTIGAÇÃO DE DELITOS NA *DEEP WEB* E NA *DARK WEB*

A complexidade envolvida de uma investigação de crimes virtuais não são tarefas fáceis, sejam pela possibilidade desses crimes ocorrerem em qualquer lugar, bastando apenas que criminoso tenha acesso à rede. Nesse nítido cenário, a internet é uma grande incentivadora e facilitadora para prática desses crimes virtuais, seja em razão da dificuldade de se encontrar o responsável como pela capacidade técnica em mascarar e/ou ocultar a fonte propagadora destes dados. Muito além disso, é necessária uma alta demanda de profissionais capacitados, que tenham conhecimento técnico informático somados ao conhecimento legal, e que em algum momento estacaram diante das normas obsoletas das leis vigentes.

De todo modo a persecução penal pode ser dividida em fases, a Investigação Criminal e Processo Penal. A primeira etapa se limita à colheita de provas, apuração de indícios de autoria e materialidade da ação criminosa, enquanto que a segunda fase tem por escopo a função de processar e julgar.

As noções de crime, delito, ato e efeito são os mesmos empregados no âmbito do direito penal e direito penal digital, cibernético, eletrônico ou informático, suas distinções se referem à territorialidade e à análise de provas, bem como a formação de novos tipos penais em reação ao surgimento de crimes cometidos exclusivamente através dos meios tecnológicos.

Conforme explica Wendt (2013) durante o processo inicial de investigação de crimes cibernéticos, existe a fase técnica, e fase consequencial. A finalidade da fase técnica é localizar o dispositivo utilizado para a conduta criminosa. Nesta etapa, analisa-se as informações narradas pela vítima e um perfil para compreensão do fato ocorrido na web, são feitas orientações à vítima afim da preservação do material comprobatório do crime e a sua proteção pessoal e virtual, coleta de provas em ambiente virtual, conferindo maior formalização da conduta por meio do registro do boletim de ocorrência, e por consequência instauração do procedimento, investigação inicial de dados na rede mundial de computadores, sobre possíveis autores, mais comum quando e com origem por e-mails, registros e hospedagens de domínios. Formalização das provas coletadas e apuração preliminar, representação ao Poder Judiciário para expedição de autorização judicial para quebra de sigilo dos dados, conexão ou acesso.

Tal como afirma Wendt (2013, p. 53):

> A partir da identificação e localização do computador que permitiu a conexão e o acesso criminoso na internet surge a denominada fase de campo, quando há necessidade de deslocamento de agentes policiais para realização de diligências com o intuito de promover o reconhecimento operacional no local. Essa diligência deverá ocorrer sempre de maneira discreta, pois poderá haver a necessidade de solicitar uma medida processual penal cautelar, em regra a representação para que o Poder Judiciário conceda o mandado de busca e apreensão. Ela ocorrerá de imediato nos casos de identificar o endereço que corresponda a uma residência e/ou rede não corporativa.

O Brasil conta ainda com outros meios para combate de crimes virtuais, implementados por divisões especializadas nos crimes cibernéticos, sendo responsabilidade da Polícia Federal ou Civil, regulamentada por uma política de segurança pública e

estruturada a partir do caso concreto, usando métodos locais ou diante da matéria regulamentada a qual as autoridades policiais estão vinculadas.

A facilidade do uso da internet além de oferecer enormes comodidades, também facilitou a pratica de crimes, e é nítida a dificuldade que as autoridades possuem para identificar e combater estes delitos. Com toda complexidade e evolução das condutas criminais no ciberespaço, houve também a necessidade de aperfeiçoamento, pessoal e técnico para com as entidades policiais, creditando maior estrutura e inteligência policial, com possibilidade até de infiltração de agentes no ambiente virtual, consequentemente, tonando-se essencial para o combate ao cibercrime.

De modo combativo, a infiltração de agentes policiais no mundo cibernético, é lícita, seja para investigação nos crimes de organização criminosa, tráfico de drogas, pornografia infantil, pedofilia e/ou *cyber* terrorismo. A Lei 13.441/17, regulamenta a infiltração de agentes de polícia na internet com a finalidade de investigar crimes contra a dignidade sexual de criança e de adolescente. Seguindo os mesmos moldes que os criminosos a investigação possui técnicas que os mantém anônimos na rede, possibilitando que os policiais vislumbrem possíveis vulnerabilidades destes criminosos, seja de forma direta ou indireta, coletando provas dos delitos, utilizando também do anonimato oferecido pela Deep Web e Dark Web.

Desta forma, vários acordos internacionais foram ratificados pelo Brasil para cooperação e combate ao Cibercrime, o que favorece a comunicação e prevê maior estrutura entre os países, favorecendo também a assistência rápida e a comunicação destes no combate ao crime. Por conseguinte, Domingos (2017, p. 247) afirma que:

> Nos delitos cibernéticos de disseminação de pornografia infantil via web, é comum que no bojo dessas investigações em determinado país sejam identificados IP's e dados de conexão utilizados na prática criminosa de usuários de Internet pertencentes a outro país. Situação em que a polícia desse país e envia as informações para o país onde os IP's identificados são alocados para que as investigações sejam desenvolvidas com relação às imagens e vídeos disseminados a partir desse local, tanto por ser de atribuição do país investigar e processar os delitos cometidos a partir de seu próprio território, quanto por ser mais provável que o criminoso seja identificado no local de onde disseminou as imagens e vídeos. Nesses casos, em que há a troca pelas autoridades competentes de diferentes estados de informações relevantes às investigações que ocorre em geral por intermédio da INTERPOL, há a presunção de regularidade na obtenção e transmissão de tais informações conforme a legislação do país de origem. No entanto, afigura-se prudente que os investigadores submetam a prova ao Judiciário para validação e autorização de uso.

No país, a Policia Federal é referência no combate aos crimes cibernéticos, duas grandes operações com o intuito de combater a pornografia infantil obtiveram enorme

sucesso. Utilizando um esquema técnico de inteligência inédito de investigação, os policias conseguiram quebrar o anonimato oferecido pelos ambientes da internet obscura, onde até então não era possível identificar o IP, fazendo se valer do novo mecanismo, identificaram mais de 90 pessoas envolvidas que acessavam e/ou replicavam pornografia infantil. Estas significativas operações, demonstram que o serviço de investigação brasileiro tem avançado significativamente no ambiente virtual, apesar das falhas na legislação, e das vantagens oferecidas pela Deep Web e Dark Web aos criminosos.

CONSIDERAÇÕES FINAIS

O que se objetivou no presente trabalho, foi analisar a sistemática técnica das camadas da Web, entendê-la em seu contexto no cotidiano, vislumbrando suas fragilidades e analisando tal arquitetura tecnológica à luz das leis brasileiras.

Desse modo, constatou-se, portanto, que ao se esbarrar em uma rede complexa, subdivida, coberta de procedimentos técnicos que demandam conhecimento prévio, diante de peculiaridades inerentes ao próprio espaço, que se amalgama e modificam diante da criatividade e tecnicidade humana em reflexo da Ciência da Computação em si, portanto, fica nítido a oportunista tentativa privada ao desafio, seja em sua grande parte anônima e/ou também infrutífera com identificação e dados falsos.

Assim, verificou-se que o Estado, conforme provocado, tenta criar mecanismos, leis próprias, a fim de restringir, ou seja, com o objetivo de tentar controlar, identificar e punir eventuais crimes.

Neste contexto, foi possível a constatação de que as leis implementadas aos códigos brasileiros, em alguns pontos vieram de encontro a garantias inerentes aos indivíduos, fazendo com que fossem em parte investigados, em parte sanados, entretanto, insatisfatória em sua maioria. Desse modo, na tentativa de sanar algumas dessas tratativas, foram concebidas diversas leis em detrimento da posição de fragilidade que se encontra o particular.

Assim, portanto, resta o entendimento de que se busca mecanismos eficazes, vigilância capacitada, seja por meio de tecnologias físicas e/ou pessoal capacitado e habilitado, haja vista a limitação que estes últimos enfrentam ao pleitear o direito líquido, certo, de todo modo, árduo e de extrema pericia, seja em sua compreensão, como também diante da volatilidade do ciberespaço.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Leandro Farias dos. **A Segurança das Informações nas Redes Sociais**. 2011 disponível em http://www.fatecsp.br/dti/tcc/tcc0023.pdf. Acesso em 15 . 2022.

AGÊNCIA ESTADUAL DE NOTICIAS, GOVERNO PARANÁ. **Lei contra stalking completa um ano e reforça proteção da privacidade**. 04 de abril de 2012 – Disponível em: https://www.aen.pr.gov.br/Noticia/Lei-contra-stalking-completa-um-ano-e-reforca-protecao-da-privacidade#:~:text=%E2%80%9CFrequentar%20locais%20nos%20mesmos%20hor%C3%A1rios,persegui%C3%A7%C3%A3o%20e%20acrescenta%20o%20Art. Acesso em 29 out. 2022.

ATWOOD, M. **O dialeto sombrio: todos os aspectos da tecnologia humana têm um lado sombrio, incluindo o arco e a flecha**. Espectro IEEE, New York, 22 outubro de 2017. Disponível em: https:// s2.smu.edu/~fmoore/misc/IEEE-Spectrum-The-Dark-Dialect- Oct-2017.pdf. Acesso em 22 out. 2022.

BECKSTROM, M.; Lund, B. Casting L: **Um guia para exploração segura na Dark Web**. New York: Rowman & Littlefield Publishers, 2019. Disponível em: https://periodicos.saude.sp.gov.br/bis/article/view/36720. Acesso em 10 nov. 2022.

BERGMAN, M. K. White paper: : **O valor oculto da superfície da deep web. Jornal de Publicação Eletrônica**, v. 7, n. 1, 2001. Disponível em: https://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main.

BRASIL. **Lei n° 13.709, de 15 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei n° 12.965 de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em 05 nov. 2022.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012** (Lei Carolina Dieckman). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011 2014/2012/lei/l12737.htm. Acesso em 22 nov. 2022.

BRASIL. **Lei nº 13.441, de 08 de maio de 2017.** Disponivel em: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=13441&ano=2017&ato=c44oXRU5EeZpWT5f7. Acesso em 25 out. 2022.

BRASIL. **Lei nº 13.441, de 08 de maio de 2017**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13441.htm. Acesso em 28 out. 2022.

BRITO, Gleice Kelly Silva. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web**. Goiânia, 2019. Disponível em: http://repositorio.anhanguera.edu.br:8080/jspui/bitstream/123456789/227/1/TCC%20CAP.%201%2c%202%20E%203%20GLEICE.pdf Acesso em 05 nov. 2022.

CABETTE, E. L. S, NAHUR, M. T. M. **Criminalidade Organizada & Globalização Desorganizada**. Rio de Janeiro: Freitas Bastos. Disponível em: https://ambitojuridico.com.br/site/?. Acesso em 14 nov. 2022.

CÉNDON, B. V. **Ferramentas de busca na web. Ciência da Informação**, v. 30, n. 1, p. 39-49, 2001. Disponível em: http:// www.scielo.br/pdf/ci/v30n1/a06v30n1. Acesso em: 23 abr. 2020. Acesso em 28 out. 2022.

CHEN, H. **Dark web: explorando e minerando dados no lado obscuro da web**. New York: Springer, 2012. Disponível em: https://www.scielo.br/j/tinf/a/8QrnXfB7VXrG4G6ywmhZngK/?lang=pt. Acesso em 23 out. 2022.

CRESPO, M. X. de F. **Crimes Digitais**. São Paulo: Saraiva, 2011. Disponivel em https://pt.scribd.com/document/388242827/Crimes-Digitais. Acesso em 23 nov. 2022.

DARK WEB (darknet): **WhatIs.com. Newton: What Is**, 2019. Disponível em: https://whatis.techtarget.com/definition/dark-web. Acesso em 11 nov. 2022.

DOMINGOS, F. T. S. **A obtenção das provas digitais na investigação dos delitos de violência e exploração sexual infantil online**. In SILVA, Ângelo Roberto Ilha da (Org.). Crimes Cibernéticos. Porto Alegre: Livraria do Advogado. 2017.

DUCK DUCK GO. **A ferramenta de busca que não rastreia você**. [S.l.], c2019. Disponível em: https://duckduckgo.com. Acesso em 19 nov. 2022.

EAST, C. S. **Desmistificando a Dark Web. Isso agora**, v. 59, n. 1, p. 16-17, 2017. Disponível em: https://doi.org/10.1093/itnow/bwx007. Acesso em 11 nov. 2022.

FIDENCIO, M. V.; Monteiro, S. D. **Web invisível: compreendendo a invisibilidade no ciberespaço. In: Seminário em Ciência da Informação**, 5., 2013, Londrina. Anais [...]. Londrina: Univer-sidade Estadual de Londrina, 2013. p. 683-700. Disponível em: http://www.uel.br/eventos/cinf/index.php/secin2013/ secin2013/paper/view/107. Acesso em 28 out. 2022.

FINKLEA, F. **Web escura. Washington: Congressional Research Service**, 2017. Disponível em:https://fas.org/sgp/crs/misc/ R44101.pdf. Acesso em 05 nov. 2022.

FREENET. **Browse websites, post on forums, and publish files within Freenet with strong privacy protections.** [S.l.], 2019. Disponivel em: https://freenetproject.org/author/freenet-project-inc. html/. Acesso em 03 nov. 2022.

FULTON, C.; McGuinness, C. In too deep. Em: Fulton, C.; McGuinness, C. (Org.). **Detetives digitais: resolvendo dilemas de informação em um mundo online**. New Deli: Elsevier, 2016, p. 95-118. Disponível em: https://www.scielo.br/j/tinf/a/8QrnXfB7VXrG4G6ywmhZngK/?lang=pt. Acesso em 14 nov. 2022.

GRECO, Rogério. **Código Penal: comentado-5. ed**. -Niterói, RJ: Impetus, 2011.

HEAVEN, D. **Desvendando as mitologias da dark web**. NewScientist, v. 240, n. 3209-3210, p. 82-83, 2018. Disponível em: https:// doi.org/10.1016/S0262-4079(18)32375-3. Acesso em 26 out. 2022.

HURLBURT, G. **Brilhando luz na dark web**. v. 50, n. 4, p. 100-105, 2017. Disponível em: https://ieeexplore.ieee.org/document/7912236 Acesso em 27 out. 2022.

MAIA, Teymisso Sebastian Fernandes**. Análise dos Mecanismos de Combate aos Crimes Cibernéticos no Sistema Penal Brasileiro** / Teymisso Sebastian Fernandes Maia. – 2017. Disponível em: https://repositorio.ufc.br/handle/riufc/31996#:~:text=No%20presente%20trabalho%20busca%2Dse,de%20anonimato%20idealizado%20pelos%20criminosos. Acesso em 11 nov. 2022.

MATÉRIA PORTAL DA POLICIA FEDERAL. **Combate a disseminação de pornografia infantil pela Deep Web no Rio Grande do Sul**. 15 de outubro de 2014 – Disponível em: http://www.adpf.org.br/adpf/admin/painelcontrole/materia/materia_portal.wsp?tmp.edt.materia_codigo=7080&tit=PF-combate-a-disseminacao-de-pornografia-infantil-pela-Deep-Web#.Y3WdZnbMJhE. Acesso em 14 nov. 2022.

MONTEIRO, S. D.; Fidencio, M. V. **As dobras semióticas do ciberespaço: da web visível à invisível. TransInformação**, v. 1, n. 25, p. 35-46, 2013. Disponível em: https://doi.org/10.1590/S0103-3786 2013000100004. Acesso em 03 nov. 2022.

NIEMEIER, C. **Rolando na deep web não dark: dicas para acessar e pesquisar na web oculta**. all Spectrum, v. 20, n. 6, p. 22-25, 2016. Disponível em: http://epubs.aallnet.org/i/695274-aall-spectrum-july-august-2016-volume-20- number-6/23? Acesso em 01 nov. 2022.

NIGRI, D. F. **Crimes e segurança na internet**. In Verbis, Rio de Janeiro: Instituto dos Magistrados do Brasil, Ano 4, n. 20, p. 34-41, 2017.

PAIXÃO, Gleice Kelly Silva. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na Deep Web e Dark Web**. Goiânia- GO, 2019. Disponível em: http://repositorio.anhanguera.edu.br:8080/jspui/handle/123456789/227?mode=full Acesso em 23 out. 2022.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4 ed. Saraiva: São Paulo, 2010. Disponível em: https://egov.ufsc.br/portal/sites/default/files/o_direito_digital_e_as_implicacoes_civeis.pdf Acesso em 31 out. 2022.

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica, 2004. Disponível em: http://www.dhnet.org.br/dados/cursos/anp/rossini_cibercrime.pdf. Acesso em 12 nov. 2022.

SANTOS, L.R; MARTINS, L.B; TYBUCSH, F.B.A. **Os Crimes Cibernéticos e o Direito a Segurança Jurídica: Uma Análise da legislação Vigente no Cenário Brasileiro Contemporâneo**. Anais do 4º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede. Santa Maria-RS, 2017.

SAWAYA, M. R. **Dicionário de informática e internet**. São Paulo: Nobel, 1999. 545 p. Disponível em: https://nosda18.files.wordpress.com/2009/04/dicionariode-informatica-e-internet.pdf. Acesso em 24 out. 2022.

SHERMAN, C.; Price, G. **A web invisível: descobrindo fontes de informação: os motores de busca não conseguem ver.** Medford: Cyberage Books, 2001.Disponivel em: https://docplayer.com.br/7515214-Web-invisivel-compreendendo-a-invisibilidade-no-ciberespaco-invisible-web-understanding-the-invisibility-in-cyberspace.html. Acesso em 9 nov. 2022.

TEFFÉ, C.S; MORAES, Maria Celina B. **Redes Sociais Virtuais: privacidade e responsabilidade civil análise a partir do marco civil da internet.** Pensar, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017. Acesso em 29 out. 2022.

THE TOR PROJECT. **Orbot Proxy com Tor.** Versão 16.0.5-RC-2- tor-0.3.4.9. [S.l.]: Guardian Project, 2018. Disponível em: https://www.torproject.org/ Acesso em 06 nov. 2022.

VIGNOLI, R. G**. A topografia da dark web e seus não lugares: por um estudo das dobras invisíveis do ciberespaço**. 2014. 153 f. Dissertação (Mestrado em Ciência da Informação) – Universidade Estadual de Londrina, Londrina, 2014. Disponível em: http://www.bibliotecadigital.uel.br/document/?view=vtls 000191992. Acesso em 18 out. 2022.

VIGNOLI, R. G.; Monteiro, S. D. **A Dark Web e seu conteúdo informacional. In: Seminário de Ciência da Informação, 5., 2015,** Londrina. Anais eletrônicos […] Londrina: UEL, 2015a. Disponível em: http://www.uel.br/eventos/cinf/index.php/secin2016/secin2016/paper/viewFile/266/186. Acesso em 10 out. 2022.

VIGNOLI, R. G.; Monteiro, S. D. **Dark Web e seus não lugares: por um estudo das dobras invisíveis do ciberespaço**. Link em Revista, v. 11, n. 1, p. 140-166, 2015b. Disponível em: https://doi. org/10.18617/liinc.v11i1.798. Acesso em 13 nov. 2022.

VIGNOLI, R. G.; Vechiato, F. L. **Dados pessoais, dados sensíveis e dados pessoais sensíveis: um contributo conceitual para a Ciência da Informação.** In: Farias, G. B.; Farias, M. G. G. (Org.). Competência e mediação da informação: percepções dialógicas entre ambientes abertos e científicos. São Paulo: Abecin, 2019. Disponivel em: http://www.abecin.org.br/e-books/. Acesso em 10 out. 2022.

WENDT, Emerson. **Crimes Cibernéticos: ameaças e procedimentos de investigação**/ Emerson Wendt; Higor Vinicius Nogueira Jorge. -2. Ed. – Rio de Janeiro: Brasport,2013. Disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/17. . Acesso em 14 nov. 2022.

WINKLER, I.; Gomes, A. T. **Infraestrutura adversária. In: Winkler, I.; Gomes, A. T. (Org.). Segurança persistente avançada: uma abordagem de guerra cibernética para implementar estratégias adaptativas de proteção, detecção e reação corporativa**. New Deli: Elsevier, 2017. p. 67-79.

ZILMAN, M. P. **Recursos de pesquisa e descoberta da Deep Web 2019. Recursos de direito e tecnologia para profissões jurídicas**, [S.l.], 2019. Disponível em: https://www.llrx.com/2019/01/deep-web-research-and-discovery-resources-2019/. Acesso em 22 out. 2022.