REDES
Revista Eletrônica Direito e Sociedade
Canoas, v. 8, n. 2, 2020
Direito em moviemnto em perspectiva
Recebido: 03.04.2020
Aprovado: 27.04.2020
Publicado: 01.07.2020
DOI http://dx.doi.org/10.18316/REDES.v8i2.6756

Deep Web e Dark Web: implicações sociais e repercussões jurídicas

Fernanda Viero da Silva

Universidade Regional do Noroeste do Estado do Rio Grande do Sul, Ijuí, Rio Grande do Sul, Brasil

https://orcid.org/0000-0002-3978-7395

Mateus de Oliveira Fornasier

Universidade Regional do Noroeste do Estado do Rio Grande do Sul, Ijuí, Rio Grande do Sul, Brasil

https://orcid.org/0000-0002-1617-4270

Norberto Milton Paiva Knebel

Universidade Regional do Noroeste do Estado do Rio Grande do Sul, Ijuí, Rio Grande do Sul, Brasil

https://orcid.org/0000-0003-0674-8872

Considerações iniciais

A Internet e o ciberespaço adornam quase todos os aspectos da vida atualmente, configurando-se um inédito grau de interconexão entre o mundo real e o mundo virtual. Pelo menos nas sociedades mais modernizadas é seguro afirmar que quase todos os aspectos da vida estão sendo digitalizados e processados por meio de algum sistema de computador, e essa revolução tem um aspecto dúbio: enquanto as pessoas agora podem interagir com um alto nível de facilidade (nunca visto antes), todos os dados sobre essas interações são constantemente registrados e armazenados[1].

A massiva camada populacional da contemporaneidade pensa que a Internet e a Web são termos sinônimos, quando de fato, são dois termos diferentes com elementos comuns (ou, o primeiro é gênero, enquanto o segundo, espécie ou âmbito). A Internet inclui várias redes e sua enorme infraestrutura, permitindo assim a conexão de milhões de computadores, sendo criada uma rede na qual qualquer computador pode se comunicar com os demais,

[1] BELLABY, Ross. Going dark: anonymising technology in cyberspace. **Ethics and Information Technology**, Delft, n. 20, p. 189-204, 2018.

desde que conectados à Internet; enquanto que a web é um meio que fornece acesso à informação[2]. Em outras palavras, enquanto a web é apenas um tipo (muito grande) de conteúdo, composto de sites acessíveis por meio de mecanismos de pesquisa como Google, Firefox etc., a Internet é a grande rede na qual vários âmbitos (inclusive a web, mas não apenas) estão, de alguma forma, disponíveis para acesso e comunicação dos usuários, por meio das mais variadas plataformas e aplicativos.

O problema que norteou esta pesquisa, diante do cenário exposto, pode assim ser descrito: quais os efeitos dessas redes de internet alternativas para a regulação e os direitos dos usuários da internet? Indica-se como hipótese a necessidade de regulação inovadora, frente à associação das tecnologias de rede com a lógica mercantil instaurada na *deep* ou *dark web* – sendo que atividades que afrontam a lei são dispostas de forma a serem livremente comercializadas. Essa especificidade aponta para a necessidade de conhecer essas redes em vista a não criminalizar a liberdade na internet e a defesa à privacidade, mas entender o caráter único dessas redes – um meio para exercício de atividades com fins lucrativos.

O objetivo geral deste trabalho é investigar as características da Deep Web e da Dark Web, compreendendo para além de aspectos conceituais de ambas nomenclaturas (que muitas vezes são confundidas como sinônimos), abordando-se como tais plataformas marcadas pelo expressivo anonimato operam na sociedade contemporânea pautada pela utilização massiva de tecnologias. A existência de mercados clandestinos expõe um perigo relativo ao direito absoluto à privacidade, enquanto a criminalização dessas condutas pode significar consequências significativas para privacidade de todos.

Para a consecução desse objetivo geral, três objetivos específicos foram elencados, cada qual correspondente a uma seção do artigo. Em um primeiro momento, busca-se esclarecer as diferenças entre Deep Web e Dark Web, bem como Internet e Web além de investigar questões pontuais ao longo da história. A segunda seção se destina a estudar de que formas a Dark Web proporciona a existência de mercados clandestinos com diversas destinações e toda uma lógica capitalista. Por fim, são apresentadas criticamente algumas estratégias estatais para o policiamento e investigação de tais plataformas, além de se debater como tais estratégias se relacionam ao direito à privacidade dos usuários.

A presente pesquisa tem natureza exploratória, sendo seu método de procedimento hipotético-dedutivo, sua abordagem qualitativa, e sua técnica de pesquisa bibliográfica-documental.

A Deep Web e a Dark Web na sociedade contemporânea

O termo Deep Web é usado para conceituar uma gama de conteúdos da Internet que, por razões técnicas, não é indexada pelos tradicionais mecanismos de pesquisa, e como qualquer forma de tecnologia, o anonimato trazido por si pode ser utilizado tanto para propósitos benéficos quanto perniciosos[3].

[2] SUSURI, Arsim; BESHIRI, Arbër. Dark Web and it's impact in online anonymity and privacy: a critical analysis and review. **Journal of Computer and Comunications**, Wuhan, n. 7, p. 30-34, 2019. p. 31.

[3] CHERTOFF, Michael; SIMON, Tobby. The impact of the Dark Web on internet governance and cyber security. **Global Comission on Internet Governance**, Waterloo, n. 6, 2015.

A Deep Web pode representar ameaças invisíveis, afinal as pessoas costumam usar as tecnologias digitais atualmente de forma integrada a sua rotina e, nesse contexto, seus dados passam a ser registrados pelas modalidades de pesquisa, tendo suas informações assim, vulneráveis. Tais apontamentos na verdade são a ponta de um iceberg, afinal uma plataforma de pesquisa tradicional obtém uma baixa porcentagem de informações[4]. Enquanto que grande parte do resto está imersa no que podemos entender como Deep Web, que consiste em dados que não podem ser localizados com uma simples pesquisa no Google.

A Internet e a Web são duas coisas separadas, mas se encontram relacionadas. A Internet é uma rede enorme de redes, que é capaz de conectar milhões de dispositivos que podem se comunicar, enquanto que a World Wide Web, ou simplesmente Web, é uma maneira de ter acesso a informações por meio da Internet[5]. Na atualidade, em que se consomem informações produzidas e comunicadas instantaneamente, há uma grande parcela que já ouviu falar da Dark Web, que é moldada popularmente como um covil de atividades misteriosas e ilícitas, que como a maioria dos estereótipos, para Chertoff[6] isso é um equívoco com alguma verdade por trás.

Para desmembrar a duvidosa Dark Web, é preciso primeiro entender do que se trata e como ela se difere do que a maioria dos usuários considera erroneamente a Internet. Na realidade, a internet compreende todos os servidores, computadores e outros dispositivos conectados juntos em uma rede de redes e pode ser dividida em dois elementos: o Surface Web e a Deep Web. Enquanto a Surface Web (ou seja, camada superficial da web) é o que normalmente se associa ao termo "Internet", se trata de um compilado de sites indexados por ferramentas de pesquisa (como Google, Yahoo e Bing), e que podem ser acessados por protocolos padrão, a Deep Web, por sua vez, se demonstra oculta aos usuários que se utilizam de ferramentas padrão, necessitando de outros meios mais específicos[7]. A superfície da Web, mais conhecida do usuário comum, é a parte dela que foi rastreada e indexada pelos mecanismos de pesquisa padrão, como o próprio Google ou Bing, via um navegador da Web comum. Em contrapartida, sendo utilizada a metáfora da superfície no que tange à conexão virtual/humano, devemos tão logo supormos que há uma escuridão abaixo, onde se encontra a Dark Web, também conhecida como Web Invisível ou Escondida (*hidden*)[8].

Estima-se atualmente que Deep Web responde por 90% do tráfego na Internet, o que pode ser visto de forma surpreendente para a maioria dos usuários que não percebem que estão acessando o Deep Web regularmente[9]. Os dados provenientes de mídias sociais como o Facebook ou o Twitter, por exemplo, podem ser classificados Deep Web, uma vez que só podem ser acessados por meio de interfaces de programas de aplicativos.

---

[4] CHERTOFF, Michael; SIMON, Tobby. The impact of the Dark Web on internet governance and cyber security. **Global Comission on Internet Governance**, Waterloo, n. 6, 2015. p. 01.

[5] CHERTOFF, Michael; SIMON, Tobby. The impact of the Dark Web on internet governance and cyber security. **Global Comission on Internet Governance**, Waterloo, n. 6, 2015. p. 01.

[6] CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017. p. 26.

[7] CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017. p. 26.

[8] SUI, Daniel; CAVERLEE, James; RUDESILL, Dakota. The Deep Web and the Darknet: a look inside the internet's massive black box. **SSRN Electronic Journal**, Amsterdã, n. 314, 2015. p. 06.

[9] CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017. p. 27.

Contudo, ao se tratar da Deep Web, normalmente termos como Dark Web aparecem em discussões, como se fosse uma diferente nomenclatura de tal fenômeno; neste sentido resta esclarecer que a Dark Web (de acordo com a comunidade cientifica), na verdade, é uma parte muito pequena e de difícil acesso da Deep Web, sendo estritamente responsável por menos de 0,01% dos sites na internet[10]. A única maneira de acessar a Dark Web é usando um navegador especial como The Onion Router (ou Tor), que não estranhamente necessita de uma senha. A Dark Web é um espaço marcado pelo anonimato, condição que pode facilitar a ação de grupos outsiders, desde dissidentes de regimes políticos até cibercriminosos. Nesse ponto se destaca a distinção entre *deep* e *dark web,* terminologicamente: a primeira é o conceito amplo, toda a rede alheia à *surface web*; já a *dark web* é uma especificidade, ou seja, uma parte específica da *deep web* com exigências específicas que devem ser atendidas pelo usuário, como a completa anonimidade e o acesso somente por endereços exclusivos inacessíveis pela internet comum – entre outros mecanismos extras de segurança[11].

Tal parcela da Web que não foi rastreada e indexada e assim está além do alcance do sonar dos mecanismos de pesquisa padrão. Atualmente é tecnicamente impossível estimar com precisão o tamanho da Deep Web, entretanto, sabe-se que que o Google (atualmente o maior mecanismo de pesquisa) até indexou apenas 4 a 16% da superfície da Web, enquanto que a Deep Web é aproximadamente 400-500 vezes mais ampla, afinal estima-se que os dados armazenados apenas nos 60 maiores sites Deep Web sejam 40 vezes maiores que o tamanho de toda a web superficial[12].

A Dark Web é uma questão antiga existe sob a superfície da Internet de acordo com muitos estudiosos e seu desenvolvimento da internet começou na década de 1960 como parte do esforço do Departamento de Defesa dos EUA para conectar seus sistemas de computadores em rede, mas a internet não se tornou um nome familiar até a década de 1990. A Dark Web em si permaneceu obscura para a maioria das pessoas, mas ganhou uma certa infâmia em 2013, quando Ross William Ulbricht (também conhecido como Dread Pirate Roberts), operador da Rota da Seda, foi preso[13]. A Rota da Seda era um mercado de bens e serviços ilegais acessados por meio do Tor.

Um sistema que concede o anonimato como o Tor é apenas uma ferramenta, e o que importa não é do que se trata tal tecnologia, mas sim, de como e para que é usada[14]. O acesso padrão de um usuário na Web gera um sinal de seu dispositivo pela Internet para o então servidor que abrange o material que deseja visualizar, seja ele qual for. Tal servidor lhe retorna tais dados para o seu dispositivo e assim se dá o relacionamento direto entre o usuário e a sua ferramenta de pesquisa/ navegador. Sua solicitação

[10] CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017. p. 27.

[11] CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017. p. 27.

[12] SUI, Daniel; CAVERLEE, James; RUDESILL, Dakota. The Deep Web and the Darknet: a look inside the internet's massive black box. **SSRN Electronic Journal**, Amsterdã, n. 314, 2015. p. 06.

[13] SUI, Daniel; CAVERLEE, James; RUDESILL, Dakota. The Deep Web and the Darknet: a look inside the internet's massive black box. **SSRN Electronic Journal**, Amsterdã, n. 314, 2015. p. 08.

[14] JARDINE, Eric. The Dark Web dilemma: tor, anonymity and online police. In: Global Commission on Internet Governance – Paper Series n. 21, 2015. p. 01.

de pesquisa é captada pelas redes da Internet para o local que contém as informações que você deseja visualizar e são devolvidas[15].

O Tor acessa informações na Web da mesma forma e assim, tal navegador opera como uma versão anônima de um jogo infantil em um telefone do qual o usuário envia sua solicitação para uma informação específica para um computador ou servidor em algum local na rede Tor. Este por sua retransmite essas informações para outro computador em outro lugar da rede e assim, mais uma vez, esse servidor simplesmente repassa sua solicitação para outra máquina. Essa terceira máquina solicita as informações que você deseja visualizar e as envia de volta por um caminho semelhante e desarticulado[16].

Diariamente os usuários deixam "pegadas" na internet (informações sobre horário, itinerário, tempo, etc., de seus acessos), e assim, tais dados pessoais denotam sua identidade digital, e assim, por consequência, sua representação no ciberespaço. O anonimato da Internet pode ser garantido quando os endereços de IP (Internet Protocol) não podem ser rastreados, despistando qualquer forma de localização virtual, e isso é que torna a Dark Web propicia para a ação de cibercriminosos[17]. A Dark Web oferece uma plataforma segura para os cibercriminosos patrocinarem uma grande quantidade de atividades ilegais, por exemplo, mercados anônimos por meios seguros de comunicação, sob uma infraestrutura não rastreável.

A Dark Web nesse contexto parece ser local propício para ação e desenvolvimento de terroristas, afinal suas ações implicam na necessidade da existência de uma rede anônima. Outro aspecto a ser considerado é que atualmente comprar informações de cartão de crédito roubadas nunca foi tão fácil, afinal já existem sites especializados que oferecem tais serviços, como o Atlantic Carding no qual quanto mais você paga, mais recebe[18]. Em meio a Dark Web não se pode deixar de destacar a presença da pedofilia e da pornografia infantil.

Entretanto, o que se pode extrair dos estudos de Gehl é que muito embora a Dark Web seja associada preponderantemente ao tráfico e a pornografia, esta oferece inúmeras possibilidades, com o seu anonimato, para jornalistas, ativistas e denunciantes que desejam falar livremente, apesar do monitoramento estatal da Internet[19]. Neste sentido, os agentes acima mencionados percebem que por meio de tais softwares de anonimato como o Tor, estes podem beneficiar a si mesmos ou qualquer outra pessoa, que queira dissociar sua fala da sua identidade – incluindo nesse diálogo dissidentes políticos.

---

[15] JARDINE, Eric. The Dark Web dilemma: tor, anonymity and online police. In: Global Commission on Internet Governance – Paper Series n. 21, 2015. p. 02.

[16] JARDINE, Eric. The Dark Web dilemma: tor, anonymity and online police. In: Global Commission on Internet Governance – Paper Series n. 21, 2015. p. 02.

[17] CHERTOFF, Michael; SIMON, Tobby. The impact of the Dark Web on internet governance and cyber security. **Global Comission on Internet Governance**, Waterloo, n. 6, 2015. p. 03.

[18] CHERTOFF, Michael; SIMON, Tobby. The impact of the Dark Web on internet governance and cyber security. **Global Comission on Internet Governance**, Waterloo, n. 6, 2015. p. 04.

[19] GEHL, Robert. Power/freedom on the dark web: a digital ethnography of the Dark Web social network. **New Media & Society**, Newbury Park, v. 18, p. 1219-1235, 2016. p. 1223.

A estrutura de fóruns na *Dark web* só permite o acesso há quem tenha habilidade técnica para encontrá-los, também, exige uma disposição de comunicação que respeite a privacidade a níveis profundos: conversas sobre questões como suicídios, golpes políticos e pedofilia não são tratadas como assuntos marginalizados, não pode haver retaliação. Todavia, esses sites não funcionam sem administração e é constante a exclusão seletiva de certos assuntos. Por isso que Gehl[20] considera esses fóruns experimentos fechados de poder e liberdade por meio do anonimato.

É importante esclarecer que, enquanto grandes partes da Dark Web são acessíveis apenas via Tor, o próprio navegador Tor pode realmente ser usado para outros fins benéficos, como simplesmente navegar no dia-a-dia de modo livre de restrições de conteúdo censurado e preocupação com a vigilância estatal ou corporativa[21]. Criminalizar o uso do *Tor* não faria sentido justamente porque é um aplicativo normal, que depende do comportamento do usuário, sendo possível usá-lo como qualquer outro navegador de grandes empresas, como o Google Chrome ou o Mozilla Firefox.

Assim, o resultado final deste sistema narrado é uma forma originária de usar a Internet anonimamente, com toda a imunidade que isso proporciona. Claramente esse anonimato abre a porta para abusos. A Dark Web diante do exposto se apresente como uma maneira viável para que agentes mal-intencionados troquem mercadorias ilegalmente, de maneira anônima e tem potencial para abrigar um número cada vez maior de atividades maliciosas. Pesquisadores acerca da temática de segurança e privacidade precisam permanecer vigilantes e encontrar novas formas de identificar os serviços maliciosos futuros (e que podem acarretar o surgimento de mercados específicos) para lidar com novos fenômenos o mais rápido possível[22].

A visão ideológica e capitalista a partir da Deep Web

A natureza atual da Web é dupla. Em primeiro lugar ela é composta por recursos de informação que são negligenciados nos resultados de mecanismos de pesquisa de uso geral; e o outro lado da natureza da Web é a "Dark Web", que aloca atividades ocultas atrás de portais anônimos[23]. Assim, tal plataforma é moldada e equipada pela tecnologia e igualmente pelo conhecimento limitado do público sobre o que é e como usá-la, sendo este seu combustível principal.

O mundo capitalista contribui para a criação de uma Web invisível, por meio de empresas que criam novos mecanismos de busca e assim tais formas de Webs resultam do que não é indexado por esses

[20] GEHL, Robert. Power/freedom on the dark web: a digital ethnography of the Dark Web social network. **New Media & Society**, Newbury Park, v. 18, p. 1219-1235, 2016. p. 1232.

[21] JARDINE, Eric. The Dark Web dilemma: tor, anonymity and online police. In: Global Commission on Internet Governance – Paper Series n. 21, 2015. p. 02.

[22] CHERTOFF, Michael; SIMON, Tobby. The impact of the Dark Web on internet governance and cyber security. **Global Comission on Internet Governance**, Waterloo, n. 6, 2015. p. 07.

[23] DEVINE, Jane; EGGER-SIDER, Francine; ROJAS, Alexandra. The evolving impact of the invisible web: exploring economic and political ramifications. **Journal of Web Librarianship**, Philadelphia, v. 9, n. 4, p. 145-161, 2015. p. 146.

mecanismos de pesquisa[24]. Tais empresas são responsáveis também pelo desenvolvimento de recursos internos que são protegidos por protocolos de não busca e firewalls de segurança.

Nas redes sociais atualmente, os elementos anônimos estão muito distantes do que agora reconheceríamos como mídia social convencional, que envolve identidades do mundo real cada vez mais vinculadas às preferências do consumidor e controle biopolítico. O cenário anônimo e virtual não tem fins lucrativos e não está interessado em reproduzir a partir de seus membros um novo nicho de público a ser vendido aos profissionais de marketing; além disso, por parecer ser virulentamente dedicado a proteger os membros contra a aplicação da lei e o poder do Estado[25].

As empresas responsáveis pelos mecanismos de pesquisa atendem às demandas governamentais no que tange a censura; logo como resultado, um aspecto político da Web invisível está emergindo, sendo moldado pelos governos de um lado, e por uma facção de pessoas que pretendem burlar os governos, por outro[26]. Plataformas de pesquisa como Google, Bing e Yahoo! possuem um papel primordial na captação de informações e dados de cidadãos de determinados países, mesmo em conformidade com a censura do governo. Logo, é na internet visível que os dados pesquisados são retidos, utilizados para fins de interesse das empresas que gerem essas plataformas de busca.

Com tais implicações, surge uma nova modalidade de mercado, voltado à Dark Web e seus softwares, que beneficiam a ação de hackers, que quando utilizadas, violam as leis de crimes de computador. Nos Estados Unidos por exemplo, há a incidência da Lei de Abuso e Fraude de Computadores (CFAA), que proíbe invasões, acesso não autorizado e danos a computadores no comércio interestadual ou internacional e também proíbe o tráfico de acesso não autorizado a computadores e espionagem de computadores[27].

Com a ascensão da internet, o processamento e rapidez das comunicações atingiram patamares históricos e com o fácil acesso à informação surgiram por consequência novas formas rápidas e eficientes do crime organizador operar. O tráfico de seres humanos, por exemplo, é uma atividade criminosa que é capaz de atravessar fronteiras e alcance legislativo; os responsáveis por tais ocorrências operam esse negócio visando ao lucro e se utilizam das mais recentes tecnologias disponíveis para esconder suas condutas criminosas, afinal o avanço da tecnologia proporciona lugares para os usuários se esconderem[28].

---

[24] DEVINE, Jane; EGGER-SIDER, Francine; ROJAS, Alexandra. The evolving impact of the invisible web: exploring economic and political ramifications. **Journal of Web Librarianship**, Philadelphia, v. 9, n. 4, p. 145-161, 2015. 147.

[25] GEHL, Robert. Power/freedom on the dark web: a digital ethnography of the Dark Web social network. **New Media & Society**, Newbury Park, v. 18, p. 1219-1235, 2016. p. 1232.

[26] DEVINE, Jane; EGGER-SIDER, Francine; ROJAS, Alexandra. The evolving impact of the invisible web: exploring economic and political ramifications. **Journal of Web Librarianship**, Philadelphia, v. 9, n. 4, p. 145-161, 2015. p. 150.

[27] SUI, Daniel; CAVERLEE, James; RUDESILL, Dakota. The Deep Web and the Darknet: a look inside the internet's massive black box. **SSRN Electronic Journal**, Amsterdã, n. 314, 2015. p. 11.

[28] RHODES, Leanne Maree. Human trafficking as cybercrime. **Agora International Journal of Administration Sciences**, Oradea, n. 1, p. 23-29, 2017. p. 23.

O SilkRoad foi o primeiro mercado de Dark Web predominante e que introduziu muitas práticas que são usadas até hoje em tais mercados; ideologicamente, ele foi moldado pelos fundamentos libertários do mercado: os dados de seus fundadores foram criados em um local de mercado para qualquer forma aceitável de comércio, aparentemente fora da área de abrangência do Estado. Tais mercados oferecem uma quantidade cada vez maior de reservas de bons serviços e serviços lucrativos, com destaque para medicamentos recreativos, como cocaína, cannabis e psicodélicos, mas também oferece uma ajuda a heroína, várias formas de novas substâncias bioativas, e informações digitais[29].

Quando se analisa a Dark Web, e portanto, os cibercrimes é necessário entender que o crime organizado em si é, pelo menos em parte, motivado por ganhos financeiros; entretanto gerar ganhos criminais também gera riscos, afinal os ganhos criminais, e especialmente os gastos desses ganhos, podem gerar suspeitas, o que por sua vez pode levar à prisão e confisco dos ativos, assim, lavagem de dinheiro, portanto, é uma necessidade básica para jogadores em mercados criminais cujos ganhos excedem as despesas diárias – a presença do crime organizado nessa rede pode ser definida por três fatores: a estimativa de riscos, os canais de destruição e os tipos de capital necessário para o sucesso econômico da atividade[30].

Enquanto o anonimato desempenha uma função relevante no que tange o desenvolvimento de novas ferramentas de comunicação e colaboração, as tecnologias de aprimoramento da privacidade também são apropriadas regularmente como suporte à atividade criminosa e assim, as apropriações ilícitas a partir do anonimato on-line desafiam a autoridade da aplicação da lei e reestruturam as relações de afinal a capacidade de ocultar a identidade que protege os usuários da acusação pode ser usada em vários níveis[31]. Dessa forma surgem mercados de criptomoedas que capitalizam estruturas voltada ao anonimato, lhe aprimorando; mercados ilegais que vendem drogas, armas e todo tipo de material ilícito também surgem na Dark Web com regularidade preocupante, a fim de mascarar a conduta do comércio criminoso[32].

A pornografia, por sua vez, é um exemplo de campo que muito embora já fosse consolidado no mundo do tráfico tomou proporções imensas com a ascensão da internet e da Deep Web, mais especificamente e dentre tais consequências está a preservação da identidade do consumidor, afinal, antes da atual tecnologia da informação e comunicação, era necessário encontrar um intermediário para o consumo de pornografia, gerando certo impedimento natural, atualmente, a pornografia está plenamente disponível online, portanto, não é acaso o acentuamento do uso dela na atualidade[33].

---

[29] DITTUS, Martin; WRIGHT, Joss; GRAHAM, Mark. Platform criminalism: the "last-mile" geography of the Dark Net market supply chain. In: WWW 2018: The 2018 Web Conference, ACM. Security and Privacy on the Web, p. 277-288. 2018. p. 278-279.

[30] WEBER, Julia; KRUISBERGEN, Edwin. Criminal markets: the dark web, money laundering and counter strategies **Trends in Organized Crime**, Berlim, p. 347-356, 2019. p. 347-349.

[31] SARDÁ, Thais; NATALE. Simone; SOTIRAKOPOULOS; Nikos; MONAGHAN, Mark. Understanding Online Anonymity. **Media, Culture & Society**, Newbury Park, v. 41, n. 4, 2019. p. 04.

[32] JARDINE, Eric. Privacy, censorship, data breaches and Internet freedom: the drivers of support and opposition to Dark Web Techonologies. **New Media & Society**, Newbury Park, v. 20, p. 2824-2843, 2018. p. 2825.

[33] RHODES, Leanne Maree. Human trafficking as cybercrime. **Agora International Journal of Administration Sciences**, Oradea, n. 1, p. 23-29, 2017. p. 24.

A facilidade do acesso à pornografia hoje também impulsionou um mercado virtual voltado a tal demanda, que clama adicionais por material; alguns dos quais se tornam cada vez mais hediondos por natureza, permitindo que indivíduos realizem fantasias em realidade virtual. A web combinada com fatores como esse fornece um ambiente lucrativo para os traficantes operarem seus negócios. A Fight the New Drug afirma que 25% de todas as solicitações de mecanismos de pesquisa são para material pornográfico[34].

O terrorismo e as organizações terroristas na Deep Web são preocupações constantes ao governo, uma vez que se trata de uma ameaça à segurança nacional. Extremistas, por exemplo, se beneficiam ao utilizarem a Dark Web ao recrutarem jovens vulneráveis para tais organizações. Simpatizantes ao terrorismo por sua vez, não possuem restrições na Dark Web ao se expressarem e atraem atenção de outros simpatizantes que apoiam a causa; grupos terroristas como o ISIS se utilizam da Dark Web par se comunicar entre si e organizar suas atividades, e ainda, se utilizam para prover informações e instruções pertinentes as suas pretensões[35].

A internet também está se tornando um local de escolha para os traficantes venderem os serviços que eles impõem às vítimas[36]. A publicidade on-line não é o único método usado pelos traficantes para vender seus produtos, mas é um componente essencial para muitos deles, garantindo que a listagem on-line ocorra no maior número possível de lugares. Alguns até obrigam suas vítimas a gastar tempo publicitando on-line com identidades fotográficas reais e diferentes, afinal fotos falsas são frequentemente usadas para ocultar a exploração por idade.

O mercado da Dark Web para além da comercialização da pornografia desenvolve o tráfico de drogas e medicamentos por exemplo; a utilização de um usuário em tal meio implica na identificação de dados em um dos maiores mercados do Tor ('Cryptomarket') que relaciona envolvidos na venda de medicamentos e tal rede permite recriar uma rede completa de transações para todos os opioides e fornecedores no mercado de criptografia[37].

Nessa mesma lógica, a internet também está sendo usada como uma ferramenta para auxiliar no recrutamento de vítima, e ainda, coletar informações delas e criar perfis falsos para criar relacionamentos virtuais, a fim de preparar futuras vítimas[38]. Assim, é perceptível que a Dark Web possibilita um tripé de atuações: (a) ser uma plataforma de tráfico; (b) plataforma de recrutamentos; e (c) uma plataforma de venda/lucro.

---

[34] RHODES, Leanne Maree. Human trafficking as cybercrime. **Agora International Journal of Administration Sciences**, Oradea, n. 1, p. 23-29, 2017. p. 24.

[35] LIGHTFOOT, Summer. Surveillance and privacy on the Deep Web. **Surveillance, Privacy and Rights**, Nova York, 2017. p. 12.

[36] RHODES, Leanne Maree. Human trafficking as cybercrime. **Agora International Journal of Administration Sciences**, Oradea, n. 1, p. 23-29, 2017. p. 24.

[37] DUXBURY, Scott W. HAYNIE, Dana. The networl structure of opioid distribution on a darknet cryptomarket. **Journal of Quantitative Criminology**, Berlim, v. 34, p. 921-941, 2017. p. 924.

[38] RHODES, Leanne Maree. Human trafficking as cybercrime. **Agora International Journal of Administration Sciences**, Oradea, n. 1, p. 23-29, 2017. p. 25.

Há de se ponderar, entretanto que o capital e as habilidades necessárias para operar em tais mercados de comercio on-line são muito diferentes daqueles necessários off-line, uma vez que o mercado on-line é mais competitivo que o mercado off-line, pois é preciso entregar um bom atendimento ao cliente, fotos de alta qualidade do produto e descrições precisas e ainda os clientes têm a oportunidade de comparar vários fornecedores e os serviços que oferecem[39]. O mercado de drogas da "*silk road*" foi capaz de difundir novas drogas e criar relações entre clientes e produtores, diminuindo o papel violento dos tradicionais intermediários de drogas (traficantes)[40].

Em contrapartida, a regulamentação internacional no que se refere a atividade cibernética ilícita se encontra ainda em um estágio inicial de desenvolvimento, afinal nenhum tratado ainda lida de maneira abrangente e eficaz com a insegurança gerada pela disponibilidade de ferramentas e ações de hackers que atuam na Darknet[41]. A mercantilização da *deep web* representa uma mudança de paradigma quanto ao estudo da criminalidade, os "criptomercados" não são um mero "Ebay para drogas ilícitas", mas representam uma transformação na cibercultura alinhada com a privacidade e a liberdade absoluta, criando um mercado descentralizado e volátil[42].

O crescimento dos criptomercados na "*dark web*" se fundamenta, também, na tomada de risco pelos vendedores de drogas, por exemplo, ao expandirem as suas operações ao nível internacional, compreendendo essa ferramenta como segura o suficiente para buscar clientes cada vez com mais recursos[43]. Portanto, esses mercados não são somente a expressão digital do tráfico de drogas, mas estão transformando profundamente esse negócio, no nível estrutural das práticas, as regulando internacionalmente[44].

O policiamento da Dark Web e as estratégias de controle por parte do Estado

Atualmente os governos se utilizam de táticas que eliminem as atividades criminosas da Dark Web e, ao mesmo tempo, protejam o anonimato de usuários inocentes, e talvez essa seja uma missão difícil. As táticas mais eficazes e razoáveis são aquelas que podem direcionar usuários anônimos específicos e responsabilizá-los por suas ações, em vez de desarmonizar vastas faixas de dados do usuário[45].

---

[39] WEBER, Julia; KRUISBERGEN, Edwin. Criminal markets: the dark web, money laundering and counter strategies **Trends in Organized Crime**, Berlim, p. 347-356, 2019. p. 347.

[40] ALDRIDGE, Judith; DÉCARY-HÉTU, David. Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. **International Journal of Drug Policy**, Amsterdã, v. 35, p. 7-15, 2016. p. 7.

[41] SUI, Daniel; CAVERLEE, James; RUDESILL, Dakota. The Deep Web and the Darknet: a look inside the internet's massive black box. **SSRN Electronic Journal**, Amsterdã, n. 314, 2015. p. 11.

[42] ALDRIDGE, Judith; DECARY-HETU, David. **Not an 'ebay for drugs':** the cryptomarket "silk road" as a paradigm shifting criminal innovation. 2014. p. 20.

[43] DÉCARY-HÉTU, David; PAQUET-CLOUSTON, Masarah; ALDRIDGE, Judith. Going international? Risk taking by cryptomarket drug vendors. **International Journal of Drug Policy**, Amsterdã, v. 35, p. 69-76, 2016.

[44] MARTIN, James. Lost on the silk road: online drug distribution and the 'cryptomarket'. **Criminology & Criminal Justice**, London, v. 14, n. 3, p. 351-367, 2014.

[45] CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017. p. 35.

Pode-se fazer uma distinção acerca de dois tipos de códigos pertinentes na presente pesquisa: (a) o legal; e (b) o tecnológico; no qual o código legal é o positivado, elaborado pelo Congresso e pelos governantes (a exemplo das leis e decretos) enquanto que o código tecnológico é o desenvolvido por programadores e possuí em si instruções contidas em softwares e hardwares que se incorporam às experiências de interação com o mundo virtual[46].

Neste âmbito é possível ponderarmos a importância de uma cooperação internacional que possa a vir ser aplicada à Dark Web e a outras atividades cibernéticas ilícitas, na proporção em que elas obstruam leis e acordos comerciais nacionais. A cooperação policial foi facilitada pela Convenção de Budapeste, que focou em crimes cibernéticos no ano de 2001 (também conhecida como Convenção do Conselho da Europa sobre Crimes Cibernéticos); o acordo gerado em tal ocasião buscou harmonizar as leis criminais e aprimorar a investigação e a cooperação entre as agências policiais (internacionalmente) em questões como segurança de redes de computadores, falsificação, fraude, pornografia infantil e violações de direitos autorais[47]. Vale destacar que no art. 6º da tal convenção ficou estabelecido que os Estados Partes devem criminalizar a venda, aquisição e distribuição de ferramentas de hacking.

É de grande importância observar que é de grande valia aplicar uma política unificada bem como recomendações padronizadas em escala internacional, uma vez que as atividades de criminosos cibernéticos que afetam a região da UE podem resultar de qualquer lugar do mundo, por exemplo[48]. Além disso, como foi descrito, a Dark Web fornece anonimato e, portanto, é altamente difícil identificar criminosos entre os usuários em geral.

A comunidade internacional tem levado a sério a colaboração e os diferentes padrões de privacidade, uma vez que em 2007, a OCDE adotou a Recomendação sobre Cooperação Transfronteiriça na Aplicação de Leis de Proteção da Privacidade para tratar da privacidade em escala global. Em resposta a isso, a Federal Trade Commission (FTC) dos EUA, juntamente com as autoridades de execução de todo o mundo, fundou a Rede Global de Reforço da Privacidade para promover o compartilhamento de informações, investigação e cooperação transfronteiriça[49].

Recentemente a INTERPOL e a Europol propuseram o estabelecimento de uma Força-Tarefa Conjunta de Cooperação e Compatibilidade com Crimes Cibernéticos para ajudar a harmonizar diferentes sistemas legais e criar um método eficiente para cooperação e tal façanha facilitou a cooperação internacional por meio uma espécie de "assistência jurídica mútua", em que um país pode solicitar ao governo de outro país que um juiz local emita um mandado para as informações em questão[50]. A Assistência Jurídica Mútua

[46] FERES, Marcos Vinício Chein. OLIVEIRA, Jordan Vinícius. Dos códigos legais aos códigos do ciberespaço: reflexões sobre direito e Deep Web. **PIDCC**, Aracaju, v. 11, n. 2, 2017. p. 235.

[47] SUI, Daniel; CAVERLEE, James; RUDESILL, Dakota. The Deep Web and the Darknet: a look inside the internet's massive black box. **SSRN Electronic Journal**, Amsterdã, n. 314, 2015. p. 11.

[48] KAVALLIEROS, Dimitrios; KOKKINIS, Georgios; CHALANOULI, Christina; PAPATHANASIOU, Anastasios. **Searching for crime on the web:** legal and ethical perspectives, 2018. p. 07.

[49] VOGT, Sophia Dastagir. The digital underworld: combating crime on the dark web in the modern era. **Santa Clara Journal of International Law**, Santa Clara, v. 15, n.1, p. 105-123, 2017. p. 121.

[50] VOGT, Sophia Dastagir. The digital underworld: combating crime on the dark web in the modern era. **Santa Clara Journal of International Law**, Santa Clara, v. 15, n.1, p. 105-123, 2017. p. 120.

pode ser considerada como uma solução para a obtenção de dados que não normalmente mantidos internacionalmente; é um acordo entre países para fornecer assistência um a um.

A coleta e a pesquisa focadas de dados, juntamente com o formulador de políticas e a educação pública, são pré-requisitos para uma revisão sistemática de qualidade e melhoria da estrutura reguladora existente nos níveis nacional e internacional. Os formuladores de políticas precisam entender melhor as condições que dão origem ao Dark Web e que são relevantes para a aplicação da lei, o design regulatório e a segurança nacional[51].

A cobertura popular da mídia no que tange a Dark Web é construída sobre uma noção de pânico moral, que está de certa forma associado à cultura da Internet nos últimos 35 anos ligada ao receio da invasão de hackers de computadores e ataques de telefone na década de 80. Nesse sentido há de se citar a Lei de Decência de Comunicações do Congresso dos EUA (1996) e a Lei de Exclusão de Predadores Online do Congresso dos EUA (2006), ambas inspiradas pelo pânico social sobre pedófilos (e o compartilhamento de pornografia por consequência) no Myspace – rede social preponderante na época[52]. A Dark Web atualmente está inspirando um pânico semelhante, voltado no medo das drogas, das armas, do comércio que surge de tais façanhas e assassinos de aluguel.

O FBI assim, desenvolveu a possibilidade de usar um verificador de endereços de protocolo de computador (CIPAV) para identificar suspeitos que suspeitem estar disfarçando sua localização usando serviços de anonimato e isso não compromete o anonimato dos usuários, mas ajuda a reduzir os parâmetros de pesquisa quando o FBI realiza uma investigação por exemplo[53].

A Agência de Projetos de Pesquisa Avançada em Defesa do Departamento de Defesa (DARPA) por sua vez está desenvolvendo uma ferramenta chamada Memex, que pode descobrir padrões para ajudar a aplicação da lei a combater atividades ilegais[54] e esse projeto especifico pode ser entendido como uma outra maneira pelas quais as agências de investigação podem entender o tráfego do Tor sem precisar desmascarar todos os usuários do desta[55].

---

[51] SUI, Daniel; CAVERLEE, James; RUDESILL, Dakota. The Deep Web and the Darknet: a look inside the internet's massive black box. **SSRN Electronic Journal**, Amsterdã, n. 314, 2015. p. 12.

[52] GEHL, Robert. Power/freedom on the dark web: a digital ethnography of the Dark Web social network. **New Media & Society**, Newbury Park, v. 18, p. 1219-1235, 2016. p. 1222.

[53] CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017. p. 35.

[54] CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017. p. 35.

[55] CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017. p. 35. Em fevereiro de 2015 o FBI usou uma ferramenta de hackers para identificar os endereços IP dos usuários que acessam um site oculto de abuso infantil Tor chamado Playpen (Cox 2016). Dentro de um mês após o lançamento em 2014, o Playpen tinha 60.000 contas de membros. Até 2015, havia 215.000 contas, 117.000 postagens e 11.000 visitantes únicos por semana (Cox 2016). Para derrubar o site, o FBI tomou a iniciativa sem precedentes de apreender o servidor Playpen e transferir o site para um servidor do FBI, sob um mandado emitido por um juiz federal no Distrito Leste da Virgínia (Satterfield 2016). O FBI executou o Playpen do servidor de 20 de fevereiro a 4 de março de 2015 e conseguiu acessar os computadores de cerca de 1000 usuários do Playpen durante esse período. Isso resultou em evidências suficientes para trazer cerca de 1500 casos contra pessoas acessando imagens de abuso infantil no Playpen.

A Dark Web é, por sua natureza, anônima e incapaz de discriminar criminosos e usuários comuns e as agências de execução devem resolver esse problema empregando táticas que mantêm a privacidade do usuário comum e desmascarando o criminoso. A maneira mais eficaz de fazer isso é procurar sites ilegais em vez de usuários ilegais[56].

Dotados de autoridade legal, hackers "do governo" podem colocar ferramentas nos computadores dos usuários que acessam o site, e se o governo apenas desligar o site, outro aparecerá em seu lugar. Mas há de se ponderar que os usuários de um site ilícito, os futuros usuários que estiverem pensando em acessar sites ilegais estarão mais hesitantes em fazê-lo por causa do risco de serem pegos. Assim a opção final seria que o governo tentasse quebrar o Tor, em outras palavras, para identificar todos os usuários do Tor, entretanto, isso também implica no desuso de uma ferramenta útil para usuários legítimos, como dissidentes[57].

A Agência de Projetos de Pesquisa Avançada em Defesa dos EUA (DARPA) desenvolveu um mecanismo de busca chamado Memex para ajudar o Departamento de Defesa a combater o tráfico de pessoas e potencialmente ajudar a descobrir outras atividades ilegais na Dark Web; resumindo, o Memex está indexando milhões de páginas da web que não podem ser acessadas por mecanismos de pesquisa tradicionais, incluindo milhares de sites apresentados em navegadores da Dark Web, como o TOR[58].

Enquanto o Memex não "desmascara" os endereços de IP ou identidades dos usuários, ele analisa o conteúdo para descobrir padrões; resta esclarecer que embora grande parte do conteúdo que o Memex seja destinado a indexar não seja acessível por meio de um mecanismo de busca comercial, as informações são, no entanto, ainda consideradas públicas[59]. Nesse sentido se instauram discursos acerca do Direito à privacidade dos usuários que se utilizam da Dark Web, e que tais mecanismos que fossem capazes de rastrear IP's apenas focassem em perfis com condutas maliciosas.

É de fato desafiador regular o espaço da Dark Web e respeitar o anonimato de usuários não criminosos simultaneamente, logo o governo deve entender essas questões coletivamente e definir uma agenda estratégica de segurança cibernética para atualizar e reforçar as regulamentações e políticas existentes[60]. Os avanços tecnológicos devem ser utilizados pelas autoridades para a identificação precoce de atividades de crimes cibernéticos e, ao mesmo tempo, respeitam os direitos fundamentais de todos os usuários.

Compreender as melhores técnicas de imposição é apenas o primeiro passo. Os Estados Unidos estão constitucionalmente comprometidos em proteger a liberdade de expressão na Internet de maneiras

---

[56] CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017. p. 36.

[57] CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017. p. 37.

[58] VOGT, Sophia Dastagir. The digital underworld: combating crime on the dark web in the modern era. **Santa Clara Journal of International Law**, Santa Clara, v. 15, n.1, p. 105-123, 2017. p. 114.

[59] VOGT, Sophia Dastagir. The digital underworld: combating crime on the dark web in the modern era. **Santa Clara Journal of International Law**, Santa Clara, v. 15, n.1, p. 105-123, 2017. p. 120.

[60] KAVALLIEROS, Dimitrios; KOKKINIS, Georgios; CHALANOULI, Christina; PAPATHANASIOU, Anastasios. **Searching for crime on the web:** legal and ethical perspectives, 2018. p. 07.

que muitos outros países não o são[61]. Alguns países desejam ter controle completo do tráfego na internet. Eles veem a liberdade de expressão como uma ameaça ao seu poder e a Dark Web como uma ferramenta que permite aos dissidentes falarem livremente[62].

Atualmente o caso de censura por parte do governo mais conhecido de é que ocorre na China. O Google.com antes mesmo do seu lançamento oficial em 2006 já era fortemente censurado e derrubado às vezes devido à pressão política em tal país, que atuava na versão Google.cn. O governo chinês detém uma longa lista de termos proibidos, como "Tiananmen", "4 de junho", "Tibet", "democracia", "democracia", "liberdade", "sexo", "Falun Gong" e assim por diante[63].

Em razão disso, em março de 2010, em vez de continuar autocensurando seus resultados, o Google decidiu fechar seu site em chinês (google.cn) e movê-lo para Hong Kong (google.com.hk) para fornecer resultados de pesquisa sem censura[64]. A realidade demonstra uma *deep web* ambígua, que ao mesmo tempo possibilita a denúncia de violências aos direitos humanos, pode promover crimes, é uma ambiguidade digna da privacidade plena do anonimato[65].

A internet é, por sua natureza, uma rede internacional de computadores, entretanto, a jurisdição aplicada a ela pode ser considerada nebulosa, então os governos devem encontrar maneiras de cooperar no estabelecimento de pelo menos alguns regulamentos mutuamente aceitáveis que governam a Dark Web. O debate em torno da Dark Web não terminou de maneira alguma, afinal o anonimato online é uma "faca de dois gumes que deve ser manuseada com cuidado, e à medida que os formuladores de políticas avançam, eles devem monitorar atentamente a evolução da Dark Web e garantir que a aplicação"[66].

Discussões sobre o uso da rede Tor e sobre criptografia em geral, são altamente polarizadas, afinal de um lado se afirma que a tecnologia precisa ser o mais próximo possível do "inquebrável" para que atores nefastos não possam obter acesso; enquanto que outro lado afirma que tecnologias criptografadas e anônimas, como o Tor, dificultam a aplicação da lei e do Direito em si[67]. A Dark Web mediante a todo

[61] VOGT, Sophia Dastagir. The digital underworld: combating crime on the dark web in the modern era. **Santa Clara Journal of International Law**, Santa Clara, v. 15, n.1, p. 105-123, 2017. p. 120. Uma grande tendência para obstáculos jurisdicionais que advêm do uso da Dark Web é a cooperação mais estreita com as agências estrangeiras de aplicação de convenções internacionais e leis domésticas. Alguns dos mais famosos casos de crimes cibernéticos ocorreram através da cooperação internacional, como a remoção de Shiny Flakes na Alemanha, e a Operação Onymous, nos quais a colaboração entre A Europol, o FBI e o Departamento de Segurança Interna dos EUA levaram à prisão de dezessete pessoas em vários países em conexão com vários grupos criminosos do mercado negro.

[62] CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017. p. 37.

[63] DEVINE, Jane; EGGER-SIDER, Francine; ROJAS, Alexandra. The evolving impact of the invisible web: exploring economic and political ramifications. **Journal of Web Librarianship**, Philadelphia, v. 9, n. 4, p. 145-161, 2015. p. 150.

[64] DEVINE, Jane; EGGER-SIDER, Francine; ROJAS, Alexandra. The evolving impact of the invisible web: exploring economic and political ramifications. **Journal of Web Librarianship**, Philadelphia, v. 9, n. 4, p. 145-161, 2015. p. 150.

[65] SILVA, Matheus Fernando de Arruda; MARTINS, Rui Decio. Reflexão sobre a relação entre a internet e o estado nas sociedades contemporâneas: a importância de uma regulamentação que compreenda a dinâmica do desenvolvimento tecnológico e valorize os direitos fundamentais. **Revista de Direito, Governança e Novas Tecnologias**, Brasília, v. 2, n. 1, p. 55-73, 2016. p. 68.

[66] CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017. p. 37.

[67] JARDINE, Eric. The Dark Web dilemma: tor, anonymity and online police. In: Global Commission on Internet Governance – Paper Series n. 21, 2015. p. 07.

exposto pode ser vista para muitos como o lado obscuro da Internet, por razões válidas, que incluem sua natureza anônima, mercados virtuais e moedas criptográficas. No entanto, a Dark Web é e sempre será uma ferramenta, e embora muitas atividades criminosas ocorram nessa rede, o Dark Web não é criminogênico, afinal muitas dessas atividades também podem existir fora dela[68].

Sob outra perspectiva, Jardine anota que o policiamento da Internet talvez não seja o ideal, mas sim, se as pessoas parassem de usar redes de anonimato, como Tor, para fazer coisas ilegais[69]. Isso permitiria que a rede fosse usada para contornar a censura e a vigilância em países repressivos, sem nenhuma das consequências lesivas que o anonimato on-line produz[70].

Naturalmente, não há como negar que a Dark Web apresenta um sério risco à segurança. Em razão às suas características únicas, como anonimato, mercados virtuais e uso de criptomoedas, uma série de atividades criminosas pode ser realizada nessa rede com facilidade; logo deve ser investigado mais seriamente[71]. O estudo de Décary-Hétu e Giommoni aponta para a ineficácia de operações polícias tradicionais em criptomercados de drogas, sendo até mesmo incapaz de causar aumento nos preços comercializados – apontando para uma já tradicional adaptabilidade do tráfico de drogas[72].

O anseio punitivista sugere que a obscuridade acerca da *dark web* deva ter como resposta a restrição da liberdade pelo Direito Penal e pela criminalização, independente da verdade, todavia, sugere-se o conhecimento dos complexos fenômenos ligados a essas redes, considerando a realidade off-line e online dos criptomercados ligados ao comércio de práticas ilícitas. A política criminal da Internet precisa estar atenta aos princípios constitucionais como o da presunção de inocência, que garante ao indivíduo, também, a tutela da privacidade[73], não podendo a justificativa do combate aos cibercrimes ser utilizada como pretexto de controle da liberdade nas redes[74].

---

[68] JUNG, Jeyong; MIREA, Mihnea; WANG, Victoria. The not so dark side of the darknet: a qualitative study. **Security Journal**, London, n. 32, p. 102-118, 2019. p. 114.

[69] JARDINE, Eric. The Dark Web dilemma: tor, anonymity and online police. In: Global Commission on Internet Governance – Paper Series n. 21, 2015.

[70] JARDINE, Eric. The Dark Web dilemma: tor, anonymity and online police. In: Global Commission on Internet Governance – Paper Series n. 21, 2015. p. 11. A rede é frágil, apesar de sua resiliência, e se tentarmos encontrar uma solução tecnológica rápida e fácil para problemas que são realmente sociais, corremos o risco real de quebrar a Internet. Em vez de descartar o Tor ou quebrar o anonimato e a criptografia do sistema pelas portas traseiras da aplicação da lei, o foco deveria estar no policiamento do que acontece na própria rede. O policiamento tem a vantagem de minimizar os custos que a Dark Web impõe à sociedade, enquanto permite que a Dark Web tenha o máximo potencial de efeito positivo globalmente. Não é perfeito, mas é o melhor que provavelmente podemos fazer.

[71] JUNG, Jeyong; MIREA, Mihnea; WANG, Victoria. The not so dark side of the darknet: a qualitative study. **Security Journal**, London, n. 32, p. 102-118, 2019. p. 114.

[72] DÉCARY-HÉTU, David; PAQUET-CLOUSTON, Masarah; ALDRIDGE, Judith. Going international? Risk taking by cryptomarket drug vendors. **International Journal of Drug Policy**, Amsterdã, v. 35, p. 69-76, 2016.

[73] PINTO, Felipe Martins; GUIMARÃES, Johnny Wilson Batista. O Direito à Privacidade e o sigilo de dados na internet. **Revista da Faculdade de Direito da UFMG**, Belo Horizonte, n. 69, p. 201-220, 2016.

[74] FERREIRA, Márcio Ricardo; BERARDI, Regina Celli Marchesini. Sociedade virtual do risco vs. filosofia libertária criptoanarquista: livre manifestação do pensamento, anonimato e privacidade ou regulação, segurança e monitoramento da rede. In: CONPEDI (Org.). **Direito, governança e novas tecnologias**. Florianópolis: Conpedi, 2016.

A política criminal precisa compreender que não há objetivo inerente nas tecnologias de rede - frequentemente associado a práticas criminosas - , mesmo nas redes alternativas como a *deep web*, o rótulo de ambiente criminógeno é injustificado e a criminalização precipitada dos seus usuários é um erro, tendo em vista que os ideias de privacidade dessas redes pode muito bem servir a fins diversos - como a resistência à violação dos dados pessoais. Essa é uma visão sociológica da infraestruturas das redes: De fato, é uma plataforma tecnológica usada por diferentes indivíduos para uma variedade de propósitos[75]. Logo a Dark Web pode ser observada sob o seguinte prisma: que nada mais é do que um espelho da sociedade: distorcida, ampliada e mutada pelas condições estranhas e não naturais da vida on-line[76].

Considerações finais

Estudar a temática da Deep Web e por consequência da Dark Web é sempre desafiador, afinal se trata de um espaço virtual marcado pelo anonimato – que por si só é alarmante na sociedade. Mesmo em meio a tudo que se afirma ainda há muito a se descobrir, pois o que se sabe é ainda pouco comparado ao vasto universo que a Deep Web de fato é.

Logo, preliminarmente se pode concluir que o presente artigo não visa exaurir a temática, e que tal problemática ainda deve ser investigada e debatida profundamente visto que em a atual sociedade, marcada pela forte presença das tecnologias digitais, a internet como um todo é um assunto de grande relevância no cotidiano dos usuários bem como as repercussões advindas desta.

Conclui-se que o anonimato oferecido pela Dark Web (uma parcela da Deep Web, portanto) desencadeia inúmeras possibilidades e dentre elas o desenvolvimento de marcados ilegais e clandestinos que operam por meio de cibercriminosos. A mídia exerce um papel importante na divulgação de dados, mas também é responsável por gerar um temor público que associa a Deep Web automaticamente a prática de crimes "nas escuras" e de fato um mercado negro. Portanto, a caracterização de um ideológico mercado de capitalismo libertário, os criptomercados, surgem como a verdadeira ameaça, não essas redes como tecnologia.

Não há como se negar que a Dark Web, mais especificadamente, gera riscos à sociedade pela forma com a qual opera, e que nela há uma forte comercialização do tráfico de drogas, pessoas, pornografia e até mesmo opera como um meio de reunir simpatizantes por exemplo, do terrorismo. Não há como se negar, portanto, os riscos advindos de tais práticas a sociedade e à eficácia da ideia de legislação estatal e a defesa aos Direitos Humanos. Entretanto, é possível concluir também, que o anonimato para além dos crimes cibernéticos opera como uma máscara para seus usuários, que por sua vez se sentem confortáveis em defenderem causas próprias e assuntos políticos, por exemplo, quando não são identificados; o anonimato gera encorajamento.

[75] JUNG, Jeyong; MIREA, Mihnea; WANG, Victoria. The not so dark side of the darknet: a qualitative study. **Security Journal**, London, n. 32, p. 102-118, 2019. p. 114.

[76] SUI, Daniel; CAVERLEE, James; RUDESILL, Dakota. The Deep Web and the Darknet: a look inside the internet's massive black box. **SSRN Electronic Journal**, Amsterdã, n. 314, 2015. p. 12.

Conclui-se que deve haver investigações mais apuradas e precisas no meio, e que a existência de convenções e acordos internacionais que visem legislar tais práticas e amparar possíveis riscos. Rejeitam-se políticas criminais punitivistas acerca da *deep* ou *dark* web, pois a literatura indica que esses termos são utilizados como forma de mascarar um controle sobre a liberdade dos usuários, é preciso compreender formas inovadoras de reprimir o verdadeiro problema, que não é a forma tecnológica das redes: os criptomercados de atos ilícitos, que possuem frentes online e off-line.

Referências

ALDRIDGE, Judith; DÉCARY-HÉTU, David. Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. **International Journal of Drug Policy**, Amsterdã, v. 35, p. 7-15, 2016.

ALDRIDGE, Judith; DECARY-HETU, David. **Not an 'Ebay for Drugs':** The Cryptomarket "Silk Road" as a Paradigm Shifting Criminal Innovation. 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436643. Acesso em: 1 mar 2020.

BELLABY, Ross. Going dark: anonymising technology in cyberspace. **Ethics and Information Technology**, Delft, n. 20, p. 189-204, 2018.

CHERTOFF, Michael; SIMON, Tobby. The impact of the Dark Web on internet governance and cyber security. **Global Comission on Internet Governance**, Waterloo, n. 6, 2015.

CHERTOFF, Michael. A public policy perspective of the Dark Web. **Journal of Cyber Policy**, London, v. 2, n. 1, p. 26-38, 2017.

DÉCARY-HÉTU, David; PAQUET-CLOUSTON, Masarah; ALDRIDGE, Judith. Going international? Risk taking by cryptomarket drug vendors. **International Journal of Drug Policy**, Amsterdã, v. 35, p. 69-76, 2016.

DEVINE, Jane; EGGER-SIDER, Francine; ROJAS, Alexandra. The evolving impact of the invisible web: exploring economic and political ramifications. **Journal of Web Librarianship**, Philadelphia, v. 9, n. 4, p. 145-161, 2015.

DITTUS, Martin; WRIGHT, Joss; GRAHAM, Mark. Platform criminalism: the "last-mile" geography of the Dark Net market supply chain. In: WWW 2018: The 2018 Web Conference, ACM. Security and Privacy on the Web, p. 277-288. 2018.

DUXBURY, Scott W. HAYNIE, Dana. The networl structure of opioid distribution on a darknet cryptomarket. **Journal of Quantitative Criminology**, Berlim, v. 34, p. 921-941, 2017.

FERES, Marcos Vinício Chein. OLIVEIRA, Jordan Vinícius. Dos códigos legais aos códigos do ciberespaço: reflexões sobre direito e Deep Web. **PIDCC**, Aracaju, v. 11, n. 2, 2017.

FERREIRA, Márcio Ricardo; BERARDI, Regina Celli Marchesini. Sociedade virtual do risco vs. filosofia libertária criptoanarquista: livre manifestação do pensamento, anonimato e privacidade ou regulação, segurança e monitoramento da rede. In: CONPEDI (Org.). **Direito, governança e novas tecnologias**. Florianópolis: Conpedi, 2016.

GEHL, Robert. Power/freedom on the dark web: a digital ethnography of the Dark Web social network. **New Media & Society**, Newbury Park, v. 18, p. 1219-1235, 2016.

JARDINE, Eric. Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web Techonologies. **New Media & Society**, Newbury Park, v. 20, p. 2824-2843, 2018.

JARDINE, Eric. The Dark Web dilemma: tor, anonymity and online police. In: Global Commission on Internet Governance – Paper Series n° 21, 2015. Disponível em: https://www.cigionline.org/sites/default/files/no.21.pdf. Acesso em: 1º mar 2020.

JUNG, Jeyong; MIREA, Mihnea; WANG, Victoria. The not so dark side of the darknet: a qualitative study. **Security Journal**, London, n. 32, p. 102-118, 2019.

KAVALLIEROS, Dimitrios; KOKKINIS, Georgios; CHALANOULI, Christina; PAPATHANASIOU, Anastasios. **Searching for crime on the web:** legal and ethical perspectives, 2018.

LIGHTFOOT, Summer. Surveillance and privacy on the Deep Web. **Surveillance, privacy and rights**, Nova York, 2017.

MARTIN, James. Lost on the silk road: online drug distribution and the 'cryptomarket'. **Criminology & Criminal Justice**, London, v. 14, n. 3, p. 351-367, 2014.

PINTO, Felipe Martins; GUIMARÃES, Johnny Wilson Batista. O Direito à Privacidade e o sigilo de dados na internet. **Revista da Faculdade de Direito da UFMG**, Belo Horizonte, n. 69, p. 201-220, 2016.

RHODES, Leanne Maree. Human trafficking as cybercrime. **Agora International Journal of Administration Sciences**, Oradea, n. 1, p. 23-29, 2017.

SARDÁ, Thais; NATALE. Simone; SOTIRAKOPOULOS; Nikos; MONAGHAN, Mark. Understanding Online Anonymity. **Media, Culture & Society**, Newbury Park, v. 41, n. 4, 2019.

SILVA, Matheus Fernando de Arruda; MARTINS, Rui Decio. Reflexão sobre a relação entre a internet e o estado nas sociedades contemporâneas: a importância de uma regulamentação que compreenda a dinâmica do desenvolvimento tecnológico e valorize os direitos fundamentais. **Revista de Direito, Governança e Novas Tecnologias**, Brasília, v. 2, n. 1, p. 55-73, 2016.

SUI, Daniel; CAVERLEE, James; RUDESILL, Dakota. The Deep Web and the Darknet: a look inside the internet's massive black box. **SSRN Electronic Journal**, Amsterdã, n. 314, 2015.

SUSURI, Arsim; BESHIRI, Arbër. Dark Web and it's impact in online anonymity and privacy: a critical analysis and review. **Journal of Computer and Comunications**, Wuhan, n. 7, p. 30-34, 2019.

VOGT, Sophia Dastagir. The digital underworld: compating crime on the dark web in the modern era. **Santa Clara Journal of International Law**, Santa Clara, v. 15, n.1, p. 105-123, 2017.

WEBER, Julia; KRUISBERGEN, Edwin. Criminal markets: the dark web, money laundering and counter strategies **Trends in Organized Crime**, Berlim, p. 347-356, 2019.