*Disciplinarum Scientia*. Série: Sociais Aplicadas, Santa Maria, v. 19, n. 2, p. 73-91, 2023.
Recebido em: 20.09.2023. Aprovado em: 27.12.2023.
ISSN 2318-678X
DOI: 10.37778/dscsa.v19i2.4689

# DESAFIOS E IMPLICAÇÕES DO DIREITO PENAL NA ERA DIGITAL: EXPLORANDO AS PROFUNDEZAS DA *DEEP WEB*

## *CHALLENGES AND IMPLICATIONS OF CRIMINAL LAW IN THE DIGITAL AGE: EXPLORING THE DEEP WEB*

**Guido Ruviaro Neto[1] e Alexandre de Oliveira Zamberlan[2]**

**RESUMO**

A *Deep Web* é uma ferramenta ou, até mesmo, uma cultura da sociedade digital e *online* que é formada por pessoas de diferentes idades, credos, gêneros, raças, intenções e tecnologias. Essa ferramenta tem gerado inúmeras interpretações e usos diversos, principalmente, em contextos controversos, ligados a grupos e/ou comunidades mal-intencionadas. Dessa forma, este texto aborda uma reflexão do assunto *Deep Web* sob a perceptiva do Direito Penal, tratando a concepção, funcionalidade e, sobretudo, as eventuais responsabilidades que podem ser implicadas a seus usuários. A discussão pretende correlacionar o tema com casos ocorridos e associados a aspectos do Direito Penal brasileiro, ou seja, suas leis e marcos jurídicos. Portanto, utilizou-se a pesquisa qualitativa, com objetivo exploratório, apoiada de pesquisa bibliográfica. O trabalho justifica-se, pois o impacto da *Deep Web* na sociedade digital pode ser considerado complexo e multifacetado, e pode variar dependendo de como é utilizada, pois pode influenciar questões sociais, políticas, econômicas e jurídicas.

**Palavras-chave:** *Deep Web*; Direito Penal; Internet.

***ABSTRACT***

*Deep Web is a tool or even a culture of digital and online society that is made up of people of different ages, creeds, genders, races, intentions and technologies. This tool has generated numerous interpretations and diverse uses, mainly in controversial contexts, linked to groups and/or communities with bad intentions. In this way, this text deals with a reflection on the subject of Deep Web from the perspective of Criminal Law, addressing design, functionality and, above all, the possible responsibilities that may be imposed on its users. The discussion intends to correlate the subject with cases that have occurred and are associated with aspects of Brazilian Criminal Law, that is, its laws and legal points. Therefore, we used qualitative research, with an exploratory objective, supported by bibliographical research. The research is justified, as the impact of the Deep Web on digital society can be considered complex and multifaceted, and can vary depending on how it is used, as it can influence social, political, economic and legal issues.*

***Keywords:*** *Deep Web; Criminal Law; Internet.*

1 Bacharel em Direito - FADISMA. Mestre em Nanociências - UFN. E-mail: guido.ruviaro@ufn.edu.br. ORCID: https://orcid.org/0009-0002-3072-4360.

2 Professor dos cursos de Computação UFN. E-mail: alexz@ufn.edu.br. ORCID: https://orcid.org/0000-0002-9815-2031

## INTRODUÇÃO

A Internet invisível, também conhecida como *Deep Web,* denota uma fração da Internet que permanece ausente nos índices dos tradicionais mecanismos de busca, ou seja, *Deep Web* é uma parte da World Wide Web que não está indexada pelos motores de busca convencionais e não é facilmente acessível pelos de navegadores padrão. Ela contempla conteúdos variados, como páginas web não indexadas, fóruns privados, redes sociais criptografadas e outros recursos *online* que exigem autorização para acesso (ORMSBY, 2019). Dessa forma, é possível afirmar que a *Deep Web* não necessariamente infringe leis, já que hospeda uma variedade de serviços legítimos, abarcando desde sistemas internos empresariais ou corporativos (redes locais), até bibliotecas protegidas *online* e serviços de correspondência eletrônica privada, por exemplo. Porém, frequentemente, entrelaça-se com sites que hospedam conteúdos questionáveis, que configuram domínios enigmáticos na Internet, nos quais transações de natureza criminosa e ilegal são perpetradas, englobando práticas como o tráfico de substâncias entorpecentes, comercialização de armamentos, esquemas fraudulentos, exploração de menores, entre tantas outras atividades ilícitas (LUCAS, 2015).

O crime digital apresenta-se de forma crescente e com um grau de complexidade nos processos de reconhecer, vigiar, analisar, combater e punir, principalmente, pelos meios dos órgãos formais vinculados aos campos da Lei, Justiça e do Direito Penal. Esse contexto é gerado ou promovido pelo fácil acesso à tecnologia (programas, *scripts*, ferramentas), métodos e, fundamentalmente, à informação (tutoriais e manuais *online*) disponibilizados em páginas web, vídeos ou fóruns de discussão, por exemplo. E todas essas facilidades possibilitam diversos delitos, desde fraudes, roubos de identidade, danos em infraestrutura computacional, desvio de valores, notícias falsas (FAVERO; FAVERO, 2021), ou seja, crimes cibernéticos.

Por meio da Internet, crimes tradicionais podem ser cometidos de forma que a vítima não tenha qualquer conhecimento da identidade física do autor da infração penal. E como já referido, em virtude desse ambiente digital, o cotidiano digital e *online* de uma pessoa pode ser integralmente invadido e exposto, fazendo com que a intimidade pessoal, em última análise, possa ser facilmente acessada com um simples clique em um computador (GRECO, 2019).

Dessa forma, um dos desafios que os campos da Lei, da Justiça e do Direito Penal enfrentam é acompanhar e, rapidamente, adaptar-se à evolução tecnológica, que ocorre em um ritmo acelerado. Essa necessidade de adaptação envolve a criação e atualização de leis que abordem questões emergentes relacionadas à cibercriminalidade, privacidade digital, crimes virtuais e outras complexidades tecnológicas, a fim de garantir a eficácia do sistema legal diante das transformações contínuas no cenário digital (PAULA *et al*., 2023).

Por fim, esta pesquisa buscou problematizar a questão dos desafios e aplicações do Direito Penal na era digital, com enfoque na *Deep Web*, esclarecendo que seus conteúdos podem ser vistos de

forma positiva e/ou negativa para a sociedade em geral. E para responder a problemática, utilizou-se de pesquisa qualitativa, apoiada em pesquisa bibliográfica, a fim de aprofundar a compreensão da temática, com foco exploratório em leis, artigos relacionados manuais e tutoriais de recursos computacionais, entre outros.

## EVOLUÇÃO HISTÓRICA E A SOCIEDADE EM REDE

A sociedade contemporânea atravessa um momento inquestionável no qual a Internet emerge como uma das tecnologias mais impactantes do mundo. Seja como um recurso vital para aqueles que nasceram em períodos equivalentes ou posterior à sua ascensão, ou como um desafio significativo para aqueles que a precederam. A Internet configura-se como uma intrincada rede, conectando dezenas de milhões de computadores e dispositivos móveis. Essa rede não apenas possibilita o acesso a uma quantidade virtualmente ilimitada de informações, mas também encurta as distâncias entre continentes, alterando fundamentalmente as bases materiais de tempo e espaço. Desse modo, proporciona a qualquer cidadão do mundo a capacidade de explorar uma vastidão de informações e culturas diversas, tudo isso sem sair do conforto de sua casa (PAESANI, 2014). Portanto, essa ferramenta não apenas transformou integralmente o cotidiano humano, mas também deu origem a novos métodos de trabalho e tendências comerciais que rompem com o modelo tradicional, no qual era necessário possuir uma loja física para prosperar no comércio (CAIÇARA JUNIOR; PARIS, 2007).

É relevante, neste contexto, traçar um breve, mas significativo histórico da Internet, desde seus primórdios até a sua atual configuração amplamente difundida e utilizada pela sociedade. Contudo, para melhor compreensão do atual cenário da Internet, onde há sua integração ao cotidiano, é crucial reconhecer o marcante avanço tecnológico que tornou isso possível. O surgimento da Internet pode surpreender muitos, uma vez que, inicialmente, foi concebida para propósitos militares. Em sua origem, trata-se de uma rede de computadores estabelecida por uma agência do Departamento de Defesa dos Estados Unidos no ano de 1969 (CASTELLS, 2003).

Desse modo, de sua gênese, então denominada *Arpanet* (*Advanced Research Projects Agency Network* - Rede da Agência de Pesquisas em Projetos Avançados), a ferramenta surgiu da necessidade de se criar um sistema de telecomunicações que não fosse interrompido por um ataque nuclear inimigo aos Estados Unidos. Um pressuposto criado em meio a chamada guerra fria, entre os anos de 1962 e 1979 (CAIÇARA JUNIOR; PARIS, 2007). Dessa forma, cientistas militares e civis norte-americanos criaram em sua agência de projetos avançados pequenas redes locais (*LAN - Local Area Network*), distribuídas em todo o país e ligadas por meio de redes de telecomunicação geográfica (*WAN - Wide Area Network*). Assim, caso alguma cidade norte-americana fosse destruída por um ataque nuclear, essa rede (chamada de *Inter Networking*) conhecida como Internet, continuaria a permitir comunicação entre as cidades que restassem (BERNERS-LEE, 1999).

Ademais, essa criação trouxe revolução para a preservação documental, por trazer a capacidade de digitalizar documentos físicos e armazená-los *online.* Assim, bibliotecas e instituições culturais adotaram a digitalização como uma forma de proteger e disponibilizar seus acervos de maneira acessível a um público global. A digitalização não apenas evitou a deterioração física de documentos frágeis, mas também permitiu que esses documentos fossem pesquisados, compartilhados e replicados virtualmente (KENNEY; MCGOVERN, 2003).

Outro fator que impulsionou o crescimento da Internet, foi seu desmembramento em duas redes, a *Arpanet*, cuja finalidade ficou atrelada a pesquisas científicas e universitárias, e a *Milnet* (*Military Network)*, cujo propósito e utilização tinha cunho exclusivamente militar e de defesa. Para que esse desmembramento fosse possível, o protocolo TCP/IP foi fundamental, uma vez que por meio dele ambas as redes puderam se comunicar e suportar milhões de conexões à rede (LEINER *et al*., 2009).

Essa rede mundial de computadores, ou Internet, pode ser considerada como o maior repositório de informações existente, pois serve de repositório para informações diversas e de livre acesso na maioria dos casos. E com o aumento da disponibilidade e de velocidade da, ao redor do mundo, ela tornou-se também um meio de comunicação em massa, uma vez que as pessoas podem realizar videoconferências, compartilhar vídeos, realizar transmissões digitais e *online* (NETFLIX, 2020).

Paralelamente a criação da *Arpanet*, uma comunidade de jovens pesquisadores californianos desenvolvia um projeto que viria a revolucionar completamente o mundo. Tratava-se do computador pessoal, que era um projeto de pessoas no momento certo e no período certo, pois tinham acessos às pesquisas e aos diversos componentes eletrônicos que eram disponibilizados no Vale do Silício (LEVY, 2010).

Portanto, a Internet surgiu em um período em que computadores pessoais chegavam ao mercado e que as comunicações estavam em processo de barateamento. E isso propiciou o aumento considerável do consumo de computadores com acesso à rede mundial, o *World Wide Web* ou *Web*, ou ainda *WWW.* E no ano de 1989, na Europa, mais especificamente em Genebra, Suíça, definiu-se o padrão de comunicação (protocolos) em que usuários, empresas, grupos, instituições e organizações estariam submetidos para comunicação e utilização de serviços, como navegar por páginas web, trocar arquivos, reproduzir áudios e vídeos, entre tantos outros (ABBATE, 2000).

A interatividade aprimorada na web decorre do fato de as páginas estarem conectadas por meio de *hyperlinks*. A *World Wide Web* opera com base em três elementos essenciais. O primeiro é a URL (*Universal Resource Locator*), que especifica o endereço único de cada página na Internet. O segundo elemento é o HTTP (*Hypertext Transfer Protocol*), que padroniza a linguagem de comunicação entre clientes e servidores web. Por fim, há o HTML (*Hyper Text Markup Language*), que codifica informações para que possam ser exibidas em diversos dispositivos simultaneamente. Essa integração resulta em maior facilidade para os usuários navegarem na Internet, já que imagens e textos estão interligados por palavras-chave, proporcionando uma experiência de navegação mais ágil e leve para os computadores (MARQUES; MARTINS, 2006).

No início da década de noventa, uma significativa parcela dos computadores nos Estados Unidos já contava com acesso à Internet, impulsionada pelo surgimento de diversos provedores e pela comercialização das conexões. Esse cenário desencadeou um crescimento exponencial da Internet, transformando-a em uma rede global de computadores interconectados. Esse avanço foi viabilizado pelo projeto pioneiro da Arpanet, que permitia o estabelecimento descentralizado de redes, adotando protocolos abertos e uma abordagem de múltiplas camadas. Ao longo do tempo, novos nós foram adicionados, expandindo e aprimorando essa intrincada teia que representa a Internet (CASTELLS, 2003).

No Brasil, a chegada da Internet também testemunhou êxitos semelhantes aos experimentados globalmente. O país viu replicadas situações bem-sucedidas ocorridas em diversos lugares do mundo, como a utilização da web para serviços bancários, declaração de imposto de renda e comércio eletrônico. Esses usos catalisaram uma expressiva quantidade de transações na rede global. Similarmente aos Estados Unidos, a Internet teve seu início no meio acadêmico brasileiro, ingressando no país em 1989 por meio da Rede Nacional de Pesquisas (RNP). Esse marco resultou de uma colaboração robusta entre a comunidade acadêmica de ciência da computação e o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), refletindo um esforço conjunto para viabilizar a expansão e o acesso à internet no Brasil (SILVA, 2000). No entanto, a Internet comercial só chegou efetivamente ao público brasileiro em 1995, com uma velocidade inicial de 2 Mbps (megabytes por segundo), disponibilizada por um servidor da Embratel. Esse serviço foi resultado da colaboração entre a Embratel e outras 11 empresas. No mesmo ano, visando regulamentar os serviços de Internet no país, foi instituído o Comitê Gestor da Internet no Brasil (CGI.br), por meio da Portaria Interministerial nº 147, datada de 31 de maio de 1995 (CAIÇARA JUNIOR; PARIS, 2007).

Até este ponto, é possível que ainda ocorra questionamentos sobre o verdadeiro significado da Internet, pois seu conceito permanece pouco claro. É possível compará-la a uma teia de aranha, uma rede que conecta milhões de computadores ao redor do planeta de maneiras diversas, como através de cabos, redes telefônicas e até mesmo satélites. Essa complexa rede pode ser analogamente relacionada a uma rede telefônica, embora, a partir de um computador, o usuário tenha inúmeras possibilidades de utilização, muito além do que seria viável em um telefone fixo. A Internet oferece possibilidades infinitas, conforme destacado por Castells (2003).

Entretanto, a Internet não se destaca apenas pelos seus aspectos positivos. Segundo o cientista político Norman Nie, da Universidade de Stanford em São Francisco, a Internet pode ser uma ferramenta de isolamento social. Nie observa que as pessoas muitas vezes dedicam mais tempo aos seus computadores do que às relações interpessoais, resultando na perda do contato com outros seres humanos e, consequentemente, no distanciamento das emoções do mundo real (PAESANI, 2014). Além disso, Zygmunt Bauman (1999) aborda a ideia de que alguns indivíduos, em vez de sair para viajar, imergem na web, explorando-a e compartilhando mensagens de todas as partes do globo na tela do computador. Essa perspectiva reitera a noção de que, nos dias de hoje, as pessoas têm a tendência

de conhecer o mundo principalmente através da janela de seus computadores, o que pode resultar na perda do apreço por experiências reais de descoberta.

Na mesma linha de pensamento, há estudos que fortalecem a perspectiva do isolamento social relacionado ao uso da Internet, sugerindo que a rede de computadores contribui para o afastamento dos usuários de seus círculos familiares e sociais, podendo agravar situações de solidão e depressão. Importante ressaltar que esse comportamento não é universal, mas sim pode afetar indivíduos mais engajados na utilização frequente da Internet (CASTELLS, 2003; NETFLIX, 2020).

Em contrapartida a essa perspectiva, Castells (2003) também discute a ideia de que a Internet pode desempenhar um papel crucial no fortalecimento da comunicação, deixando de ser meramente um instrumento de alienação do mundo real. Isso se deve ao fato de que a interação *online* pode complementar e enriquecer os laços já existentes. As facilidades proporcionadas pela Internet ampliam significativamente as opções e formas de nos relacionarmos, possibilitando a interação com indivíduos distantes e facilitando o contato com um número mais amplo de pessoas.

Um aspecto que tem gerado desconforto entre os usuários da Internet é o uso do *marketing* digital por meio de sistemas de recomendação. Essa ferramenta tem a capacidade de exibir anúncios baseados nas atividades de pesquisa e acesso do usuário em redes sociais, por exemplo. Para muitos, isso representa uma clara violação da privacidade, já que a ferramenta sugere que todas as interações do usuário na rede ficam registradas em servidores. Essas informações são posteriormente compartilhadas com sites de comércio, que as utilizam para direcionar publicidade específica aos nossos gostos pessoais. Embora alguns vejam esse comportamento da web como positivo, uma vez que usuários apenas receberiam informações alinhadas aos interesses, há também o argumento contrário. Esse método pode limitar a exposição a usuários a novas descobertas, limitando as possibilidades de resultados ou oportunidades às pesquisas e interesses de usuários (TAGIAROLI, 2014; NETFLIX, 2020).

Diante desse percurso da Internet, torna-se evidente uma evolução natural da sociedade em direção a uma Sociedade em Rede. Esse avanço nas tecnologias de informação e comunicação pode ser equiparada à transformação proporcionada pelas energias, eletricidade e combustíveis fósseis durante a Revolução Industrial (CASTELLS, 2018). A troca de informações em tempo real, que caracteriza esse cenário, representa um novo paradigma na comunicação, agora respaldado por inúmeras ferramentas inovadoras. Esse avanço consolida as Tecnologias Digitais de Informação e Comunicação como elementos fundamentais nessa trajetória evolutiva (TICs) (LEVY, 2010).

Outro aspecto relevante a ser abordado sobre a Internet diz respeito à cultura *hacker*. Originada como uma subcultura de entusiastas da tecnologia e da computação ao longo da história, essa cultura não apenas se destaca por suas contribuições positivas, mas também por práticas controversas e impactos negativos. Embora muitos adeptos da cultura *hacker* tenham canalizado seus esforços para aprimorar sistemas, promover a disseminação livre de informações e conceber soluções

inovadoras, uma vertente obscura desse movimento revelou-se por meio de atividades de natureza maliciosa e ilegal (HIMMA, 2018).

Nesse contexto, as motivações subjacentes às atividades *hackers* prejudiciais podem variar desde a busca por reconhecimento até a exploração de vulnerabilidades de segurança com o intuito de obter lucros. Em algumas situações, *hackers* adotam práticas de "hacktivismo" para defender agendas políticas ou sociais, o que resulta em complexas implicações legais e sociais. Logo, essas ações frequentemente instigam dilemas éticos, questionando os limites entre a liberdade de expressão, os direitos individuais e os danos causados a terceiros (MOORE, 2005).

Além disso, as consequências decorrentes das atividades *hackers* prejudiciais podem ser abrangentes e de longa duração. Para além dos prejuízos financeiros, organizações correm o risco de sofrer danos em sua reputação e na confiança pública depositada nelas. Frequentemente, governos e agências de aplicação da lei respondem com medidas rigorosas para identificar, processar e sancionar os *hackers* envolvidos em atividades criminosas. No entanto, a natureza global da Internet e a habilidade dos *hackers* de operarem de forma anônima apresentam desafios significativos para a aplicação efetiva da lei (HIMMA, 2018).

Outra manifestação adversa da cultura *hacker* abrange a invasão da privacidade e a espionagem cibernética. *Hackers* têm a capacidade de comprometer sistemas, buscando acesso não autorizado a dados pessoais, informações financeiras e comunicações privadas. Adicionalmente, governos e grupos com agendas específicas podem empregar *hackers* para conduzir operações de espionagem cibernética, visando a coleta de informações sensíveis de indivíduos, organizações e até mesmo de outras nações (DEIBERT; ROHOZINSKI, 2010).

Nesse sentido, a relação entre a cultura *hacker* e a Deep Web pode ser complexa, visto que alguns *hackers* podem ser atraídos por essa parte da Internet com o objetivo de investigar e compreender as tecnologias que sustentam o anonimato e a privacidade. No entanto, essa exploração pode rapidamente evoluir para atividades ilícitas, à medida que indivíduos se aproveitam do manto do anonimato para cometer delitos. Paralelamente, *hackers* com uma ética sólida podem demonstrar interesse em explorar a Deep Web com o intuito de identificar ameaças à segurança cibernética e propor soluções apropriadas (LEVY, 2010).

## *DEEP WEB*

Para qualificar a compreensão sobre a *Deep Web*, é necessário abordar o aspecto do tamanho da Internet, uma característica que escapa a uma descrição direta, sendo, na verdade, algo praticamente inimaginável. Muitos veem a Internet como uma teia, uma rede de tubos interconectados ao redor do mundo. No entanto, uma concepção mais contemporânea compara a Internet a um *iceberg*, uma analogia trazida à tona pela natureza dos *icebergs*, em que apenas cerca de 10% de seu tamanho

é visível acima da água, enquanto o restante permanece nas profundezas do oceano (LUCAS, 2015). Dessa maneira, a Internet que se visualiza e se acessa em computadores, frequentemente por meio de buscadores como Bing, Google ou Yahoo, pode ser comparada a um iceberg. O conteúdo que se tem acesso representa apenas 10% da capacidade total da Internet, sendo esses 10% denominados *Surface Web* ou Internet da superfície. A Internet da superfície está sujeita a uma vigilância constante por parte do governo. O que está abaixo da superfície, contendo o restante do conteúdo da Internet, é conhecido como *Deep Web* ou Internet profunda, estimando-se que seu tamanho seja quinhentas vezes maior que o da *Surface Web*. Esse ambiente é propício para não ser rastreado, sendo utilizado para diversos fins, tanto lícitos quanto ilícitos (LUCAS, 2015).

Embora a *Deep Web* seja consideravelmente maior que a *Surface Web*, sua popularidade ainda permanece relativamente baixa. Este fenômeno pode ser atribuído à má reputação que a *Deep Web* possui entre o público em geral. Além disso, a mídia tende a destacar predominantemente os aspectos negativos da *Deep Web*, contribuindo para a percepção negativa. É importante observar que muitos usuários fazem uso do anonimato proporcionado por essa rede para realizar atividades ilícitas (ORMSBY, 2019).

Ao contrário da *Surface Web*, que possui motores de busca para facilitar a localização de informações, na *Deep Web*, esse tipo de ferramenta não existe. Portanto, os usuários precisam saber onde procurar o que desejam encontrar. Para isso, existem alguns sites em formato de fóruns, sendo o mais conhecido o *Hidden Wiki*, que atua como um índice para os usuários da *Deep Web*. Nele, é possível encontrar uma variedade de *links* para outros sites e artigos em formato WIKI (SANTOS; VIDAL, 2014).

Desse modo, diversos projetos dedicam-se à investigação, construção e aprimoramento de sistemas de comunicação anônimos que são usados para o acesso da *Deep Web*, como é o caso do programa *Onion Routing*, tendo este o foco na baixa latência de tráfego na internet, assim, oferecendo como característica a resistência à análise de tráfego, o que proporciona uma espécie de proteção à ataques de espionagem tanto interno quanto externo em uma organização (KOZAKIEWICZ, 2018).

## O LADO POSITIVO DA *DEEP WEB*

Um dos principais motivos que leva pessoas a utilizarem a *Deep Web* é o anonimato. Para muitos, a prática de *marketing* digital por meio de sistemas de recomendação viola a privacidade, e, por isso, alguns usuários buscam essa privacidade. Em países como China, Irã e Coreia do Norte, onde a Internet convencional é rigidamente controlada, a *Deep Web* é utilizada como meio de comunicação. Isso possibilita que usuários e correspondentes internacionais se comuniquem, permitindo que jornalistas estrangeiros realizem coberturas para seus meios de comunicação diretamente desses países com forte controle sobre as mídias. Vale ressaltar que especialistas atribuem o sucesso da Primavera Árabe ao uso da *Deep Web*, destacando a importância desse meio em contextos de regimes autoritários (MELLO, 2013). A Primavera Árabe, que ocorreu entre 2010 e 2012, representou um

conjunto de movimentos sociais que emergiram no Oriente Médio e no Norte da África, resultando em profundas transformações políticas e sociais na região. Concomitantemente, a utilização da *Deep Web* como ferramenta de mobilização e comunicação ganhou destaque durante esses eventos, proporcionando uma plataforma para a coordenação e disseminação de informações por meio de fóruns em redes anônimas. Essa abordagem permitiu discussões abertas sobre as questões políticas e sociais enfrentadas pelos manifestantes, fomentando a conscientização e a participação ativa (CASTELLS, 2016).

Outro aspecto positivo encontrado na *Deep Web* é sua utilidade para a área acadêmica, sendo um ambiente propício para a pesquisa. Isso se deve ao fato de existirem sites que realizam buscas na web profunda e disponibilizam seu conteúdo em sites convencionais da Internet. Um exemplo notável é o site *BrightPlanet*, criado por Mike Bergman, que utiliza uma ferramenta de busca na *Deep Web* para trazer informações para a *Surface Web.* Isso permite que usuários que tenham receios de acessar diretamente a *Deep Web* possam usufruir do seu conteúdo em um local que considerem mais seguro (SOUZA, 2014).

Embora a *Deep Web* ainda sofra com uma má reputação para muitos, devido ao mau uso por alguns usuários, é amplamente reconhecido entre os usuários o ponto crítico de a rede ser utilizada por pedófilos para divulgação e apologia à prática desse crime. No entanto, paradoxalmente, foi na própria *Deep Web* que foi testemunhado um movimento significativo contra a pedofilia infantil, conhecido como "Operação Darknet". Esse nome foi atribuído pelo grupo *Anonymous*[3] a uma série de ataques que realizaram contra esses pedófilos (CIRIACO, 2011).

Assim, essa operação realizada pelo grupo *Anonymous* retirou serviços da rede profunda e divulgou os nomes de mais de 1,5 mil usuários que acessavam conteúdo ilícito. Os ataques resultaram no desligamento de um servidor que hospedava cerca de 40 sites com pornografia infantil. Anteriormente, o grupo havia alertado os mantenedores do servidor para que apagassem esse conteúdo, mas, como não foram atendidos, invadiram e removeram o material. O *Freedom Hosting*, um site que continha mais de 100 gigabytes de conteúdo relacionado à pedofilia, também foi tirado do ar (CIRIACO, 2011).

Logo, é importante ter de perceber que nem toda atividade na *Deep Web* é ilegal ou maliciosa. A *Deep Web* também é usada para fins legítimos, como preservação da privacidade, pesquisa acadêmica, comunicação segura e outras atividades que requerem anonimato. No entanto, é crucial ter consciência dos riscos associados e das atividades ilícitas presentes nesse ambiente (KOZAKIEWICZ, 2018).

## O LADO NEGATIVO DA *DEEP WEB*

Da mesma forma que o anonimato proporcionado pela rede profunda pode ser considerado positivo, é possível enxergá-lo por outro ângulo, uma vez que o uso desse anonimato pode ser direcionado para práticas nocivas e ilícitas na *Deep Web*. Um dos temas mais destacados quando se trata

3 Grupo de ativistas *hackers* que se destacou por suas ações de protesto online, defesa da liberdade de expressão e participação em uma variedade de operações digitais em todo o mundo. Disponível em: https://tecnoblog.net/responde/qual-a-origem-e-historia-do-grupo-anonymous/

de atividades ilícitas nesse ambiente é a pedofilia infantil. Usuários pedófilos aproveitam o anonimato para divulgar materiais e experiências na *Deep Web*, como mencionado anteriormente. Embora o grupo *Anonymous* tenha conduzido uma grande operação contra esses usuários, isso não os desencoraja, bem pelo contrário, novos usuários com essa finalidade entram frequentemente na *Deep Web* (ORMSBY, 2019).

Foram identificados sites do tipo *crowdfunding*[4] na *Deep Web*, nos quais usuários divulgam conteúdo de pedofilia infantil. Nesses sites, os usuários seguem uma dinâmica semelhante ao *Kickstarter*[5]: eles estabelecem um valor específico como meta e, quando essa quantia é atingida, o conteúdo abusivo com menores é divulgado na *Deep Web* para aqueles que contribuíram financeiramente. Além disso, alguns desses sites apresentam uma seção denominada "*We Care*", na qual afirmam que essa prática se destina a garantir um salário justo para as crianças e jovens envolvidos, revelando a obscuridade presente nessa rede (COOK, 2014).

Outra prática ilícita comum na rede profunda está associada ao tráfico de drogas, exemplificado pelo caso do conhecido site *Silk Road*, também conhecido como Rota da Seda. Esse caso ganhou notoriedade a ponto de ser documentado no filme "*Deep Web*", que narra a história de Ross William Ulbricht, detido por ser o cérebro por trás do *Silk Road*. Este site é considerado o primeiro mercado anônimo de grande impacto na *Deep Web*, tendo sido fundado em 2011 e modelado a partir da plataforma da Amazon. O *Silk Road* tinha o propósito de ser uma plataforma para transações entre vendedores e compradores de drogas, aproveitando-se do anonimato oferecido pela rede profunda (THOMPSON, 2015).

Conforme informações do FBI (*Federal Bureau of Investigation* - Departamento Federal de Investigação), até o encerramento do site *Silk Road*, em 2013, ele contava com 1.400 fornecedores e mais de 950 mil usuários registrados. Estima-se que o site intermediou mais de 1,2 milhão de transações entre fornecedores e compradores, totalizando cerca de 214 milhões de dólares (THOMPSON, 2015). Além disso, o FBI sugere que o criador do *Silk Road* teria lucrado aproximadamente 20 mil dólares por dia por meio das comissões de vendas, totalizando cerca de 3,4 milhões de dólares (EDWARDS, 2013).

Uma outra prática frequentemente associada à *Deep Web*, embora com poucas provas concretas, seria a contratação de assassinos de aluguel na rede profunda. Apesar de ser bastante comentada, não há evidências substanciais que comprovem essa prática. No caso envolvendo o criador do *Silk Road*, a polícia americana encontrou indícios de que ele teria contratado um assassino de aluguel em resposta a chantagens feitas por outro usuário da *Deep Web* (EDWARDS, 2013).

---

4 Prática de financiamento coletivo que envolve a obtenção de fundos para um projeto, causa ou empreendimento por meio de contribuições financeiras de um grande número de pessoas. Disponível em: https://sebrae.com.br/sites/PortalSebrae/artigos/entenda-o-que-e-crowdfunding,8a733374edc2f410VgnVCM1000004c00210aRCRD

5 Uma das plataformas de financiamento coletivo *online* mais populares e bem-sucedidas do mundo. Disponível em: https://canaltech.com.br/startup/o-que-e-o-kickstarter/

Cabe ressaltar que a *Deep Web* A Deep Web é conhecida por abrigar uma variedade de atividades, algumas das quais podem ser consideradas negativas ou ilícitas, como: tráfico de drogas; pornografia infantil; mercados negros e contrabando (informações de cartões de crédito, podem ser encontrados em mercados negros *online*); atividades criminosas (serviços contratados para realização de ataques cibernéticos); fóruns de crime e violência (ambientes de discussão de atividades criminosas, incluindo esquemas de fraude e violência); contratação de assassinos (ORMSBY, 2019).

## DIREITO PENAL NA ERA DIGITAL

Diante dessa constante evolução tecnológica no campo da informação, tem-se observado uma gradual substituição e modificação de conceitos e terminologias. Expressões que, em tempos passados, eram reservadas ao domínio computacional, agora fazem parte do léxico da Doutrina Jurídica e dos poderes constituídos. Consequentemente, à medida que a terminologia se transforma, é inevitável que a criminalidade adquira novas modalidades de manifestação, especialmente considerando as lacunas que, por vezes, subsistem no âmbito da lei penal (CRESPO, 2011). Nesse contexto, novos atos delituosos emergem, como os crimes digitais ou cibernéticos, cometidos no ambiente virtual por meio da informática em geral. Esses crimes são perpetrados por dispositivos tecnológicos e atentam contra os dados de terceiros, notadamente contra a vítima. Assim, o criminoso utiliza-se desse sistema de informática para atentar contra interesses ou bens protegidos, tais como o direito individual à privacidade, à honra, à ordem econômica, integridade corporal, entre outros (ROSA, 2002).

Ainda, os delitos perpetrados por meio de sistemas informáticos apresentam características notáveis, sendo três significativas. A distância no tempo e no espaço destaca-se, pois, no contexto digital, o suposto criminoso não necessita de presença física ou temporal para a execução do delito. Outra característica é a facilidade de encobrimento, conforme o próprio nome indica, reside na aptidão para ocultar evidências e rastros da prática criminosa. Por fim, a dificuldade probatória é uma decorrência da complexidade inerente aos delitos informáticos, envolvendo a manipulação de dados e programas, criando obstáculos significativos na obtenção de provas sólidas (GRECO, 2019).

Assim, diante do aumento notório de novos golpes criminosos, surge a necessidade de aplicação da legislação vigente no ordenamento jurídico brasileiro para coibir, de maneira eficaz, as infrações perpetradas no ambiente virtual. É imperativo também intensificar as investigações e estabelecer sanções mais severas, com o intuito de dissuadir os infratores e penalizá-los adequadamente. Até o momento, persiste uma considerável lacuna no que concerne às punições e investigações relacionadas aos delitos no âmbito digital. Os crimes virtuais praticados nesse espaço, tendem a não deixar rastros que possam levar à identificação do autor da transgressão, revelando a vulnerabilidade do nosso ordenamento jurídico perante tais práticas delituosas (ALVES, 2020).

Ademais, todas as condutas direcionadas a bens jurídicos relacionados à informática, como sistemas e dados, podem ser classificadas como crimes digitais próprios. Em contraste, aquelas condutas que visam bens jurídicos tradicionais, não relacionados à tecnologia, são consideradas crimes digitais impróprios. Essa distinção fundamenta-se na divisão entre meios eletrônicos como objeto protegido (bem jurídico) e meios eletrônicos como instrumentos utilizados para prejudicar outros bens (CRESPO, 2011; ALVES, 2020).

Ainda é possível citar alguns exemplos de crimes digitais, como a intrusão informática, também conhecida como invasão de dispositivo informático, ou ainda *hacking*, que consiste no acesso não autorizado de um usuário ao sistema alheio. Também se pode mencionar o 'furto' de identidade virtual, no qual o criminoso se apropria das características e identificações da vítima para se passar por ela. Por fim, um dos tipos mais comuns de crimes digitais é a inserção de *malwares*, também conhecido como inserção de código malicioso em dispositivo informático alheio, visando modificar, alterar ou até mesmo destruir dados da vítima (ALVES, 2020). Desse modo, pode-se trazer exemplos de crimes digitais impróprios, como os crimes contra a honra, ameaça, falsidade ideológica e estelionato. Esses delitos, já tipificados no Código Penal, passaram a ser cometidos por meio do auxílio da tecnologia, ganhando grande repercussão midiática. Isso ocorre porque geram sensação de insegurança e medo entre os usuários de dispositivos tecnológicos (RONCADA, 2017).

Até o momento, a legislação penal brasileira, em sua estrutura fundamental, é essencialmente composta pelo Código Penal (Lei 2.848/40) e pelo Código de Processo Penal (Lei 3.689/41), complementada por uma variedade de leis esparsas que introduziram alterações ao longo do tempo nesses documentos. Além disso, a legislação penal brasileira é enriquecida por normas especiais que abordam questões específicas, reforçando o arcabouço legal. Em resposta às inovações do Direito Digital, diversas dessas legislações mais recentes têm demonstrado uma crescente preocupação, buscando regulamentar de forma precisa as condutas que possam ser consideradas como crimes no contexto digital (PAULA *et al*., 2023). Desse modo, a Lei 12.015/2009 desempenhou um papel pioneiro ao abordar, dentro do arcabouço legal, a crescente preocupação que surgia na época em relação à criminalidade digital. Esta legislação incluiu uma emenda ao Estatuto da Criança e do Adolescente (ECA), Lei 8.069/90, por meio do artigo 244-B, acréscimo legal que estabeleceu que o crime de corrupção ou facilitação à corrupção de menores também poderia ser perpetrado por meios eletrônicos (PAULA *et al*., 2023).

Ainda, é possível trazer à tela a Lei 12.737/2012, popularmente conhecida como 'Lei Carolina Dieckmann'. Essa lei recebeu esse nome em homenagem à atriz Carolina Dieckmann, que teve sua privacidade violada por meio da divulgação indevida de fotos íntimas. Essa legislação foi aprovada e promoveu alterações no Código Penal, introduzindo a conduta tipificada como 'invasão de dispositivo informático'. Além disso, estabeleceu sanções e circunstâncias agravantes para essa nova categoria de delito. Posteriormente, a referida lei foi aprimorada e atualizada pela Lei 14.155/2021, expandindo a definição de infração para abranger qualquer conduta que envolva a invasão de dispositivo

informático, com o objetivo específico de acessar dados e informações de forma não autorizada, seja essa autorização expressa ou tácita por parte do titular dos dados em questão (BARRETO *et al*., 2022). Nesse contexto, no que diz respeito à invasão de dispositivo informático, não é incomum que usuários optem por não utilizar senhas de acesso em seus computadores, o que, por conseguinte, permite que qualquer pessoa com acesso ao dispositivo possa acessar seu conteúdo. No entanto, é importante ressaltar que mesmo na ausência de senhas de acesso, é proibido invadir um computador alheio, a menos que haja uma permissão expressa ou tácita por parte do proprietário. Já em termos de tipificação legal, a infração penal somente ocorrerá quando o agente invasor efetuar uma violação indevida do mecanismo de segurança, em conformidade com os requisitos estabelecidos no tipo penal em análise (GRECO, 2019).

Ademais, cabe ressaltar que o delito em questão é considerado um crime formal, ou seja, sua consumação ocorre no momento em que o agente invade o dispositivo informático da vítima, por meio da violação indevida de um mecanismo de segurança ou da instalação de vulnerabilidades, independentemente da concretização do resultado almejado pelo invasor, que pode consistir na adulteração ou destruição de dados ou informações da vítima, ou na obtenção de vantagem ilícita. Não se faz necessário que o resultado visado pelo agente se efetive para que o crime seja considerado consumado (CUNHA, 2023).

Outrossim, a Lei 12.965/2014, conhecida como Marco Civil da Internet, veio estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil. Por meio dessa legislação, foram conceituados diversos termos que devem ser empregados na interpretação dos tipos penais relacionados à Internet. Um exemplo é a própria definição de Internet que a legislação traz, conforme exposto no inciso I do artigo 5º da referida lei, a descreve como um sistema composto por um conjunto de protocolos lógicos, estruturado em escala global para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diversas redes (GRECO, 2019). Logo, com a implementação do Marco Civil da Internet, a proteção dos dados dos usuários é substancialmente reforçada, sendo sua quebra permitida somente mediante ordem judicial. Isso implica que, caso um internauta deseje encerrar sua conta em uma plataforma de rede social ou serviço *online*, ele pode solicitar a exclusão definitiva de seus dados pessoais, pois, após a entrada em vigor da Lei, fica assegurado ao usuário que seus dados pertencem a ele, e não a terceiros (ALVES, 2020).

Ainda, outra inovação significativa é a garantia da privacidade das comunicações, que anteriormente era limitada e não se aplicava aos serviços de e-mail, por exemplo. Portanto, a partir desse Marco Legal, o conteúdo das comunicações privadas em meios eletrônicos passa a receber a mesma proteção de privacidade que já era assegurada nos meios de comunicação tradicionais, como cartas e conversas telefônicas. Assim, a criação explícita de valores como a inviolabilidade do usuário e de suas comunicações e dados representa uma nova realidade que merece ser protegida (ALVES, 2020).

O ordenamento jurídico brasileiro experimentou uma inovação legislativa que autoriza a infiltração policial em ambientes virtuais para a investigação de infrações penais relacionadas a atos de pedofilia, por meio da Lei 13.441/2017. Este campo prático de atuação policial suscita a aplicação de conceitos resultantes da convergência entre a Criminologia e a arte, pois a escolha do policial infiltrado requer critérios específicos, notadamente a necessidade de que este seja alguém familiarizado com os meios eletrônicos e a linguagem da Internet, bem como psicologicamente preparado para enfrentar o repugnante universo dos pedófilos e outros agressores de crianças e adolescentes (FAVERO; FAVERO, 2021).

Sendo assim, a mencionada legislação representa uma faceta adicional do Direito Penal Digital, focando na regulamentação de procedimentos destinados a contribuir para a investigação e responsabilização de condutas criminosas ocorridas no ambiente virtual. É imperativo que tais regulamentações sejam estabelecidas de forma explícita por meio de lei, a fim de assegurar um controle estrito da legalidade e da legitimidade desses procedimentos investigativos, o que é essencial para evitar que todo o esforço empreendido pelo aparato judicial seja posteriormente contestado (PAULA *et al*., 2023). Além disso, é fundamental ressaltar que o artigo 154-A do Código Penal estabelece como crime a invasão de dispositivo informático alheio. No entanto, a legislação de infiltração virtual introduziu uma cláusula de exclusão da ilicitude, conforme previsto no *caput* do artigo 190-C, destinada a proteger o agente policial infiltrado de responder por esse delito. Logo, para que essa cláusula de exclusão seja eficaz, é necessário que se cumpram alguns requisitos, tais como a infiltração somente nos casos descritos na seção V, autorização judicial, entre outros (LARA, 2021).

Nessa senda, vale destaque para a Lei 13.709/2018, Lei Geral de Proteção de Dados ou LGPD, que introduziu novos direitos e parâmetros comportamentais que, quando infringidos, podem resultar em condutas tipificadas em outros dispositivos legais já existentes, como, por exemplo, o crime de invasão de dispositivos informáticos previsto no artigo 154-A do Código Penal. Ainda que existam exceções expressas de aplicabilidade na LGPD, o reconhecimento da necessidade de regulamentar a proteção de dados também no contexto criminal não passou despercebido pelo Congresso Nacional Brasileiro. Em resposta a essa demanda, foi instituída uma Comissão Especial de Juristas com o objetivo de elaborar uma legislação específica sobre o tema (PAULA *et al*., 2023). Além disso, é relevante o notável avanço legislativo trazido pela Lei 13.718/2018, a qual promoveu alterações substanciais no Código Penal brasileiro. Esta reforma legal resultou na criminalização de condutas relacionadas à divulgação de conteúdo íntimo sem o consentimento da vítima. Sendo importante ressaltar que a prática conhecida como 'pornografia da vingança', encontra-se especificamente prevista no parágrafo primeiro do artigo 218-C do Código Penal, caracterizando-se como uma circunstância que enseja aumento da pena (FAVERO; FAVERO, 2021). Ainda, a Lei 14.132/2021 introduziu uma importante alteração no Código Penal, acrescentando o artigo 147-A para tipificar o crime de perseguição, conhecido como *stalking*. Este delito pode ser cometido por qualquer meio, desde que ocorra a invasão ou perturbação da esfera de liberdade ou privacidade da vítima. Sendo que frequentemente essa

conduta também ocorre no ambiente virtual, é válido salientar que a perseguição pode ocorrer fora do ambiente virtual, não sendo restrita aos meios eletrônicos ou à Internet. No entanto, quando realizada no ambiente virtual, a conduta de perseguição não apenas se torna mais difícil de ser comprovada ou reprimida, mas também pode resultar em outros crimes, como especialmente aqueles relacionados à proteção da intimidade e da privacidade (PAULA *et al*., 2023).

## CONSIDERAÇÕES FINAIS

A ascensão da Internet e, subsequentemente, da *Deep Web*, desencadeou uma revolução na abordagem à preservação e compartilhamento de documentos físicos. A capacidade de digitalizar e armazenar informações em um ambiente virtual abriu horizontes anteriormente inexplorados em termos de acessibilidade, disseminação e conservação de dados. No entanto, a reflexão sobre os desafios contínuos associados à preservação digital emerge como uma questão crucial, visando garantir a salvaguarda e a acessibilidade do patrimônio documental para as gerações futuras.

Como evidenciado neste trabalho, o progresso da Internet tem provocado uma reconfiguração do cenário da interação social. Esta plataforma emergiu como uma força coesiva, conectando indivíduos em diversas partes do mundo e promovendo uma revolução de alcance societário. No entanto, essa metamorfose, que transcendeu as limitações geográficas na comunicação, não está isenta de momentos de alienação entre os usuários, representando um desafio a ser enfrentado.

O advento da cultura *hacker* e as dinâmicas da *Deep Web* também se destacam como elementos fundamentais nesse cenário. Enquanto alguns *hackers* podem direcionar suas habilidades para a inovação tecnológica e segurança cibernética, outros exploram a *Deep Web* para atividades ilícitas e violações de privacidade. Essa dualidade ressalta a necessidade de uma abordagem equilibrada na regulamentação e na compreensão desses fenômenos, considerando tanto os benefícios quanto os riscos potenciais que eles apresentam para a sociedade e a preservação digital.

Considerando essa evolução, surgiram novos desafios, notavelmente evidenciados no uso e acesso à *Deep Web*. Com seu anonimato e vasta quantidade de informações, a *Deep Web* apresenta uma realidade desafiadora para os órgãos encarregados de fiscalizar delitos *online*. As ferramentas proporcionadas pela *Deep Web* tornam-se facilitadoras para que infratores escapem, em grande parte, da responsabilização. Portanto, destaca-se a responsabilidade atribuída aos usuários da Internet em relação à navegação *online*. Eles são compelidos a observar rigorosamente as leis e a evitar participar de atividades ilícitas ou prejudiciais, dada a natureza do que pode ser encontrado na *Deep Web*. A prática de atividades destrutivas e ilícitas acarreta impactos prejudiciais à sociedade como um todo, minando a confiança no ambiente digital, comprometendo a privacidade e causando danos substanciais. Assim, uma abordagem equilibrada e responsável é essencial para aqueles que fazem uso da *Deep Web*, enfrentando, ao mesmo tempo, os desafios decorrentes de manifestações negativas nessa rede.

Nesse contexto, o princípio fundamental da Legalidade, que estipula que nenhum comportamento pode ser considerado crime sem uma lei preexistente que o defina como tal, e que não pode haver pena sem uma sanção legal previamente estabelecida, torna-se inegável. O Direito Penal assume uma jurisdição crucial no âmbito do ambiente digital para estabelecer certas condutas humanas como passíveis de sanção legal, identificando-as como ilícitas.

A regulamentação no cenário cibernético, portanto, é uma medida indispensável para promover o desenvolvimento civilizado e ordenado, permitindo a responsabilização penal e a imposição de limites às ações humanas e tecnológicas. O atual ordenamento jurídico brasileiro demonstra esforços no combate aos crimes digitais, como evidenciado por leis voltadas ao enfrentamento da pedofilia, divulgação de imagens íntimas, invasão de dispositivos eletrônicos, entre outros. Entretanto, esse combate concentra-se predominantemente na esfera da Internet comum, sendo de mais fácil controle pelos órgãos fiscalizadores. No entanto, quando se trata do ambiente da *Deep Web*, surge um desafio significativo. O anonimato, a dificuldade de rastreamento e a localização dos usuários nessa rede tornam o monitoramento e a fiscalização difíceis de serem realizados.

Cabe, portanto, ao usuário, em geral, ter consciência de que o uso de redes específicas da Internet, como a *Deep Web*, pode expô-lo a situações vulneráveis e a ações de criminosos digitais. Esses criminosos podem invadir seus dispositivos em busca de benefícios pessoais. Assim, embora a *Deep Web* apresente inúmeras qualidades e ferramentas benéficas, é fundamental utilizá-la com cuidado e responsabilidade.

## REFERÊNCIAS

ABBATE, Janet. **Inventing the Internet**. MIT Press, 2000.

ALVES, Mateus de Araújo. **Crimes Digitais: Análise da criminalidade digital sob a perspectiva do direito processual penal e do instituto da prova.** São Paulo - Editora Dialética, 2020.

BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e seus reflexos no direito brasileiro**. Editora Juspodivm, 2022.

BAUMAN, Zygmunt. **Globalização: as consequências humanas**. Rio de Janeiro: Zahar, 1999.

BERNERS-LEE, Tim. **Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor**. HarperOne, 1999.

CAIÇARA JUNIOR, Cícero; PARIS, Wanderson Stael. **Informática, internet e aplicativos**. Ibpex, 2007.

CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Zahar, 2003.

CASTELLS, Manuel. **A sociedade em rede**. 19. ed. São Paulo: Paz e Terra. 2018.

CASTELLS, Manuel. **O poder da comunicação**. 5. ed. Paz e Terra. 2016.

CIRIACO, Douglas. **Hackers do Anonymous desmascaram a maior rede de pedofilia da internet**. Tecmundo, 2011. Disponível em: http://www.tecmundo.com.br/ataque-hacker/14639-hackers-do-anonymous-desmascaram-a-maior-rede-de-pedofilia-da-internet.htm.

COOK, James. **Pedophiles Have Created A Deep Web Version Of Kickstarter To Crowdfund Child Porn**. Business Insider, Nova Iorque, 14, nov. 2014. Disponível em: http://www.businessinsider.com/pedophiles-have-created-a-deep-web-version-of-kickstarter-to-crowdfund-child-porn-2014-11.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.

CUNHA, Rogério Sanches. **Manual de direito penal: parte especial - volume único**. Salvador: Jus PODIVIM, 2023.

DEIBERT, Ronald J.; ROHOZINSKI, Rafael. **Liberation vs. Control: The Future of Cyberspace**. Journal of Democracy. 21(4), 43-57, 2010.

EDWARDS, Jim. **This is the Physics Student and Used Book Seller Who Allegedly Ran the 'Silk Road' Market for Drugs and Assassins**. Business Insider, Nova Iorque, 2, out. 2013. Disponível em: http://www.businessinsider.com/meet-ross-ulbricht-the-brilliant-alleged-mastermind-of-silk-road-2013-10.

FAVERO, Bruno de Oliveira; FAVERO, Altamiro de Oliveira. **Ciber Criminologia: os meios eletrônicos e o policiamento em ambientes digitais**. Jundiaí: Pago Editorial, 2021.

GRECO, Rogério. **Curso de Direito Penal: parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa**. - 14. ed. Niterói, RJ: Impetus, 2019.

HIMMA, Kenneth. **Hacker Ethics**. In The International Encyclopedia of Media Ethics, 2018.

KENNEY, ANNE R.; MCGOVERN, NANCY Y. **The Five Organizational Stages of Digital Preservation**. D-Lib Magazine, 9(5), 2003.

KOZAKIEWICZ, Dilmar José. Deep Web e segurança da informação: uma análise e seus impactos na sociedade e nas organizações. Curitiba, 2018. Disponível em: https://repositorio.utfpr.edu.br/jspui/bitstream/1/19991/1/CT_CEREC_I_2018_01.pdf

LARA, Marcelo D'Angelo. **Discussões sobre direito penal digital na contemporaneidade**. Ed. Dialética, 2021.

LEINER, Barry M.; CERF, Vinton G.; CLARK, David D.; KAHN, Robert E.; KLEINROCK, Leonard; LYNCH, Daniel C.; POSTEL, Jon; ROBERTS, Larry G.; WOLFF, Stephen. **A Brief History of the Internet**. ACM SIGCOMM Computer Communication Review, 39(5), 22-31, 2009.

LÉVY, Pierre. **As tecnologias da inteligência: o futuro do pensamento na era da informática**. São Paulo, Editora 34, 2010.

LEVY, Steven. **Hackers: Heroes of the Computer Revolution**. O'Reilly Media, 2010.

LUCAS, Edward. **Cyberphobia: Identity, Trust, Security and the Internet**. Bloomsbury, 2015.

MARQUES, Garcia; MARTINS, Lourenço. **Direito da Informática**. 2. ed. Almedina, 2006.

MOORE, Robert. **Cybercrime: Investigating High-Technology Computer Crime**. Routledge, 2005.

NETFLIX. **O Dilema das Redes**. [documentário]. Netflix, 2020. Disponível em: https://www.netflix.com/title/81254224

ORMSBY, Eileen. **The Darkest Web: Drugs, Death and Destroyed Lives . . . the Inside Story of the Internet's Evil Twin**. Allen & Unwin, 2019.

PAESANI, Liliana Minardi. **Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil**. 7. ed. Atlas, 10/2014. VitalSource Bookshelf Online.

PAULA, Angelita de. *et al*. **Manual de Direito na Era Digital: Penal e Internacional**. São Paulo. Editora Foco, 2023.

RONCADA, Rodiner. **A prova da materialidade delitiva nos crimes cibernéticos**. São Paulo: EMAG, 2017.

ROSA, Fabrízio. **Crimes de Informática**. Campinas: Bookseller, 2002.

SANTOS, Rafael Teixeira dos; VIDAL, Lívia Ferreira. **Deep Web:** Como acessar e porque não acessar? II Simpósio de pesquisa e de práticas pedagógicas, 2014.

SOUZA, Antonio Alberto Silva. *et al*. **Deep Web: A face oculta da internet, o que ela oferece de útil para a área acadêmica**. In: Encontro Regional de Computação e Sistemas de Informação, Maio. 2014. Manaus.

TAGIAROLI, Guilherme. **Propagandas 'perseguem' você na web? Saiba como esses anúncios funcionam**. UOL, São Paulo, 18, Julho. 2014. Disponível em: http://tecnologia.uol.com.br/noticias/redacao/2014/07/18/propagandas-perseguem-voce-na-web-saiba-como-esses-anuncios-funcionam.htm.

THOMPSON, Cadie. **Beyond Google: Everything you need to know about the hidden internet**. Business Insider, Nova Iorque, 16, Dezembro. 2015. Disponível em: http://www.businessinsider.com/difference-between-dark-web-and-deep-web-2015-11.