Boletim do Instituto de Saúde
Volume 21, Número 1, Julho 2020, Páginas 9-16.

Ensaio

Profilaxia para a Internet aberta e a Dark Web

Prophylaxis for open Internet and Dark Web

Rodrigo Filev Maia,[1] *Adriana Shimabukuro*[2]

Assita ao vídeo produzido pelos autores:

***Link* de acesso ao vídeo: https://youtu.be/gEsEOMqiEYs**

Resumo

A Internet aberta, amplamente conhecida e utilizada, é considerada um terreno onde há livre circulação de ideias, sem direcionamento de conteúdos, tendo como antagonista a *Dark Web*, ambiente criptografado e hostil, origem de crime e de conteúdos maliciosos de toda ordem, com destaque para conteúdos perigosos à saúde física e mental. Neste ensaio, é discutido o que é a *Dark Web*, bem como quais são de fato seus conteúdos e suas tecnologias básicas. Da mesma forma, é abordado o que é a Internet aberta, explicitando-se que essa está muito longe de ser o território da liberdade e livre expressão, pois pode sim controlar o que é oferecido para o Internauta. Tal controle pode ser feito em parte por causa da tecnologia fundamental da rede, assim como, pelo comportamento das pessoas e pela organização do conteúdo, que segue uma estrutura matemática, chamada de redes complexas. Essas estruturas podem ser utilizadas para se criar bolhas de opiniões ou situações que podem ser utilizadas para infindáveis propósitos. Por fim, pontua-se que a educação e o conhecimento dos fatos sobre ambas as redes são elementos profiláticos para utilizá-las de forma mais segura e saudável.

Palavras-chave: Internet; redes de comunicação; análise de sistemas; *Dark Web*.

Abstract

The open Internet is broadly known and accessed by the general population. It is considered an open and free world that promotes the circulation of free ideas, where any content could be spread and accessed without any sort of *manipulation*. The Dark Web is considered to be the opposite. It is a network in which cryptography creates a hostile world, full of criminal activities and all sorts of malicious contents, including several dangerous for mental and physical health and wellbeing. This work seeks to present what the Dark Web is, what are its contents and basic technologies to access it. The open Internet is also discussed by the same approach in order to emphasize that it is not an open and free world of ideas and speeches since content can be segmented according to the sort of criteria. Such control is performed from the basic internet technology up to the way that people behavior and content organization is done because, both follow a mathematical model called complex network. Such structure may be used to organize content and opinion bubbles. The education and knowledge about both networks are a prophylactic method to protect ourselves and make us use the Internet in a safe and healthy way.

Keywords: Internet; communication network; system analysis; Dark Web.

[1] *Senior Researcher*, Centro de Estudos Sociedade e Tecnologia - CEST - USP, São Paulo, SP, Brasil (r.filevmaia@deakin.edu.au). POBOX 192, Hanwood, NSW, Australia, 2680.

[2] *CyberSecurity Expert, Ministério Público Federal, São Paulo, SP, Brasil (adrianashimabukuro@mpf.mp.br).*

Introdução

Internet é controle! Uma afirmação verdadeira e proferida por um dos criadores da Internet, Robert Kan, em uma conversa muito animada sobre a Internet e o seu futuro. Embora a Internet pareça um território livre, onde muitos podem divulgar o que bem entender e qualquer conteúdo pode ser visto por outros tantos, há muitos que têm sua liberdade cerceada por governos ou grupos que detêm poder político ou econômico. Isso pode ser feito porque a *Internet* é realmente controle. Controle porque para um conteúdo ser acessado, tem que ser endereçado de alguma forma e esse endereço deve garantir acesso a todos. A consequência da tecnologia fundamental da Internet é que qualquer comunicação passa por um mecanismo de controle único, o que torna possível monitorar qualquer fluxo de dados na Internet, ou seja, qualquer comunicação, mesmo que isso seja uma tarefa árdua.[1]

Contudo, é possível se comunicar de forma sigilosa através de técnicas que utilizam esse mesmo mecanismo de controle para trocar dados. Um conjunto dessas técnicas forma o que é conhecido como *Dark Web*, que na verdade são grupos de pessoas que possuem um programa de computador especial e um segredo (como uma senha) que lhes garante a comunicação apenas entre aqueles que compartilham o mesmo programa e o mesmo segredo.[2]

É praticamente impossível dizer quantas redes compõem a *Dark Web*, por isso evitamos afirmar que ela possui "camadas" e sim diversas tecnologias diferentes que são utilizadas para diversos tipos de atividades, sejam estas lícitas ou ilícitas. Podemos citar algumas redes utilizadas atualmente como a *TOR*, *Freenet*, *I2P*, *ZeroNet*, *Hyperboria*, *Galet*, *Onion*, *StealthNet*, *Globaleaks*, *Perfect Dark*, *Alienet*, *Twister*, *Morphis*, *Infinit*, *Maelstrom*, *Resilio*, *Ricochet*, *Retroshare*, dentre inúmeras outras.

Beckstrom e Lund[3] detalham um pouco sobre três destas redes anônimas: a rede TOR, a rede FREENET e a rede I2P. A TOR ou "The Onion Router" é a mais usada, por isso, equivocadamente, considerada como "a" *Dark Web*. A rede Freenet, igualmente anônima, tem peculiaridades, como o armazenamento ponto a ponto que pode manter os dados indefinidamente e independentemente do dono do conteúdo, ao contrário da TOR que fica a cargo da manutenção (ou destruição) dos dados pelo dono do conteúdo. Ainda podemos mencionar a I2P que traz características das duas redes anteriores, anonimidade e dados descentralizados, mas combina a velocidade de uma rede menor e mais eficiente. Em diversos locais, pode-se ler que a *Dark Web* permite a qualquer um se comunicar de forma livre e anônima, irrastreável. Isso não é verdade. Para permitirem que você encontre um conteúdo, essas tecnologias têm como efeito colateral a possibilidade de rastreamento, novamente não trivial, por aqueles que pertencem a essa rede, ou a esse nível.

No livro *Inside the Dark Web*, Ozkaya e Islam[4] listam as técnicas mais utilizadas para tentar identificar usuários criminosos da *Dark Web*. Entre elas, explicam o uso do Netflow, Weblog, Apache Hadoop, MapReduce e até o uso da Inteligência Artificial, através do Processamento Natural de Linguagem (NLP), que auxilia na análise do conteúdo dos *sites*. Na *Dark Web*, existem muitos tipos de conteúdos e, notadamente, há muito material tétrico. Conteúdos de pornografia infantil são trocados por pessoas que se utilizam da maior dificuldade de rastreamento para não serem identificadas. Há diversos *sites* de compra e venda de cartões de crédito roubados, drogas, cenas mórbidas de diversas ordens com a participação de animais e pessoas em situações degradantes. As autoridades sabem e trabalham para mitigar e prender indivíduos que produzem, compartilham e acessam tais materiais. Há

fartos materiais sobre indivíduos presos que operam na *Dark Web* em publicações como *The Guardian* e BBC. A Polícia Federal Brasileira, entre os anos de 2014 e 2016, desenvolveu uma tecnologia nacional e inédita, lançando a chamada Operação Darknet[5] que prendeu mais de 100 pedófilos e resgatou seis crianças em cativeiro de abuso sexual. Esses criminosos e vítimas estavam protegidos por um suposto anonimato, vendido pelas técnicas da *Dark Web*. A cada inovação ou nova camada de segurança desenvolvida para anonimizar predadores, novas pesquisas e técnicas são criadas pelas polícias mundiais para manter um mínimo de segurança aos usuários do que deveria ser uma "Internet Sem Fronteiras".

O terrorismo também se desenvolve na *Dark Web*, grupos convocam pessoas para sua causa, arrecadam recursos via *dark coins*, ensinam a construir artefatos, como armas e bombas. Há estudos acadêmicos que apresentam e discutem essas questões, mas Becsktrom e Lund[3] mostram que esses mesmos terroristas utilizaram tanto a *Dark Web* quanto a Internet mapeada (essa que todos usamos) para recrutar membros em vários momentos da história. O Estado Islâmico (ISIL/ISIS) é um dos mais famosos exemplos. Conteúdos falsos também podem ser criados e propagados tanto na *Dark Web* quanto na Internet que conhecemos, e pode ser difícil discernir o que é fato e o que é falso. Esse tipo de conteúdo pode criar uma emergência de saúde pública, além daquelas já vividas?

Desenvolvimento

O Lado positivo da *Dark Web*

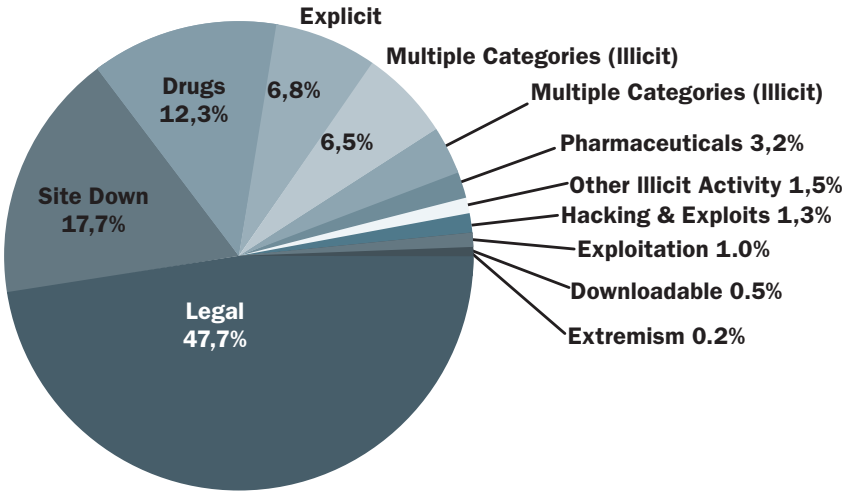
Nem tudo é como parece. Nem sempre o anonimato significa criminalidade. Nem tudo na na *Dark Web* é ilegal e pernicioso; se a pornografia é proeminente nas redes, não significa que toda pornografia é ilícita. As fraudes se instalam preferencialmente na Internet aberta, pois precisam de vítimas que são minoria neste ambiente criptografado. Extremismos e extremistas se encontram na *Dark Web*, na Internet aberta e na vida dos mundos físico e virtual.

A *Dark Web* ajuda as pessoas a manter a privacidade e expressar livremente seus pontos de vista. A privacidade é essencial para muitas pessoas inocentes aterrorizadas por perseguidores e outros criminosos. A crescente tendência dos empregadores em potencial de rastrear postagens nas mídias sociais também pode dificultar o envolvimento público em discussões honestas. Por fim, a popularidade da *Dark Web* com os criminosos torna a maneira perfeita de os policiais disfarçados se comunicarem e entenderem a mente do criminoso, seu modo de pensar e agir.

A figura 1 ilustra os tipos de conteúdos que podem ser encontrados na *Dark Web*. Para questões de saúde pública, dois conteúdos são destacados: drogas (12,3%) e fármacos (3,2%). Em ambos os casos, as pessoas podem comprar materiais e mesmo encontrar fórmulas de preparo de substâncias que podem causar severos prejuízos à saúde. Mas não é só na *Dark Web* que tais materiais podem ser encontrados, pois há na Internet aberta formas de uso de materiais ainda não clinicamente testados e que podem causar severos problemas de saúde.[6]

Como na *Dark Web* realmente há total privacidade para troca de conteúdo e informações, grupos como o Wikileaks e o Anonymous se utilizam desta tecnologia para publicar e proteger documentos sigilosos. Revolucionários que participaram da Primavera Árabe também a usaram para facilitar a articulação dos rebeldes e despistar a inteligência policial. É nesse ambiente digital também que muitos jornalistas, militares e políticos se comunicam e acobertam suas ações, tornando-o um local seguro para troca de informações valiosas e, às vezes, controversas.

Figura 1 - Conteúdos presentes na *Dark Web*.



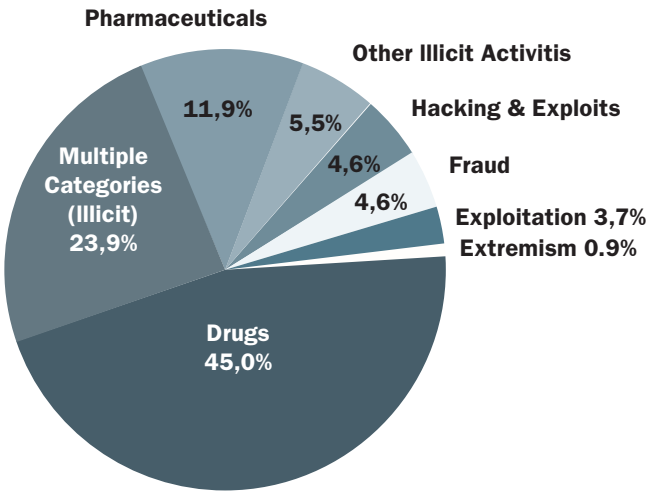
Fonte: Terbium Labs.[7]

Mas, ao mesmo tempo em que a *Dark Web* fortalece pessoas comuns, algumas pessoas abusam inevitavelmente desse poder. A *Dark Web* pode facilitar a prática crimes, por exemplo, a combinação da *Dark Web* e das criptomoedas facilitam muito a contratação de alguém para cometer um assassinato, para violar a privacidade de outros através do vazamento de fotos particulares, registros médicos e informações financeiras. A tecnologia utilizada na *Dark Web* é um vetor dessas aberrações humanas ou seria uma tecnologia que permite uma catarse da loucura da humanidade?

A figura 2 explicita o volume de dados sobre drogas e fármacos, considerando apenas o conteúdo considerado ilícito na *Dark Web*. Mas engana-se quem supõe que lá é o único foco na venda destes produtos. O Núcleo Técnico de Combate aos Crimes Cibernéticos do Ministério Público Federal de São Paulo recebe diariamente denúncias de *sites* que vendem medicamentos controlados ou proibidos. Muitos desses *sites* estão na Internet aberta.

Sob certo ponto de vista, tais conteúdos podem se tornar uma questão de saúde pública. Os conteúdos divulgados nesses círculos podem

Figura 2 - Conteúdos ilícitos identificados na *Dark Web*.



Fonte: Terbium Labs.[7]

induzir pessoas a cometerem ofensas contra os valores da civilização, contra instituições? Um indivíduo que encontra vídeos e conteúdos suicidas pode ser induzido a seguir os passos dos protagonistas? Conteúdos extremistas podem mobilizar pessoas de poucos valores e convicções a aderir a tais movimentos? O que acontece com uma pessoa exposta por muito tempo a conteúdos desse tipo? Poderia acontecer algo similar ao protagonista de Laranja Mecânica?[8]

Em um seminário realizado em São Paulo em 2008, Gilles Michel Ouimet, psicólogo clínico, explicou sobre os perigos dos grupos e fóruns que serviam para racionalizar e encorajar atos criminosos. Pedófilos propensos a abusar de crianças, encontravam apoio e simpatia ao abordar suas parafilias sexuais nestes ambientes anônimos da *Dark Web*. O comportamento disseminado em um grupo pode ser tomado como verdadeiro por seus membros, independentemente dos fatos.

As bolhas e os filtros invisíveis

A Internet, dentro das suas nuances, deveria permitir o maior acesso às mais diversas informações, o estreitamento das relações interpessoais e liberdade de expressão sem amarras de governos e de corporações.

Parisier[9] discute que a personalização de uma Internet moldada por corporações, como Google, Facebook e Amazon, tem deixado os usuários presos em uma bolha invisível. Essa bolha possui uma estrutura conhecida e matematicamente definida, chamada de redes complexas.[10], Se essas redes complexas moldam a forma de como encontramos as informações, ou estas nos são apresentadas, cabe a questão: "como lidar com uma população que passa a ver somente aquilo que estas empresas selecionam? Não seria o conceito de rede anônima uma possibilidade de retirar usuários de dentro de suas bolhas?"

As redes sociais são hoje uma das formas preferenciais de comunicação entre as pessoas, e reproduzem o comportamento de guetos amplamente conhecidos e presentes na sociedade há gerações. Há infindáveis exemplos de guetos, sejam por raça, cultura ou valores. Da mesma forma, na Internet, também há a formação de guetos que em geral se iniciam com a rede de contatos do indivíduo e que, em muitos aspectos, são os mesmos de seu convívio social. Mas rapidamente alguém dessa rede de contatos acrescenta mais alguém ou um novo conteúdo de um outro grupo que possuem um membro em comum e a rede cresce, mas não indefinidamente. Via de regra as suas redes sociais são apenas dos amigos ou das pessoas próximas, quem não tem o grupo da família, ou dos colegas de trabalho? Esses grupos têm uma formação e relações tais que subitamente os conteúdos recebidos pelo seu grupo são oriundos de pessoas que você não conhece e que chegam até você através de um amigo do seu amigo. O conteúdo é crível? Muitos acreditam que sim, pois o conteúdo é oriundo de uma pessoa de minha confiança. Guetos do mundo físico e do mundo virtual também são modelados como redes complexas.

Esse fenômeno das redes complexas é bastante conhecido e é estudado desde os anos de 1967, quando o assunto ficou conhecido como os "seis graus de separação" ou "small world problem".[11] Milgram[11] discute que, se você quiser falar com o presidente, você conseguiria, desde que falasse com uma pessoa de seu círculo de relacionamento e, a partir dela, iniciasse uma cadeia de comunicação que passasse por até seis pessoas, até chegar à pessoa de interesse. Isso acontece porque provavelmente você tem um amigo que conhece alguém que trabalha no governo local, que conhece alguém que trabalha no governo federal, que trabalha com um assessor do ministro que fala com o presidente. Outro estudo que costumo chamar do teorema da festa foi proposto por Granovetter[12] e modela como um grupo de amigos se aproxima de um grupo de amigas: em geral há

uma ligação entre os grupos, pois há um rapaz que conhece uma das moças, seja porque são vizinhos, estudaram juntos ou porque já a viu em algum local que ambos frequentam. Exceção feita aos super extrovertidos, também contemplados no experimento.

As redes complexas e a propagação das idéias

A forma como se propagam as informações também segue um conjunto de regras estudadas por Milgram,[11] Granovetter[12] e outros, com modelos abrangidos pelas redes complexas. Para uma informação se tornar muito conhecida, deve fazer parte de um nó de alto grau.[13,14] Como a teoria descreve muito bem os comportamentos esperados, pode-se, portanto, estimar como uma determinada mensagem irá se propagar. Empresas como Cambridge Analytica e outras se utilizam desse tipo de conhecimento para influenciar as redes sociais e interferir até mesmo em processos eleitorais e criar pós-verdades.[15]

Com a polarização de nossa época, em que as verdades são absolutas e a opinião contrária é simplesmente errada, algumas mensagens têm uma grande chance de se propagarem em uma determinada rede de pessoas, e podem até mesmo chegar a muitas redes ou grupos de pessoas. Uns acreditarão piamente na mensagem, afinal vai ao encontro de suas verdades e crenças. Já a outra parte considerará a mensagem imprópria, errada e, portanto, deve ser ignorada ou "cancelada", mas ainda assim compartilhada, mesmo que com críticas.

Neste momento, o mundo atravessa um momento histórico, uma pandemia que desafia a forma de organização social e coloca em xeque valores e crenças. O país mais rico do mundo teme, a olhos vistos, uma batalha de desinformação via redes sociais que influencia a mídia e que traça contornos das atividades e atitudes do mundo físico. O mesmo acontece no Brasil.

Pode-se dizer que uma bolha é formada pelos nós que circundam um nó de maior grau. Esse nó pode ser chamado de influenciador. Um influenciador pode ser criado em uma rede. Uma das formas é fazer o grau de um determinado nó aumentar, por exemplo, através do uso de robôs, que são programas que se conectam ou fazem referência ao nó que se quer reforçar. Com isso, aquele nó tem maior chance de se conectar a outros, os quais serão alcançados por esse novo influenciador. Uma vez que se inicia o envio de mensagens e essas são replicadas por robôs e atingem muitas pessoas, tem-se a formação de uma bolha de influência. Logo, a Internet aberta pode prender as pessoas em bolhas que podem ser criadas e manipuladas e, segundo uma personagem muito lembrada recentemente apregoou: uma ideia dita mil vezes se torna uma verdade. O princípio dos robôs segue essa máxima.

As redes complexas modelam as conexões na *Dark Web* e na Internet aberta, nas redes sociais e no mundo físico. Retomando as origens dos fundamentos das redes anônimas, o professor do Departamento de Informática e do Programa de Pós-Graduação em Informática da UFES Magnos Martinello explica que "a motivação dos criadores vem da filosofia de que cada pessoa tem o direito de se expressar livremente sem revelar sua identidade".[16] O uso do anonimato tem como essência ser uma rede de comunicação que criptografa informações, a fim de tornar o rastreio algo complexo. Esse princípio é usado também por grupos sociais que são perseguidos em contexto político, como aponta a pesquisadora em Comunicação no contexto da cibercultura e mestranda do Programa de Pós-Graduação em Comunicação e Territorialidades (PósCom-Ufes) Leilane Cruz. Ela salienta que "as redes anônimas são uma resistência a este ecossistema, é um dos caminhos possíveis para fatias da sociedade que mantém uma voz de protesto para conseguirem burlar a criminalização".[16] Ainda com anonimato, a estrutura das redes complexas se faz presente.

Considerações finais

Pessoas podem ser influenciadas por valores, ideias e discursos presentes nos níveis da *Dark Web*, e podem ser tão danosos quanto epidemias. Contudo, não encontraremos vacina para dirimir os males, não há antivirais. Mas há profilaxia.

A tecnologia permitiu a criação destes locais na Internet e há uma mística de mistério nesse assunto, o que talvez seja bastante convidativo para certas parcelas da população. A tecnologia também pode combater a *Dark Web*, mas não com proibição de acesso ou difamação da mesma, mas oferecendo educação. Da mesma forma que apresentar para jovens o que é sexo, sexualidade, doenças venéreas, pode auxiliar na prevenção de males e situações indesejadas mesmo para aquele que decidem explorar o assunto; o mesmo pode ser feito com a *Dark Web*. Que se apresente para todos de forma muito clara, objetiva e sem preconceitos o que é o que se pode encontrar por lá, assim como conversar sobre os males e como se prevenir. Educação ainda é uma ferramenta poderosa para emancipação do ser humano, para a conservação dos valores criados pela civilização e para a evolução contínua de nossa espécie. Tratar a *Dark Web* com preconceito e valores extremados, independentes de direção e sentido, só trará radicalismo e ignorância.

Algo similar ocorre nas redes sociais e na Internet aberta. As redes sociais estão no centro do debate de como podem influenciar decisões, votações e crenças de toda ordem. As discussões estão sendo veiculadas na grande mídia. As estruturas de como as informações são organizadas e propagadas são bastante estudadas, mas quase não são conhecidas do grande público. Educação auxiliará em como as pessoas podem se proteger e ser resilientes às potenciais confusões e influências difundidas na Internet aberta.

Um aviso importante sobre a *Dark Web*: alguém que se aventurar a navegar por esses níveis deve tomar os devidos cuidados com segurança e proteção, pois caso contrário você poderá ser rastreado e monitorado após se desconectar. Isso é mais claro na Internet aberta e redes sociais devido aos anúncios direcionados aos seus interesses, mesmo que você não os informe diretamente. E por quem você seria monitorado em ambos os casos? Internet é controle!

Declaração de conflito de interesses

Os autores declaram não haver conflitos de interesse, em relação ao presente estudo.

Referências

01. Comer D. Mansfield-Devine S. Tor under attack. Computer Fraud & Security [internet]. [acesso 10 abr 2020]. Disponível: https://www.sciencedirect.com/science/article/abs/pii/S136137231470523.
02. Mansfield-Devine, S. Tor under attack. Computer Fraud & Security [internet]. [acesso 20 jul 2020]. Disponível: https://www.sciencedirect.com/science/article/abs/pii/S1361372314705238.
03. Beckstrom M, Lund B. Casting light on the *Dark Web*: A guide for safe exploration. New York: Rowman & Littlefield Publishers; 2019.
04. Ozkaya E, Islam R. Inside the *Dark Web*. Boca Raton: CRC Press; 2019.
05. Brasil. Ministério Público Federal.Operação Darket-Balanço [internet]. Porto Alegre: 2020 [acesso 20 jul 2020]. Disponível: http://www.pf.gov.br/agencia/noticias/2014/10/operacao-darknet-balanco
06. Vanhee C, Francotte A, Janvier S, Deconinck E. The occurrence of putative cognitive enhancing research peptides in seized pharmaceutical preparations: An incentive for controlling agencies to prepare for future encounters of the kind. Drug Testing and Analysis [internet]. [acesso 10 abr 2020]. Disponível: https://pubmed.ncbi.nlm.nih.gov/31667971/.
07. Terbium Labs, Gollnick C, Wilson E. Separating fact from fiction: The truth about the *Dark Web* [internet]. [acesso 10 abr 2020]. Disponível: https://dsimg.ubm-us.net/envelope/385643/510233/The%20Truth%20About%20The%20Dark%20Web.pdf.
08. Burgess A. A Clockwork Orange: Restored Edition. London: Penguin Books; 2013.

09. Pariser Eli. O filtro invisível: o que a internet está escondendo de você. Rio de. Janeiro: Zahar; 2012.
10. Barabási AL. Linked: The new science of networks. Manchester: Perseus Books Group; 2003.
11. Milgram S. The small world problem. Psychology today. 1967;2(1):60-7.
12. Granovetter M. The strength of weak ties: A network theory revisited. Sociological theory. [internet]. 1983;1:201-233. [acesso 10 abr 2020]. Disponível:ttps://www.jstor.org/stable/202051.
13. Albert R., Barabási, A.L. Statistical mechanics of complex networks. Review of Modern Physics [internet].2001; 74(1). [acesso 10 abr 2020]. Disponível: https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.74.47.
14. Barabási AL, Bonabeau E.Internetworking with TCP/IP Vol. I: Principles, Protocols, and Architecture. New York: Prentice Hall; 1995.
15. Santaella L. A pós-verdade é verdadeira ou falsa? Barueri: Estação das Letras e Cores, 2019.
16. Marriel G, Cássia J. A Deep Web e os limites do anonimato. Universo Ufes. [internet] 2019; 21 maio [acesso 30 mar 2020]. Disponível em: https://universo.ufes.br/.t/10.1103/RevModPhys.74.47.
14. Barabási AL, Bonabeau E.Internetworking with TCP/IP Vol. I: Principles, Protocols, and Architecture. New York: Prentice Hall; 1995.
15. Santaella L. A pós-verdade é verdadeira ou falsa? Barueri: Estação das Letras e Cores, 2019.
16. Marriel G, Cássia J. A Deep Web e os limites do anonimato. Universo Ufes. [internet] 2019; 21 maio [acesso 30 mar 2020]. Disponível em: https://universo.ufes.br/