LATURA ÎNTUNECATĂ A INTERNETULUI

THE DARK SIDE OF INTERNET

COLȚENIUC Anatolie,
magistru în drept, Facultatea de Drept, USM

Summary

The Internet is supposed to be one of the most discussed topic in recent years, especially, the interest is concentrated on the dark side of the Internet (DarkWeb). However, from a legal point of view, we cannot identify sufficient studies and research that would clarify the legal status of this issue, but also the legal limits of the possible activities in the dark web. We can say that DarkWeb is a space for cybercriminals and black markets, arguing that the emphasis is on its anonymity. This is also a reason why it has remained undirected by the state. Governments must emphasize the institutionalization of the possibility of the anonymous use of the Internet, ensuring the rights and freedoms of all web users regardless of the virtual area where it is located, SurfaceWeb, DarkWeb.

Keywords: *DarkWeb, internet, policies, competence, TOR, SurfaceWeb, DeepWeb, silk road.*

În ultima perioadă de timp, internetul se impune a fi subiect destul de abordat, mai ales datorită părții sale întunecate, și anume așa numitului Dark web. Din perspectivă legală, însă, nu putem identifica suficiente studii care ar clarifica statutul juridic a acestei realități, dar și limitele legale a activităților posibile a fi realizate în spațiul virtual întunecat.

Drept urmare, prin prezentul articol, propunem o prezentare a fenomenului de Dark web și analiza eventualelor riscuri, provocări dar și reglementări care ar trebui să apară,

Abordarea părții întunecate a internetului nu poate fi realizată în afara înțelegerii aspectelor tehnice.Astfel, din perspectivă structurală spațiul virtual este determinat de existența a 3 dimensiuni și anume **SurfaceWeb**, **DeepWeb** și **DarkWeb**. Pentru a prezenta mai ușor conținutul tridimensional al spațiului virtual, de obicei se utilizează interpretarea acestuia prin utilizarea analogiei cu structura ghețarului, avînd în vedere conținuturile prezentate în imaginea din

Fig. 1[1].

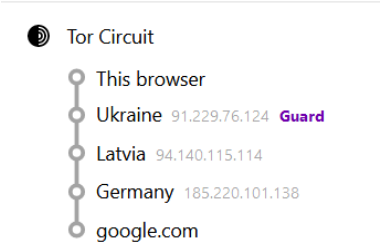


(Fig. 1. Reprezentarea Internetului sub forma unui ghețar)

Surface Web (internetul de suprafață) reprezintă totalitatea informației postate în internet, accesibilă spre vizualizare și accesare utilizatorilor obișnuiți. La aceaste categorii de informații atribuim inclusiv informația indexată de Google, YouTube, Yahoo etc. Utilizatorii acestor categorii de informații nu au nevoie de competențe speciale de utilizare sau acces rețelistic special dezvoltat. Spațiul virtual de tip DeepWeb, mai numit și „internetul profund" conține informații care pot fi accesate doar în baza unei utilizări anonime, bazate pe utilizarea seviciilor de accesare de către autorul informației distribuite, fie prin acordarea de acces pe adresa IP sau prin restricționarea accesului la informație doar prin accesarea link-ului direct sau logarea pe platformă. În aceast nivel se includ diferite lucrări științifice, cărți, monografii, iar ce ține de site-urile web, aici se includ fișierele ce oferă accesul la panoul administratorului, datele de logare, internetbanking, forumuri private. Ca exemplu ce este cunoscut de fiecare dintre noi, putem lua Netflix, practic cel mai mare portal de filme. Desigur, este foarte ușor de găsit folosind un search pe Google, dar această acțiune ne oferă acces doar la pagina de start. În acest context putem spune că tot ce se află dincolo de pagina de start, este în nivelul „DeepWeb", deoarece acces veți avea doar dacă contul îndeplinește unele cerințe dictate însăși de Netflix. Un alt exemplu ar fi GoogleDrive sau DropBox, din moment ce urci un document pe această platformă, nimeni nu va avea acces la acel document până nu veți seta personal accesul. În comparație cu SurfaceWeb, resursele din DeepWeb nu vor fi niciodată afișate în motoarele de căutare și la liber acces, în așa mod lucrează conținutul la care se oferă acces în schimbul unui abonament. Referitor la estimarea dimensiunii Deep Web, putem

spune că mereu a fost o provocare, însă cercetătorii afirmă că Deep Web ar fi de câteva mii ori mai mare decât Surface Web. Majoritatea utilizatorilor accesează Deep Web, chiar și fără să își da seama de acest lucru, motivul fiind faptul neinformării despre această secțiune. Al treilea nivel este DarkWeb mai numit și „internetul întunecat", desigur acest nivel fiind o subcategorie a DeepWeb-ului ce este reprezentat de un procent foarte mic, conform datelor oferite de CIGI[2]. Matt Beckstrom, specialist digital al Bibliotecii Lewis și Clark din Helena, Montana, a comparat internetul cu un Iceberg (*foto n1.*): „*Web-ul întunecat ar trebui să fie numit, mai degrabă, web-ul ascuns. Termenul de întunecat îți dă impresia că e rău sau greșit*"[1, p.55]. Suntem de acord cu ideea lui Beckstrom, conform căreia este important ca lumea să știe că au loc activități ilegale pe paginile care alcătuiesc Dark Web-ul, însă trebuie să ținem cont și de faptul că sistemele acestui nivel nu au fost concepute pentru activitățile ilegale ce au loc la momentul dat. Singura modalitate de a putea accesa această porțiune a internetului este utilizarea unui browser conceput însăși pentru aceasta: The Onion Router, prescurtat TOR[3], un exemplu de acest site ar fi: *http://silkroad7rn2puhj.onion;* „*union*" fiind domenul specific acestui nivel. Am putea spune că DarkWeb este un spațiu pentru criminali cibernetici și piețe negre, argumentând prin faptul că se pune accent pe anonimat. Acesta fiind și un motiv de ce a rămas un nivel nedirijat de către stat. Astfel pentru o monitorizare a acestei părți a internetului, este necesară e studiere mai aprofundată. DarkWeb este foarte des confundat cu DeepWeb, din acest motiv trebuie să ținem cont de unele condiții ce sunt necesare de a fi îndeplinite: este de tip TOR, în același timp să nu fie accesibil pentru SurfaceWeb. Pe de altă parte site-ul trebuie să solicite utilizatorului existența adresei unice TOR. Unele site-uri, pentru o securitate mai bună, pot cere utilizatorilor să introducă și o anumită parolă, setată de către administratorii site-ului în cauză. DarkWeb a fost mult timp lăsat în umbră, obținând un interes sporit în anul 2013 când Ross William Ulbricht, mai numit și Dread Pirate Roberts, administrator al Drumului Mătăsii, a fost arestat[4]. Drumul Mătăsii fiind o piață centralizată a serviciilor și obiectelor ilegale ce putea fi accesată doar prin TOR.

Inițial TOR nu a fost conceput pentru scopuri meschine. Fiind dezvoltat de NRL (Naval Research Laboratory) cu scopul de a oferi anonimat personalului militar american, angajați în operațiuni internaționale. Acest sistem complică determinarea adresei IP a solicitantului inițial. În anul 2003, NRL a oferit acest browser open-source gratuit, ceea ce reprezintă că traficul angajaților militari, era mixat cu traficul mulțimii de utilizatori civili. Mecanismul acestui browser este destul de simplu. Circuitul funcționează prin tirmiterea unei cereri prin cel puțin 3 calculatoare aleatoriu.



(Fig.2. Exemplu de circuit TOR)

Aceste calculatoare sunt numite relee. Însăși numele de TOR, provin de la faptul că fiecare calculator adaugă un strat de protecție la semnalul ce doar el îl poate decripta. La sfârșit, cererea părăsește circuitul printr-un calculator numit „releu de ieșire", care se autointitulează ca fiind locația din care ar fi inițiatorul, fiind foarte dificil de depistat, din motiv că releele de ieșire fac cereri în numele a sute de utilizatori diferiți, fiind ajutat și de un sistem de randomizare[5]. Trebuie să indicăm și faptul că TOR, nu a fost singurul factor care a dus la dezvoltarea nivelului DarkWeb. Ultimul fiind susținut de două resurse puternice și anume: HWiki și Bitcoin. Aceste două servicii au s-au impus drept modalități comode de lucru pe spațiul întunecat al internetului. Până a-și face apariția HWiki, site-urile din nivelul DarkWeb erau practic imposibil de găsit, astfel HWiki a adus în 2004 un prim val de utilizatori a acestui nivel. O altă modalitate de accesare a site-urile din DarkWeb, este derminată de utilizarea motoarelor specifice TOR, spre exemplu Ahmia, care indexează site-urile ascunse și Grams – motor de căutare a site-urilor ce reprezintă piețe de droguri și arme[6]. Evident caracteristic oricăror piețe este faptul că este necesar o modalitate de achitare. Astfel, a apărut întrebarea: Dacă totuși DarkWeb este un spațiu anonim, atunci este necesară o monedă care nu va putea fi urmărită, astfel a crescut interesul pentru Bitcoin. Cu timpul Bitcoin a devenit o monedă standard a DarkWeb-ului, fiind o monedă stocată în portofele digitale criptate. Moneda dată a fost concepută pentru a eradica procesul de urmărire a traseului invers, adică de a depista persoana care a efectuat achitarea/transferul. Fiecare tranzacție este înregistrată într-un jurnal public, dar specific monedei date este faptul că se înregistrează doar ID-ul portofelului nu și datele despre cumpărător/vânzător. Obținerea Bitcoin se poate realiza prin două modalități: prima este de a se conecta la un serciviu de schimb bitcoin, iar a doua constă în punerea la dispoziția unei persoane terțe a capacității calculatorului/serverului pentru a rezolva diferite sarcini (termen tehnic utilizat "minare") personale, de exemplu oferirea de la distanță a capacității

grafice a unui calculator unei alte persoane. Un moment important este faptul că nu toți utilizatorii TOR, accesează neapărat site-urile interzise, astfel adesea sunt persoane care doresc din principiu a păstra statutul de anonim navigând chiar și pe Surface Web. Desigur că nu putem nega faptul că sunt utilizatori care folosesc DarkWeb-ul în scopurile ilegale sau amorale.., dar totuși putem menționa și situațiile în care DarkWeb-ul poate fi utilizat și în scopuri nobile, de exemplu, asigurarea dreptului informațional prin accesarea cărților electronice, sau deconspirarea informațională. Jurnaliștii folosesc unele site-uri special create pentru a le permite să se exprime liber sau ca să își expună părerea/analiza asupra unor fenomene discutabile, fără a sta cu frica că poate fi demascat. DarkWeb-ul conține site-uri care au un strat sporit de confidențialitate care permit expedierea de fotografii specifice, având siguranța că nu vor fi difuzate public. Un rol aparte îl are anonimatul și în cazul activiștilor pentru drepturile omului care se află în regimurile opresive. Conform studiului realizat de către Dr. Gareth Owen și Nick Savage, cercetători de la Universitatea din Portsmouth, timp de 6 luni, au explorat utilizarea serviciilor TOR, ajungând la concluzia că mai mult de 80% din solicitările TOR, au fost redirecționate către site-uri cu conținut referitor la abuz asupra copiilor. Cercetătorii au recunoscut faptul că este posibil o eroare în datele finale, deoarece serviciile speciale ale statelor folosesc calculatoare care vor accesa automat aceste site-uri având ca scop colectarea de date. Chiar și în această situație, fiind și 50% trafic din partea utilizatorilor, cifra dată este foarte mare. Un alt studiu efectuat de către Fundația caritabilă „Internet Watch", a demonstrat că aproximativ 32.000 site-uri ce conțin imagini de abuz asupra copiilor, dintre care doar 51 site-uri erau din nivelul DarkWeb, desigur trebuie să ținem cont și de faptul că metodele de depistare a site-urilor din DarkWeb, sunt diverse și niciodată nu putem garanta că sunt depistate integral. Al doilea subiect, foarte activ pe DarkWeb, este traficul de droguri și arme având ca fundament arestarea administratorului pieței Silk Road[1], ce a dus la descentralizarea furnizorilor de droguri și/sau arme, formând astfel o mulțime de alte piețe mai mici, având o diferență prin faptul că aceste piețe, ulterior formate, vând absolut tot ce le oferă furnizorii. Aceste exemple ne arată foarte clar că comerțul în DarkWeb, avansează în ritm rapid.

Având la bază tentații destul de atractive și relație atât de bine formată dintre cerere și ofertă, este evident că pericolul acestor piețe nu va dispărea de la

[1] Silk Road a fost creată în 2011 de Ross William Ulbricht, se estimează că ultimul ar fi obținut peste 13 milioane dolari doar din comisioane, permițând furnizorilor să folosească platforma sa. La momentul închiderii de către FBI, a fost depistat faptul că au avut loc vânzări în sumă de peste 1,2 miliarde dolari, cu implicarea a 150 000 clienți și 4000 de furnizori. DPR fiind condamnat la închisoare pe viață.

sine, astfel statul trebuie să se implice în elaborarea unor politici orientate spre înlăturarea amenințărilor internetului întunecat, dar și după caz să creeze cadru pentru dezvoltarea potențialului. Având în vedere cele expuse supra, politicile legale propuse ar trebui să încadreze juridic inclusiv posibilitatea utilizării anonimatului. O legislație „rapidă", în cele mai multe cazuri nu este o legislație eficientă, astfel trebuie să se țină cont și de faptul de a nu aduce atingeri drepturilor persoanelor care utilizează TOR în scopuri legale, de exemplu navigarea simplă pe internet (Google Search, rețele de socializare etc). În această ordine de idei, în acțiunile guvernelor, ar trebui să găsim răspuns la cele mai importante întrebări, și anume: „*Cum trebuie să se implice guvernele în combaterea acestui fenomen nedirijat*" și „*Ce acțiuni trebuie de întreprins pentru a le numi eficiente?*".

În cele cel urmează, vom analiza prima întrebare și anume „*Cum trebuie să se implica guvernele în combaterea acestui fenomen nedirijat?".* Asfel, considerăm că este necesar să se țină cont de faptul că progresul tehnologic schimbă aplicarea legislației, și astfel aceasta urmează să fie modificată în coraport cu inovațiile apărute. Luând în calcul, faptul că Dark Web este un subiect foarte fragil și nou pentru mulți factori de decizie, desigur că nu putem simula nici o situație în care putem învăța din greșeli, neavând acest drept. Analizând DarkWeb, observăm că cel mai mare accent se pune pe anonimizare (ceea și ce îl diferențiază de Surface Web), fără acest esențial criteriu nu putem aborda existența DarkWeb, aici desigur TOR fiind cea mai mare problemă în neutralizarea acestei secțiuni a Internetului. Astfel iau naștere două condiții esențiale: „protejarea anonimatului" și „uniformizarea politicilor de combatere a fenomenului de DarkWeb". Referitor la prima condiție menționăm că însăși navigarea/utilizarea TOR, nu include nimic ilegal, însă din motivul că toți sunt anonimi, nu este identificat, pe moment, nici un mijloc funcțional care ar permite sortarea uilizatorilor după criteriul de intenție (legală sau ilegală). Desigur că este și foarte dificil de a trage la răspundere o persoană pentru acțiunile sale ilegale, din moment ce nu este cunoscută identitatea ultimei. A doua condiție reprezintă un nivel mai înalt de complexitate, deoarece se referă la uniformizare, o unificare a legislației cibernetice. Oricât de mult nu și-ar dori, o singură țară nu poate deține controlul asupra întregului spațiu „internet", din acest motiv este foarte important de a se găsi un consens în formarea acestui paravan de protecție.

În prezent, activitatea de contracarare a activităților cibernetice în Republica Moldova este direcționată de setul de activități incluse în Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 (HG 811/2015). Programul are drept scop crearea unui sistem de management al

securității cibernetice a Republicii Moldova prin securizarea serviciilor societății informaționale[7]. Problema cea mai mare reprezintă Hackerii[2], deoarece mediul lor de activitate este DarkWeb, folosindu-se de anonimizare maximă. Chiar dacă Republica Moldova depune efort pentru contracararea infracționalității, această realitate totuși persistă, ori atacurile de multe ori nu pot fi controlate doar cu eforturile unui stat.

În ceea ce urmează vom analiza experiențele 3 state, în eliminarea TOR. Prima analiză se referă la Federația Rusă, stat care a depus efort în a dezanonimiza TOR în scopuri politice, al doilea exemplu se referă la China, care a blocat accesul la TOR, și al treilea exemplu se referă la Austria, care a eliminat definitiv traficul TOR pe terioriul țării. China având una dintre cele mai riguroase politici în privința reglementării internetului, transformând paravanul de protecție într-o închisoare chineză în care are loc promovarea agresiunii. Din anul 2008, China, luptă cu dezvoltarea site-ului TOR, astfel în 2008, a fost blocat accesul la acest site, apoi în 2009 a încercat să blocheze toate calculatoarele ce serveau drept relee în asigurarea anonimatului utilizatorilor în spațiul TOR. În 2010, China a declarat că „*Pe teritoriul chinez, internetul se află sub jurisdicția suveranității chineze, iar reglementările chineze interzic în mod clar răspândirea informațiilor care au în vizor puterea statului sau se încalcă onoarea și interesele naționale.[9]* ". Una dintre cele mai dure acțiuni a fost luată în Austria, în anul 2014, când autoritățile au arestat un bărbat ce a oferit calculatorul său drept releu TOR, ulterior fiind tras la răspundere pentru contribuția la finalizarea unei infracțiuni cibernetice comisă de un alt utilizator, ce nu avea nici o implicare cu bărbatul arestat, exceptând faptul că traficul a fost redirecționat prin calculatorul releu[10] încălcând astfel punctul 12 din Strafgezetzbuch[3]. Astfel s-a creat un precedent ce concluzionează faptul că este practic ilegal să oferi un releu, în Austria. Dar pentru a înțelege cât de irațional este acest lucru, voi da următorul exemplu: Se va trage la răspundere directorul unui salon auto, deoarece el a vândut mașina care a fost folosită ulterior într-un jaf.

Este evident faptul că practica de a stabili cadru legal pentru activitatea

[2] Un hacker este un expert în informatică, care se ocupă cu studiul în profunzime al programelor informatice (sisteme de operare, aplicații), adesea folosind tehnici de inginerie inversă (demontare), cu scopul de a obține cunoștințe care nu sunt accesibile publicului larg. Cei ce folosesc aceste cunoștințe în scopuri ilegale, pentru a compromite securitatea sistemelor informatice sau a aplicațiilor, sunt de fapt crackeri (spărgători), însă în percepția publicului (formată de obicei de mass-media) noțiunile de hacker și cracker adesea se confundă.

[3] „Not only the immediate offender commits the offense, but also anyone who intended another to carry it out, or otherwise contributes to the completion of said criminal action."

TOR se impune drept o provocare. De exemplu ca răspuns la acțiunile Chinei de a bloca toate adresele IP cunoscute, TOR a creat alte relee speciale, numite poduri, având adrese IP secrete. În eventualitatea în care adresele sunt secrete, este necesar un timp mai îndelungat pentru a obține adresa unui pod. Acest proces îndelungat nu a fost o problemă pentru utilizatorii chinezi, care erau gata să aștepte oricât doar să obțină acel acces, din contra era o problemă imensă pentru guvernul chinez, deoarece nu putea solicita toate IP-urile simultan, astfel cât timp era măcar un singur pod activ, utilizatorii se puteau conecta. Această acțiune demonstrează încă odată ideea analizată mai sus, referitor la faptul că reglementările benefice ieri, pot să fie ineficiente în ziua de azi.

Astfel, Republica Moldova trebuie să facă față acestei provocări în asigurarea unui echilibru între protejarea anonimatului și prevenirea activităților ilegale în mediul online. Fiecare stat are poziții diferite în ceea ce privește lupta cu TOR. În această situație, evidențiind faptul că cooperarea internațională este esențială în această luptă, guvernele trebuie să colaboreze în vederea creării unor reglementări eficiente referitor la DarkWeb. În continuare vom trece la a doua problemă *Ce acțiuni trebuie întreprinse pentru a le numi eficiente?*, exemplificând necesitatea abordării eficiente a unor reglementări învățând din greșelile din trecut. Guvernul trebuie să utilizeze tactici ce ar permite, pe cât de mult posibil, să elimine criminalitatea din DarkWeb, dar în același timp să protejeze anonimatul utilizatorilor ce folosesc conexiunea dată în scopuri legale. Ulterior vom discuta despre exemplele făcute publice, dar care au avut un impact în lupta împotriva criminalității din DarkWeb. Un caz nereușit a avut loc în luna martie, anul 2015 când anchetatorii federali au trimis o citație către Reddit[11], în care se cereau datele personale a 5 utilizatori care au accesat darkwebmarkets (un forum în care anonimii discutau piețele negre). Această acțiune a fost clasificată ca inutilă și fără un rezultat pozitiv pe termen lung, deoarece din moment ce utilizatorii sunt alungați de pe forumurile deschise liber, de unde se poate colecta informația și ține sub supraveghere, ei se vor ascunde pe forumurile DarkWeb, de unde este mult mai dificil de a obține informații.

Al doilea caz a fost însăși eliminarea Drumului Mătăsii, cazul dat a fost nominalizat mai sus, care a avut un efect pozitiv de scurtă durată. Din luna octombrie 2013, când FBI l-a arestat pe Ross Ulbricht, a avut loc o explozie a pieților negre pe DarkWeb. Nu putem afirma că Drumul Mătăsii era benefic pentru societate sau mai bine spus pentru un control al bunurilor ilegale, dar totuși restul pieților erau pe lângă această mare piață, astfel se ține un mic control asupra dezvoltării micilor piețe. Reddit deține un „director" ce conține

lista piețelor de încredere și care nu se bucură de această încredere primind calificativul de „piețe fantomă". Clar este faptul că lista piețelor de încredere, este foarte mică în comparație cu cealaltă categorie. Foștii administratori ai Silk Road, au relansat Silk Road 2.0 la doar o lună de la închiderea Silk Road-ului original. Acesta a fost de scurtă durată deoarece, un furnizor a sustras 2,7 milioane dolari în bitcoin[12]. Ulterior în luna mai, anul 2016 a apărut Silk Road 3.0, aceasta fiind considerată cea mai securizată. Din acest caz putem concluziona că distrugerea acestei piețe nu a avut pe departe un efect pozitiv în crearea unei idei de a nu mai fortifica aceste piețe, ci din contra formând o descentralizare și un haos prin crearea mai multor piețe la nivel mai mic.

Un al treilea exemplu a avut loc în luna februarie 2015, când FBI a folosit instrumente speciale pentru a identifica adresele IP ale utilizatorilor ce accesau un site din DarkWeb cu conținut de abuz asupra copiilor „Playpen", creat în anul 2014, sub adresa: *http://upf45jv3bziuctml.onion/*, aceasta a fost posibil datorită faptului că serverul nu a fost configurat și a permis scurgerea adresei IP reale ce a dus către o companie de hosting din SUA. În decurs de o lună s-a ajuns la un număr de 60.000 conturi. În 2015, Playpen deja avea 215.00 conturi, 117.000 postări și 11.000 vizitatori unici pe săptămână. Pentru eliminarea acestui site FBI a recurs la o acțiune fră precedent, de a confisca serverul și a transfera site-ul către un sever FBI[13]. Timp de 13 zile cât a rulat site-ul Playpen pe serverul FBI, a fost posibilitatea de a colecta dovezi împotriva a peste 1300 utilizatori. Prin urmare din cele 3 exemple aduse, acesta ar fi cel mai potrivit, deoarece a reușit să colecteze probe împotriva utilizatorilor ce accesau site-ul cu conținut de abuz asupra copiilor, însă în același timp neatingând utilizatorii ce accesau TOR legal. Totuși creând o stare de incertitudine a utilizatorilor ce vor dori ulterior să acceseze site-urile ilegale, persistând riscul de a fi dezanonimați.

Concluzionând, menționăm că DarkWeb este o realitate a lumii virtuale, care are dreptul la existență, mai ales datorită facilităților existențiale oferite. Guvernele trebuie să pună accent pe instituționalizarea posibilității de utilizare a internetului sub anonimat, asigurarea drepturilor și libertăților tuturor utilizatorilor mediului on-line indiferent de zona virtuală în care se află, surfaceweb, darkweb. La fel, acțiunile urmează a fi consolidate și în contextul demascării infractorilor fără a aduce atingere confidențialității utilizatorilor simpli. Activitățile, astfel urmează a fi demarate, atît în plan legislativ cât și în plan operațional, criminalistic și chiar criminologic.

Referințe bibliografice:

1. Matt Beckstrom „Casting Light on the Dark Web: A Guide for Safe Exploration (LITA Guides)", Rowman & Littlefield Publishers.

Resurse Web:

1. Figura Iceberg reprezentată în majoritatea artcolelor. [accesat 27.11.2020] https://www.cyberdb.co/dark-web-need-know/

2. Centre for International Governance Inovation [accesat 27.11.2020] https://www.cigionline.org/

3. https://www.torproject.org/ [accesat 27.11.2020]

4. Daniel Sui, James Caverlee, Dakota Rudesill) Naval Research Laboratory [accesat 28.11.2020] https://www.wilsoncenter.org/sites/default/files/media/documents/publication/deep_web_report_october_2015.pdf

5. Tor Documentation, [accesat 28.11.2020] https://2019.www.torproject.org/docs/documentation.html.en

6. Congressional Research Service, Kristin Finklea, [accesat 29.11.2020] https://fas.org/sgp/crs/misc/R44101.pdf

7. Securitatea Cibernetică. [accesat 29.11.2020]https://mei.gov.md/ro/content/securitate-cibernetica

8. TOR Sponsors, 2020 [accesat 29.11.2020] https://www.torproject.org/about/sponsors/

9. Clemmitt, M. 2016. "The Dark Web." [accesat 29.11.2020] http://library.cqpress.com/cqresearcher/document.php?id=cqresrre2016011500

10. Internet relay op convicted for child porn [accesat 29.11.2020] https://www.thelocal.at/20140705/internet-relay-op-convicted-of-child-porn-offenses -

11. https://www.reddit.com/ [accesat 30.11.2020]

12. https://finance.yahoo.com/news/death-silk-road-darknet-markets-142500702.html Swearingen, J. 2014. "A Year after Death of Silk Road, Darknet Markets are Booming." [accesat 30.11.2020]

13. Admin of Dark Web Child Pornography Website „Playpen" [accesat 30.11.2020]https://news.softpedia.com/news/admin-of-dark-web-child-pornography-website-playpen-found-guilty-508405.shtml