Masarykova univerzita
Filozofická fakulta

Bakalářská práce

2016 **Eva Šteinigerová**

Masarykova univerzita
Filozofická fakulta

Kabinet informačních studií a knihovnictví

Informační studia a knihovnictví

Eva Šteinigerová

Technické a etické aspekty Onion routingu

Bakalářská práce

Vedoucí práce: Mgr. Michal Černý

BIBLIOGRAFICKÝ ZÁZNAM

Šteinigerová, Eva. Technické a etické aspekty Onion routingu. Brno, 2016. 62 s. Bakalářská práce. Masarykova univerzita, Filozofická fakulta, Ústav české literatury a knihovnictví, Kabinet informačních studií a knihovnictví. Vedoucí práce Mgr. Michal Černý.

ANOTACE

Předkládaná práce s názvem *Technické a etické aspekty Onion routingu* seznamuje čtenáře s problematikou anonymity v online prostředí, přičemž se zaměřuje především na představení software a sítě Tor, zdařilé implementace teoretického mechanismu onion routingu. Tato technologie je ve světě relativně známá a používaná, cílem této práce je její uvedení do českého prostředí a představit ji běžnému internetovému uživateli. Tor je zařazován mezi tzv. anonymizéry, a proto se práce věnuje také fenoménu anonymity, anonymitou jako bezpečnostní funkcí a jsou zde představeny také její psychologické aspekty. Jak název práce předesílá, na téma anonymity poskytované technologií Tor je pohlíženo po stránce technologické a etické. Etické ukotvení možnosti anonymního pohybu v online prostředí je vyloženo v kontextu konkrétních vyznávaných hodnot informační etiky.

ANNOTATION

Presented thesis entitled *Technical and ethical aspects of Onion routing* introduces readers to the issue of online anonymity, focusing primarily on introducing Tor as a software and anonymity network. This technology is already well known in the world, therefore the aim of this study is to introduce it into Czech environment and to an ordinary Internet user. Tor is classified among the so-called anonymizers, therefore this paper also focuses on the phenomenon of anonymity, looking at anonymity as a security feature and presenting its psychological aspects as well. As announced in the title of this thesis the topic of anonymity provided by Tor technology is percieved in terms of technology and ethics. Ethical anchoring the possibility and ability of online anonymity is interpreted in the context of the certain values professed by information ethics.

KLÍČOVÁ SLOVA

Onion routing, Tor, anonymita, informační etika, soukromí, demokracie, dohled

KEYWORDS

Onion routing, Tor, anonymity, information ethics, privacy, democracy, surveillance

Prohlašuji, že jsem diplomovou práci vypracovala samostatně s využitím uvedených pramenů a literatury.

……

Podpis autora práce

I. ÚVOD

O dnešní společnosti se hovoří jako o informační, případně znalostní, nebo též jako o společnosti sítí, přičemž společný jmenovatel takových přívlastků představují informační technologie. S rychlostí a masovostí jejich vývoje nestačí držet krok disciplíny, které by poskytly technickému a technologickému vývoji patřičné ukotvení, ať už legislativního nebo etického charakteru. Hovoří se o tom, že proběhla jakási informační revoluce, která vyžadovala diskuzi o etických hodnotách a principech. Tato diskuze však také proběhla a poukázala na potřebu vyhotovení nového legislativního ukotvení etických problémů spojených s informačními technologiemi. Můžeme říct, že takové legislativní zpracování informační etiky proběhlo a průběh pokračuje i nadále. Co je potřeba udělat dál?

V zahraničních zdrojích se stále ve větší míře objevují články o potřebě limitovat dohled vládních a korporátních agentur, poukazuje se na nedostatečnost legislativního ukotvení této problematiky a nutnost nabídnout technický způsob řešení. I do veřejné diskuse v českém prostředí zvolna prosakuje relativně nový termín společnosti pod dohledem. Jedná se o zdánlivě novodobý fenomén, ačkoliv nová je spíše jeho technologická forma. Tento koncept hovoří o technologiích ohrožujících naše soukromí a upozorňuje na potřebu, ale zároveň i na možnost využít tyto technologie právě naopak, a to k ochraně našeho soukromí a dalších práv, které přirozeně přesahují rámec virtuálního prostředí.

Prací a analýz, věnujících se konkrétním nástrojům a mechanismům znemožňujících identifikace internetových uživatelů byla publikována celá řada, stejně jako pojednání a studií, zabývajících se anonymitou na Internetu. V předložené práci se oba tyto přístupy pokusím spojit, a tak uvést tak konkrétní anonymizační nástroj do etického rámce a užívání tohoto nástroje, potažmo možnost a schopnost pohybovat se v online prostředí anonymně budou hodnoceny z hlediska předem definovaného etického rámce, přičemž ochrana soukromí bude reprezentovat klíčovou vyznávanou hodnotu.

Cílem mé práce tedy je koncept Onion routingu, lépe řečeno software Tor a jeho funkčnost představit běžnému uživateli Internetu. Mou snahou je rovněž poukázat na legitimnost užívání této technologie a možnosti pro ochranu hodnot vyznávaných moderní společností, kterou nabízí.

Práce je členěna do třech větších oddílů:

I. Technické aspekty, kde je představen koncept Onion routingu a primárně vysvětlena funkčnost jeho implementace Tor. Je zde uvedeno několik dalších projektů souvisejících s mechanismem Tor, největší prostor je věnován nástroji Tor Browser a problematice skrytých služeb.

II. Anonymita je tématem druhého oddílu. Tento fenomén je představen z několika hledisek. Kromě klasického uvedení konceptu anonymity, je na tento stav nahlíženo rovněž z technického hlediska a jsou zmíněny také psychologické aspekty anonymního pohybu v online prostředí.

III. Etické aspekty je oddíl, ve kterém je zvolen přístup, na jehož základě bude mechanismus onion routing, respektive software Tor a jím zprostředkovaná anonymita, s přihlédnutím ke stávající legislativě, usouvztažněni.

II. TECHNICKÉ ASPEKTY

V následujícím oddílu bude věnována pozornost konceptu Onion routing a jeho implementaci The Onion Routing, technologii pro tuto práci klíčové. Je popsána funkčnost mechanismu a představena podoba zapojení uživatel do sítě. Následuje kapitola představující uživatele Tor a služby, které síť Tor zprostředkovává.

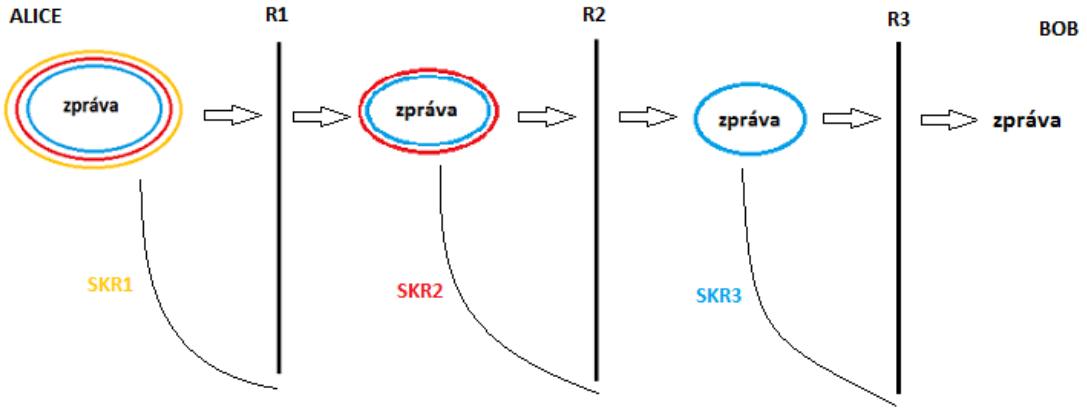
1. Koncept Onion routingu

Onion routing, v překladu cibulové směrování, byl odvozen z konceptu mixnetu, který staví na modelu, kde každý uzel v síti představuje zároveň router, přes který prochází tok dat. Onion routing, zkráceně OR je označení pro mechanismus představující obecné řešení pro obousměrnou anonymizaci spojení řady aplikačních protokolů (HTTP, FTP, SSH, SMTP aj.), vhodný pro anonymní komunikaci při použití veřejné sítě. Název této techniky je odvozen od struktury zpráv a jejich zpracování. Zašifrování zprávy v několika vrstvách připomíná cibuli, každý průchod přes router odšifruje, tedy jakoby sloupne jednu vrstvu. Mechanismus onion routingu je detailněji popsán v následujícím textu.

Alice se chce Bobovi zaslat zprávu, ke které zvolila komunikační cestu o třech routerech, které si označíme jako R_1, R_2 a R_3. Tuto zprávu zašifruje Bobovým veřejným klíčem s tím, že k ní přidá pokyn (cell) pro router R_2 , aby následně zaslal zprávu na router R_3. Celý tento paket navíc zašifruje veřejným klíčem R_2. Následně s přidáním pokynu pro R_1, aby po obdržení zaslal zprávu dál routeru R_2, k takto zašifrované zprávě celý paket zašifruje veřejným klíčem prvního routeru R_1.

Zjednodušené schéma:

ALICE – {{{zpráva}}} -> R_1 – {{zpráva}} -> R_2 – {zpráva} -> R_3 – zpráva -> BOB



Obrázek 1: Znázornění šifrování zprávy, vlastní zpracování

Data jsou posílána přes sérii několika routerů, přičemž každý z nich má informaci pouze o svých sousedních routerech, zná tedy pouze svého předchůdce a následovníka. Zároveň každému z routerů je přidělen pár klíčů (soukromý a veřejný), jednotlivé vrstvy paketu se totiž autentizují digitálním podpisem pro zaručení integrity posílaných dat.

První uzel tedy zná IP adresu odesílatele, ale nezná obsah dat. Druhý uzel nezná původního odesílatele ani obsah zprávy, zná jen uzel, od kterého pakety získal, a uzel, kterému je má poslat dál. Poslední, koncový uzel opět zná, odkud pakety přišly, rozšifruje i obsah, který přenese k cílovému serveru, ale nezná původce této zprávy, ten zůstává vůči cílovému serveru i koncovému uzlu anonymní.

Teoretický prototyp konceptu je funkční, reálné implementace jsou občas problematické.

1.1 Od onion routingu k Tor

Dějiny této techniky se začínají psát od roku 1995, kdy U.S. Naval Research Laboratory inicializuje první práce na konceptu, jenž by ochraňoval komunikaci zpravodajského společenství Spojených států. Rok nato Paul Syverson se svými kolegy, Michaelem G. Reedem a Davidem Goldschlagem, oficiálně představili koncept označený jako Onion routing1. Dílčí dohled nad dalším vývojem a rovněž i část financování převzala Agentura ministerstva obrany

[1] GOLDSCHLAG, David M., Michael G. REED a Paul F. SYVERSON. *Hiding Routing information* [online]. s. 137 [cit. 2016-04-22]. DOI: 10.1007/3-540-61996-8_37. Dostupné z: http://link.springer.com/10.1007/3-540-61996-8_37

pro pokročilé výzkumné projekty (DARPA). V roce 1998 Námořnictvo Spojených států amerických podalo žádost o patentování této techniky[2], patent byl udělen o tři roky později. Roku 1999 jsou vývojářské práce pozastaveny, jednak z důvodu nedostatečných dotací, jednak díky dalším projektů vývojářského týmu, nicméně výzkumná a analytická činnost nadále pokračuje.

Výrazným milníkem je rok 2002, kdy se k týmu vývojářů připojili počítačoví odborníci Roger Dingledine a Nick Mathewson. A právě tato dvojice stojí za tou nejzdařilejší a nejúspěšnější implementací onion routingu, tzv. The Onion Routing[3] neboli TOR. Od roku 2003 je zdrojový kód Tor šířen pod svobodnou a otevřenou licencí MIT. V této době rozsah sítě odpovídá asi dvanácti americkým uzlům s výjimkou jednoho německého. Následujícího léta jsou na síti spuštěny skryté služby. Rok 2006 rovněž významný pro založení neziskové organizace Tor projekt, pod záštitou a též parciálním dotováním Electronic Frontier Foundation (EFF), organizace zabývající se ochranou práv v digitálním světě.

2. The Onion Routing

The Onion Routing, častěji znám pod akronymem Tor, je úspěšnou implementací konceptu onion routing. Jedná se o open source software, který zajišťuje anonymní pohyb uživatele na Internetu tak, že skrývá informace o IP adrese a další údaje, které by mohly vést k identifikaci uživatele. Primárně je Tor určen k ochraně osobních údajů uživatelů a jejich soukromí, stejně tak podporuje svobodný přístup k informacím. Tor je též označení pro síť, jež je vytvořena na základě dobrovolných uzlů provozovaných uživateli z celého světa.

Oproti jiným nástrojům, založeným na tomto principu (např. AN.ON), disponuje Tor adresářovými servery s informacemi o jednotlivých routerech a podporu skrytých služeb a míst setkání. Tor umožňuje jak anonymní prohlížení webu, tak i anonymní webhosting. Hlavním rozdílem vzhledem k původnímu teoretickému konceptu, je možnost uživatele síť Tor používat, aniž by v ní musel figurovat jako router. Pro užívání Tor není zapotřebí ani žádných změn

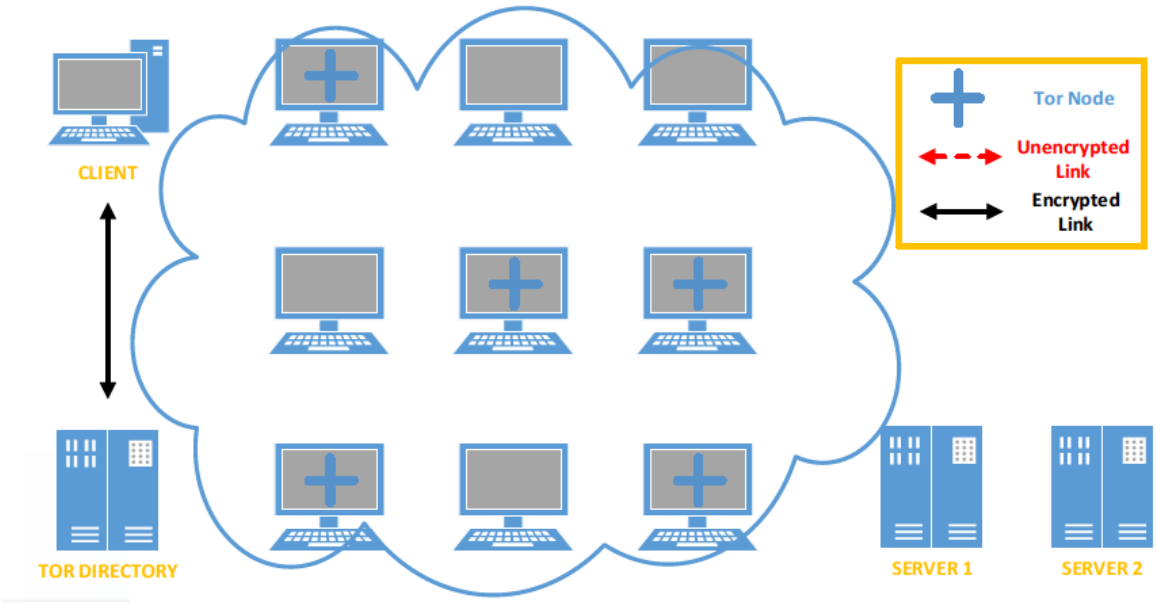
[2] THE UNITED STATES OF AMERICA AS REPRESENTED BY THE SECRETARY OF THE NAVY. *Onion routing network for securely moving data through communication networks*. US 6,266,704 B1. United States. 09/086,541. Přihlášeno 29. 5. 1998. Uděleno 24. 7. 2001. Dostupné také z: https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US6266704.pdf

[3] Tor: The Second-Generation Onion Router. In: *Proceedings of the 13th conference on USENIX Security Symposium* [online]. USA: USENIX Association Berkeley, 2004 [cit. 2016-04-23]. Dostupné z: http://dl.acm.org/citation.cfm?id=1251375&picked=prox&cfid=767814377&cftoken=95122783

v jádře operačního systému, jedná se o volně dostupný software, který podporuje většinu aplikací bez nutnosti jejich modifikace, přináší navíc dokonalé dopředné utajení. Protože se jedná o systém s nízkou latencí, je vhodný pro komunikaci v reálném čase. Nedochází zde k pozdržení zpráv, jako v případě Stop-and-go mixů, uživatel rovněž vybírá z předem připravených komunikačních cest, které jsou vytvářeny asynchronně v pozadí. Na rozdíl od teoretického mechanismu, Tor poskytuje testování integrity přenášených dat, zejména z důvodů obrany vůči tagging útokům.

2.1. Jak Tor funguje

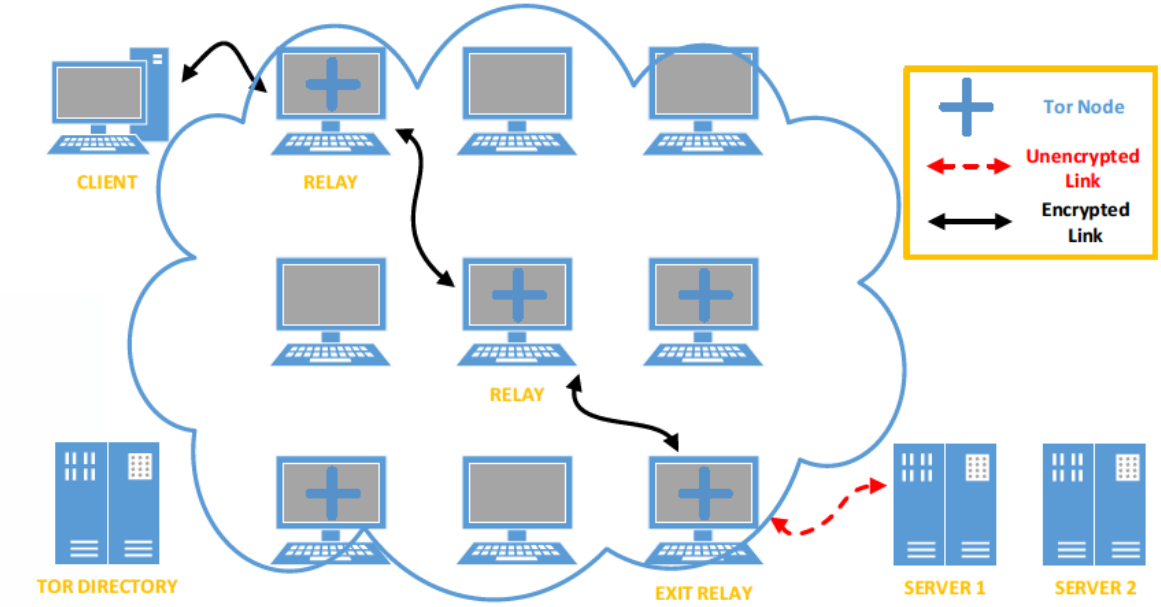
Obrázek 2 zobrazuje jednoduchý nákres sítě Tor. Počítače označené křížkem představují uzly v této síti. První krok pro připojení k síti, je zaslání zašifrovaného požadavku, na základě kterého klient (*CLIENT*) obdrží od adresářového serveru (*TOR DIRECTIORY*) seznam Tor uzlů. Bezprostředně poté může být zahájeno připojení k síti, respektive k těmto uzlům. Cílové servery, se kterými se chceme prostřednictvím sítě Tor spojit, jsou označeny jako *SERVER 1* a *SERVER 2*.



Obrázek č. 1: Jak funguje Tor, nákres sítě [4]

[4] ÇALIŞKAN, Emin, Tomáš MINÁRIK a Anna-Maria OSULA. *Technical and Legal Overview of the Tor Anonymity Network* [online]. Tallinn, 2015 [cit. 2016-01-20]. Dostupné z: https://ccdcoe.org/sites/default/files/multimedia/pdf/TOR_Anonymity_Network.pdf

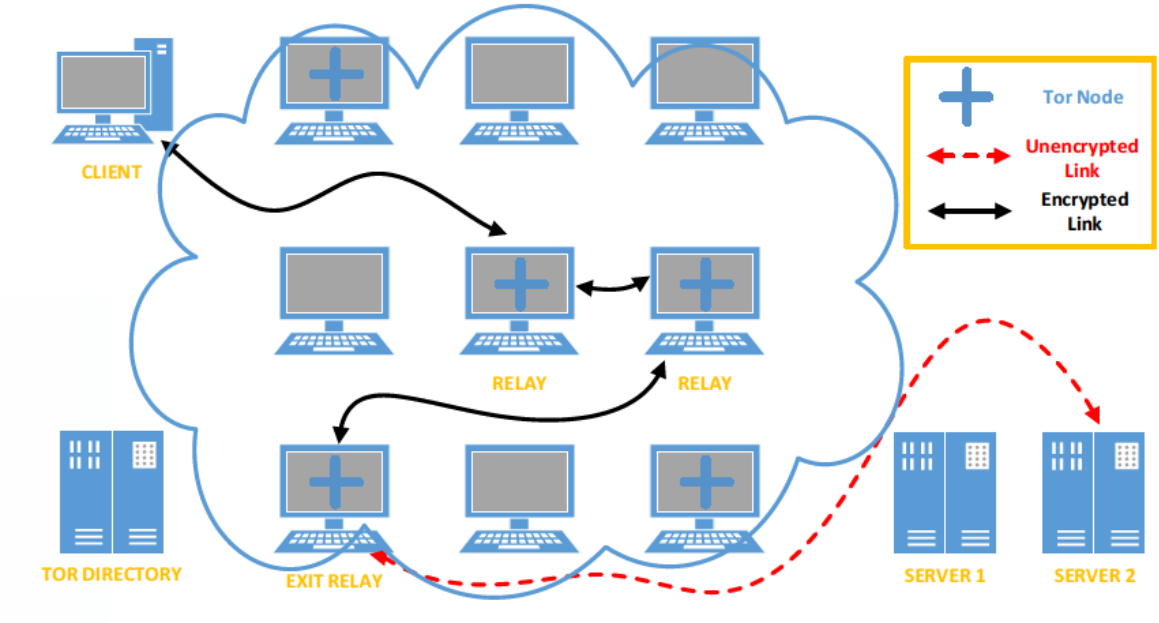
Vizualizace na obrázku 3 představuje vytvoření již zmíněné komunikační cesty. Ta v tomto případě sestává ze dvou prostředních uzlů a jednoho koncového, neboť se chceme spojit se *SERVEREM 1*, který se nachází mimo síť Tor. Komunikační cesta je zašifrována až do okamžiku navázání spojení s vnějším serverem, nešifrovaný je úsek mezi koncovým uzlem a tímto serverem, který představuje např. webovou stránku s HTTP protokolem. Jestliže by se jednalo o server s HTTPS protokolem, pak by byl šifrovaný i poslední úsek, avšak v závislosti na implementaci webové služby.



Obrázek 1:Jak funguje Tor, komunikační cesta[5]

Na obrázku 4 je zobrazena situace, kdy chce uživatel navázat další spojení, tentokrát se SERVEREM 2. Pro toto připojení, stejně jako pro každé další, byť by se operace opakovaně týkala totožného cílového serveru, je vytvořena jiná cesta.

[5] ÇALIŞKAN, Emin, Tomáš MINÁRIK a Anna-Maria OSULA. *Technical and Legal Overview of the Tor Anonymity Network* [online]. Tallinn, 2015 [cit. 2016-01-20]. Dostupné z: https://ccdcoe.org/sites/default/files/multimedia/pdf/TOR_Anonymity_Network.pdf



Obrázek 4: Jak funguje Tor, další připojení[6]

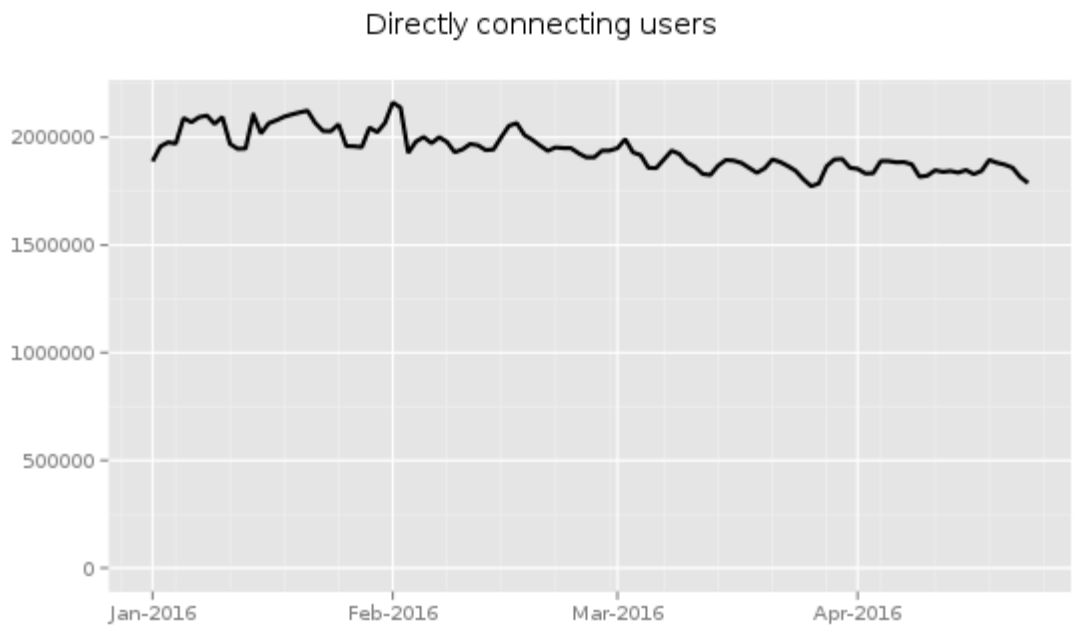
2.2. Podoba účasti v síti Tor

Jak bylo zmíněno výše, uživatel automaticky nepředstavuje další router v síti, zapojení uživatele do sítě Tor nabývá třech podob.

První možností je prostá účast jako klient, který si stáhnul prohlížeč Tor a používaje jej k vyhledávání na síti. Takové možnosti využívá nejvíce uživatelů. Následující graf (graf 1) zobrazuje odhad počtu uživatelů, kteří se takovým způsobem k Toru denně připojí. Tito uživatelé nejčastěji pochází ze Spojených států (19,37 %), z Ruska (11,58 %) a z Německa (9,90 %)[7].

[6] ÇALIŞKAN, Emin, Tomáš MINÁRIK a Anna-Maria OSULA. *Technical and Legal Overview of the Tor Anonymity Network* [online]. Tallinn, 2015 [cit. 2016-01-20]. Dostupné z: https://ccdcoe.org/sites/default/files/multimedia/pdf/TOR_Anonymity_Network.pdf

[7] TorMETRICS [online]. [cit. 2016-04-20]. Dostupné z: https://metrics.torproject.org/userstats-relay-table.html



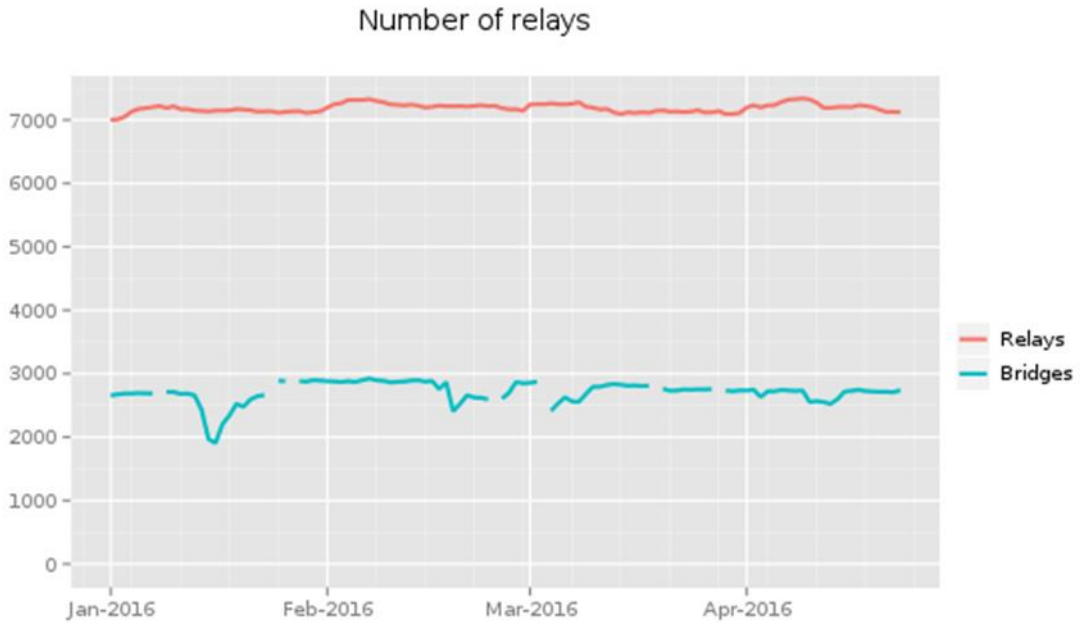
Graf 1: Počet uživatelů připojeným k síti Tor přímo[8]

Provozovat uzel (relay), je další z možností, jak se zapojit. Tyto uzly jsou dvojího typu. Prostřední uzel (*Middle relay)* je takový, prostřednictvím kterého jsou data přeposílána v rámci sítě, koncový uzel (*Exit relay*) zase zajišťuje komunikaci mezi sítí Tor a servery mimo tuto síť, přenášejí zprávu ze sítě Tor ke zvolené destinaci. Na tomto místě dochází k výstupu z anonymity, IP adresa koncového uzlu je interpretována jako původce přenášených dat. Přestože je provozování koncového uzlu legální, doposud vyvolává kontroverzi, a to kvůli potencionálně škodlivému obsahu přenášených zpráv. Kromě speciální konfigurace a doporučení provozování tohoto uzlu na vyhrazeném stroji, upozorňují vývojáři softwaru na případnou pozornost ze strany orgánů činných v trestním řízení.

Poslední forma možného zapojení se do sítě Tor obnáší provoz tzv. uzlu pro přemosťování (*Bridge relay*), zkráceně mostu (*Bridge*). Mosty jsou skryté, nejsou zveřejněny na seznamu, kterým disponuje hlavní adresářový server, neexistuje ani jejich kompletní, veřejně dostupný soupis. Tento typ uzlů se využívá zejména v případech, kdy poskytovatel internetového připojení blokuje počáteční uzel cesty, nebo též všechny uzly. Toto je běžná praxe v zemích blokujících Tor. V takovém případě se pro připojení k síti použije právě mostu. Jelikož jejich IP adresy nejsou nikde zveřejněny a získat je lze např. prostřednictvím emailu bridges@bridges.torproject.org, je nepravděpodobné, že by byly blokovány.

[8] TorMETRICS [online]. [cit. 2016-04-20]. Dostupné z: https://metrics.torproject.org/userstats-relay-country.html

Počet uživatelů provozující uzel nebo most znázorňuje graf 2.



Graf 2: Počet uživatelů provozujících uzel a počet uživatelů provozující most[9]

Následující tabulka (tabulka 1) zachycuje pořadí zemí, odkud se uživatelé nejčastěji připojují k síti Tor prostřednictvím mostu.

Země	Průměrný počet uživatelů / den
Spojené státy	6426 (18,28 %)
Rusko	4591 (13,06 %)
Írán	2659 (7,57 %)
Spojené království	1701 (4,84 %)
Německo	1502 (4,27 %)
Čína	1022 (2,91 %)
Francie	891 (2,54 %)
Indie	842 (2,39 %)
Brazílie	647 (1,84 %)
Turecko	618 (1,76 %)

Tabulka 1: Počet a původ uživatelů Tor využívající pro připojení mosty[10]

Zdařilou záležitostí je rozhodně TorFlow, vizualizace toku dat prostřednictvím sítě Tor, dostupná na https://torflow.uncharted.software/.

[9] TorMETRICS [online]. [cit. 2016-04-20]. Dostupné z: https://metrics.torproject.org/networksize.html

[10] TorMETRICS [online]. [cit. 2016-04-20]. Dostupné z: https://metrics.torproject.org/userstats-bridge-table.html

2.3. Tor Browser

Tor Browser, dříve známý jako Tor Browser Bundle (v češtině prohlížeč Tor, používán je však originální název), je považován za vlajkovou loď organizace Tor Project. Jedná se o prohlížeč, jenž vznikl modifikací komerčního prohlížeče Mozilla Firefox a který je soustavně aktualizován na základě té nejnovější verze Firefox Extended Support Release. Možnost používat Tor bez nutnosti instalace dalšího softwaru nabízí Tor Browser na operačních systémech Windows, Mac OS X a Linux[11]. Podrobněji si Tor Browser uvedeme v kontextu ukázky jeho instalace.

2.3.1 Ukázka instalace

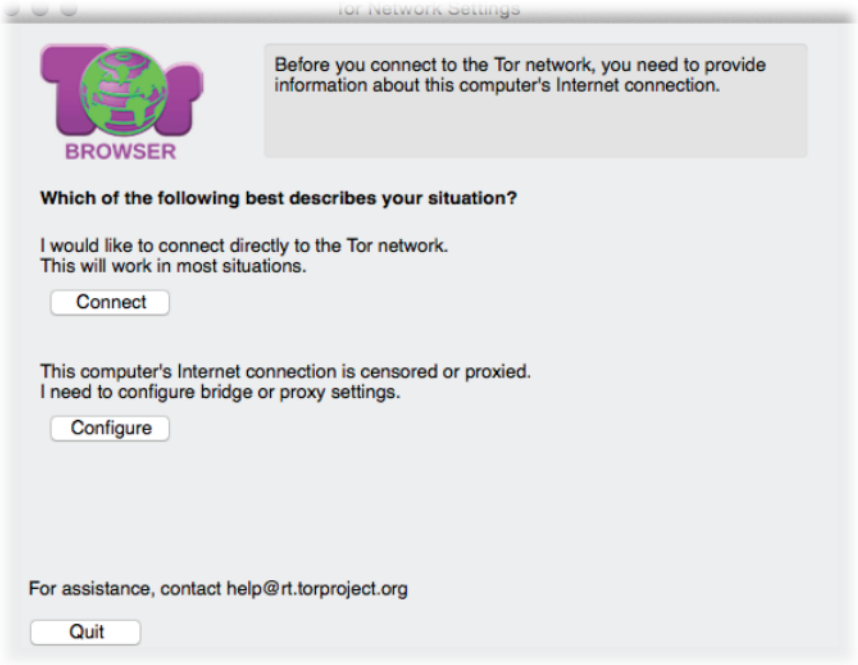
Prvním krokem (obrázek 5) je stažení tohoto prohlížeče přímo ze stránek Tor Project (https://www.torproject.org/download/download-easy.html.en).

Obrázek 5: Stáhnutí prohlížeče[12]

Na tomto místě je důležité zkontrolovat PGP podpis, který zajišťuje integritu softwaru. Při prvním otevření prohlížeče je uživatel vyzván k „připojení nebo konfiguraci“ (obrázek 6). Je příhodné před prvním připojením projít konfigurací, neboť díky ní uživatel získá lepší přehled, jak prohlížeč Tor funguje.

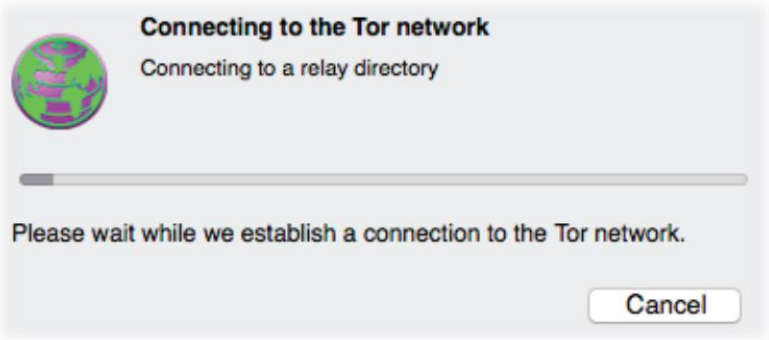
[11] THE TOR PROJECT. Tor: Anonymity Online [online]. [2012] [cit. 2015-12-29]. Dostupné z: https://www.torproject.org/projects/torbrowser.html.en

[12] How to Use Tor With Firefox. WikiHow [online]. [cit. 2016-01-20]. Dostupné z: http://www.wikihow.com/Use-Tor-With-Firefox



Obrázek 6: Výzva k přímému připojení nebo konfiguraci[13]

Pakliže se uživatel rozhodne přímo pro připojení, v dalším okně se začne navazovat spojení se sítí Tor (obrázek 7).



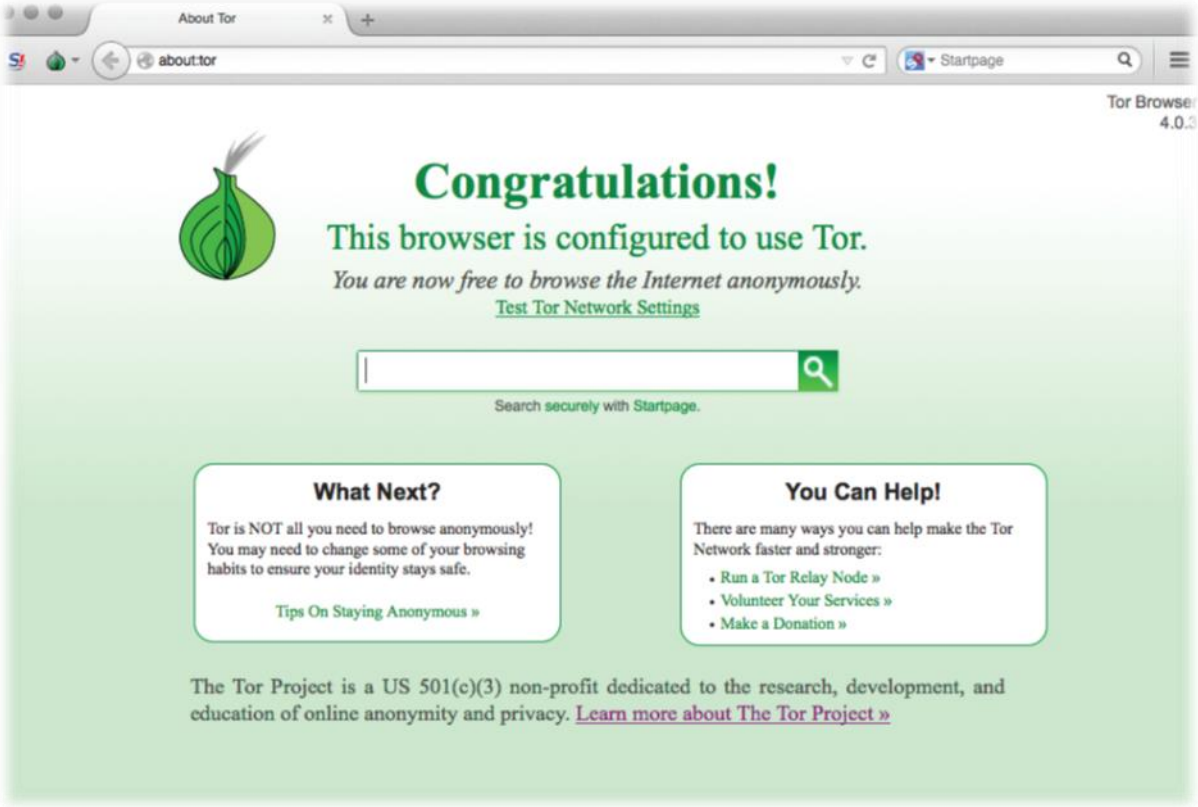
Obrázek 7: Navazování spojení se sítí Tor[14]

Toto okno se objeví při každém otevření prohlížeče. Je třeba počítat s tím, že připojování může někdy trvat delší dobu.

[13] MACRINA, Alison. Accidental Technologist: The Tor Browser and Intellectual Freedom in the Digital Age. *Reference & User Services Quarterly* [online]. 2015, **54**(4), 17-20 [cit. 2016-01-20]. ISSN 1094-9054. Dostupné z: https://journals.ala.org/rusq/article/view/5704/7092

[14] MACRINA, Alison. Accidental Technologist: The Tor Browser and Intellectual Freedom in the Digital Age. *Reference & User Services Quarterly* [online]. 2015, **54**(4), 17-20 [cit. 2016-01-20]. ISSN 1094-9054. Dostupné z: https://journals.ala.org/rusq/article/view/5704/7092

Pokud bylo úspěšně navázáno spojení, otevře se prohlížeč s uvítáním: *„Gratulujeme! Tento prohlížeč je nakonfigurován pro používání Tor.“* (obrázek 8). Úvodní stránka představuje zároveň výchozí vyhledávač. Domovská stránka prohlížeče Tor



Obrázek 8: Domovská stránka prohlížeče Tor[15]

Pod uvítáním je odkaz s označením “*Test Tor Network Settings*” (Zkušební nastavení sítě Tor), kliknutím na něj uživatel zjistí, jaká IP adresa mu byla přidělena.

Prohlížeč Tor disponuje dvěma již nainstalovanými rozšířenými, jedná se o HTTPS Everywhere a NoScript. HTTPS Everywhere je nástroj z dílny EFF, umožňující permanentní využívání protokolu HTTPS při návštěvě určitých webových stránek. Komunikace s takovými stránkami je šifrovaná a prohlížení je pak bezpečnější. NoScript je doplněk prohlížeče, jenž rovněž zvyšuje bezpečí uživatele. Toto rozšíření funguje jako přednastavení, které zakazuje používání určité formy spustitelného webového obsahu. Jedná se především o Javu, JavaScript a Flash, protože právě tyto skripty dovedou uživatele prohlížeče Tor de-anonymizovat, ať už propojením k uživatelskému účtu, ignorací konfigurace proxy serveru nebo sběrem cookies dalších dat z vyhledávače i operačního systému. Z tohoto důvodu prohlížeč Tor blokuje

[15] MACRINA, Alison. Accidental Technologist: The Tor Browser and Intellectual Freedom in the Digital Age. *Reference & User Services Quarterly* [online]. 2015, **54**(4), 17-20 [cit. 2016-01-20]. ISSN 1094-9054. Dostupné z: https://journals.ala.org/rusq/article/view/5704/7092

např. RealPlayer nebo Quicktime. Stejně tak není doporučováno instalovat další pluginy a rozšíření, neužívat torrenty a prohlížeč varuje uživatele i před automatickým otevíráním dokumentů získaných prostřednictvím externích aplikací. Všechna tato doporučení jsou shrnuta v "šesteru" správného užívání Tor[16].

Za pozornost stojí tlačítko Tor (*Tor Button*) v podobě malé cibule nalevo od příkazového řádku (obrázek 9). Toto tlačítko umožňuje uživateli provádět změny v nastavení a regulovat preference. Skrze tlačítko lze rovněž získat novou identitu, tedy nechat si přiřadit novou IP adresu.

Obrázek 2: Tlačítko Tor[17]

Je důležité mít na paměti skutečnost, že původ přiřazené IP adresy bude mít vliv na prohlížení webu. Takže pokud je uživateli přiřazena IP adresa, která se nachází např. v Itálii, pak se některé stránky budou objevovat v italštině.

2.3.2 Hluboký web

Tor Browser je používán jednak k běžnému prohlížení, tedy k surfování po povrchovém webu, jednak zprostředkovává spojení s hlubokým webem (*deep web*). Jedná se o výseč webu, která je často zaměňována s tzv. Dark webem[18], tedy temným webem, který je součástí toho

[16] Šestero správného užívání Tor:
1. Používej prohlížeč Tor
2. Nepoužívej torrent v síti Tor
3. Neinstaluj pluginy k prohlížeči
4. Používej HTTPS verzi webových stránek
5. Neotevírej dokumenty stažené prostřednictvím Tor, když jsi online
6. Používej bridges a/nebo si najdi doprovod

THE TOR PROJECT. Tor: Anonymity Online [online]. [2012] [cit. 2015-12-29]. Dostupné z: https://www.torproject.org/download/download-easy.html.en

[17] MACRINA, Alison. Accidental Technologist: The Tor Browser and Intellectual Freedom in the Digital Age. *Reference & User Services Quarterly* [online]. 2015, **54**(4), 17-20 [cit. 2016-01-20]. ISSN 1094-9054. Dostupné z: https://journals.ala.org/rusq/article/view/5704/7092

[18] Dark web nemá ustálený český ekvivalent, běžně se používá originálního termínu.

hlubokého, avšak představuje nevelkou frakci. Tyto pojmy je důležité rozlišovat, a proto se následující text bude zabývat jejich vysvětlením.

Povrchový web je internetovým uživatelům běžně znám, každodenně do něj vstupují prostřednictvím mainstreamových prohlížečů (Google, Bing aj.), řešících dotazy uživatelů přímým prolinkováním na stránku s požadovanou informací. Povrchový web je tedy označení pro:

> *„internetové informační zdroje a dokumenty, které jsou dostupné prostřednictvím standardních vyhledávacích strojů (např. Google, AltaVista apod.). Za určitý protiklad je považován tzv. neviditelný web.“*[19]

Pojem Neviditelný web poprvé použila americká knihovnice Jill Ellsworth roku 1994 pro označení takových dokumentů, které prostřednictvím prvních vyhledávačů nebylo možné najít. Termín neviditelný web se postupem času ukázal být jako nepřesný, a proto byl zaveden vhodnější termín, hluboký web, Deep web. Hovoříce o Deep webu, máme na mysli:

> *„internetové informační zdroje, jejichž obsah není dostupný prostřednictvím standardních vyhledávacích strojů. Může se jednat o informace, které jsou uloženy v databázích a generují se dynamicky až na základě interakce uživatele se systémem (např. online katalogy knihoven nebo bibliografické báze dat) nebo o informace, ke kterým je přístup chráněn heslem a jsou dostupné pouze autorizovaným uživatelům, často pouze na komerční bázi (plné texty časopisů apod.). Běžné vyhledávací nástroje (vyhledávací stroje) nemohou podobný typ informací ve svých databázích registrovat, buď pro technická omezení nebo proto, že je jejich robotům vstup do těchto zdrojů zakázán. Vyhledávací služby sice poskytnou informaci o existenci podobného informačního zdroje, ale nevyhledají informace, které jsou v něm obsaženy. Některé vyhledávací služby však již tyto informace dokáží zpracovávat (např. vyhledávací stroj Scirus - Elsevier Science).“*[20]

Historie hlubokého webu je paralelní k historii webu jako takového. Milník, od kdy dochází k rozlišování těchto dvou oblastí, představuje rok 1994 a uvedení prvního vyhledávače, WebCrawler, vytvořený Brianem Pinkertonem. Jednalo se o softwarového robota, jenž hromadil texty stránek do databáze, v rámci které bylo umožněno vyhledávání prostřednictvím

[19] Celbová, Ludmila. Volně indexovatelný web. In: *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha: Národní knihovna ČR, 2003- [cit. 2016-04-20]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000572&local_base=KTD

[20] Tkačíková, Daniela. Neviditelný web. In: *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha: Národní knihovna ČR, 2003- [cit. 2016-04-20]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000547&local_base=KTD

klíčových slov. Do doby před zavedením praktiky indexace si uživatelé posílali adresy stránek e-mailovými zprávami.
Důvodů, proč nedochází k indexaci některých webových stránek, může být několik. Často se však jedná o stránky, které jsou chráněny heslem, např. databáze, se kterými pracují vlády, knihovny nebo zdravotnické instituce, nebo stránky s dynamickým indexováním. Množství vyhledávačů má rovněž limit pro indexování stránek z určité domény a dávají přirozeně přednost těm populárním stránkám. Neindexované jsou též stránky se závadným obsahem, nebo ty vyhotovené ve specifickém formátu.

Oproti tomu Dark web je znepřístupněn standardními vyhledávači zcela záměrně. Termín Dark web hovorově odkazuje primárně na podpůrnou sít kryptografických skrytých služeb (*hidden* services) a míst setkání. Jenže to není zcela přesné, jak se dozvíme v následující kapitole.

2.3.3 Skryté služby

Britský ministr Julian Smith označil Tor jako „temný Internet se nachází dětská pornografie a obchoduje s drogami a zbraněmi.“[21] To je zapříčiněno skutečností, že Tor je slouží k prohledávání démonizovaného hlubokého webu, kde jsou skryté služby umístěny. Tyto služby fungují od roku 2004 a rozhodně nejsou využívány pouze v kontextu páchání trestní činnosti. Tuto technologii užívají i organizace pro ochranu disidentů, aktivistů, terapeutické skupiny a poradny. Mezi nejnavštěvovanější skryté služby[22] patří stránky Pastebin, Twitter, a Reddit.

Skryté služby byly navrženy tak, aby nebyly snadno vystopovatelné, připojit se k nim můžeme pouze uživatel využívající softwaru Tor, adresy těchto serverů se speciální příponou *.onion* jsou nestabilní, a díky decentralizované architektuře sítě, je složité je zmapovat.

[21] MARSHALL, Gary. Tor infinity, and beyond: everything you need to know about the Dark Web. In: *TechRadar* [online]. England: Future plc, 2015 [cit. 2016-04-15]. Dostupné z: http://www.techradar.com/news/internet/web/tor-infinity-and-beyond-everything-you-need-to-know-about-the-dark-web-1311729

[22] KOEBLER, Jason. The Closest Thing to a Map of the Dark Net: Pastebin. In: *Motherboard* [online]. 2015 [cit. 2016-04-15]. Dostupné z: http://motherboard.vice.com/read/the-closest-thing-to-a-map-of-the-dark-net-pastebin

Navzdory těmto skutečnostem se o to pokusila dvojice Daniel Moore a Thomas Rid[23]. Ve své studii se snažili kvantitativně zmapovat zastoupení skrytých služeb v rámci sítě Tor, které manuálně klasifikovali do dvanácti kategorií podle zaměření a obsahu (Tabulka 2).

KATEGORIE	PODROBNOSTI
Zbraně	Obchodování se zbraněmi
Drogy	Prodej nebo výroba nelegálních drog, včetně nezákonně získaného lékařského předpisu
Extremismu	Obsah hlásající extremistické ideologie, včetně ideologických textů, projevů podporujících terorismus, bojové instruktáže a extremistická diskusní fóra
Finance	Praní špinavých peněz, padělání bankovek, obchod s kradenými kartami a účty
Hacking	Nájemné hackerství, obchod nebo distribuce malwaru nebo DDoS
Nelegální pornografie	Pornografický materiál týkající se dětí, násilí, zvířat nebo materiálů získaných bez souhlasu účastníků
Odkazy	Webové stránky zaměřené především na propojení s jinými nelegálními zdroji v rámci Darknetu
Jiná ilegální činnost	Materiály, které nezapadají do žádné z kategorií, ale jsou problematické jako obchodování s falešnými pasy, průkazy a dalším nelegálním zbožím
Sociální	Online komunity sdílející ilegální materiály v podobě diskusních fór nebo sociálních sítí
Násilí	Nájemní vrahové, videa instruující provedení násilného útoku
Jiné	Legální a legitimní obsah s ideologickou nebo politickou náplní, zabezpečené drop-in sítě, informační repositáře
žádné	Webové stránky, které jsou nepřístupné nebo bez viditelného obsahu

Tabulka 2: Kategorizace skrytých služeb podle náplně[24]

Kolik skrytých služeb zastupuje jednotlivé kategorie, znázorňuje následující tabulka (Tabulka 3). Výsledky jsou rovněž pro přehlednost vizualizovány grafem (Graf 3).

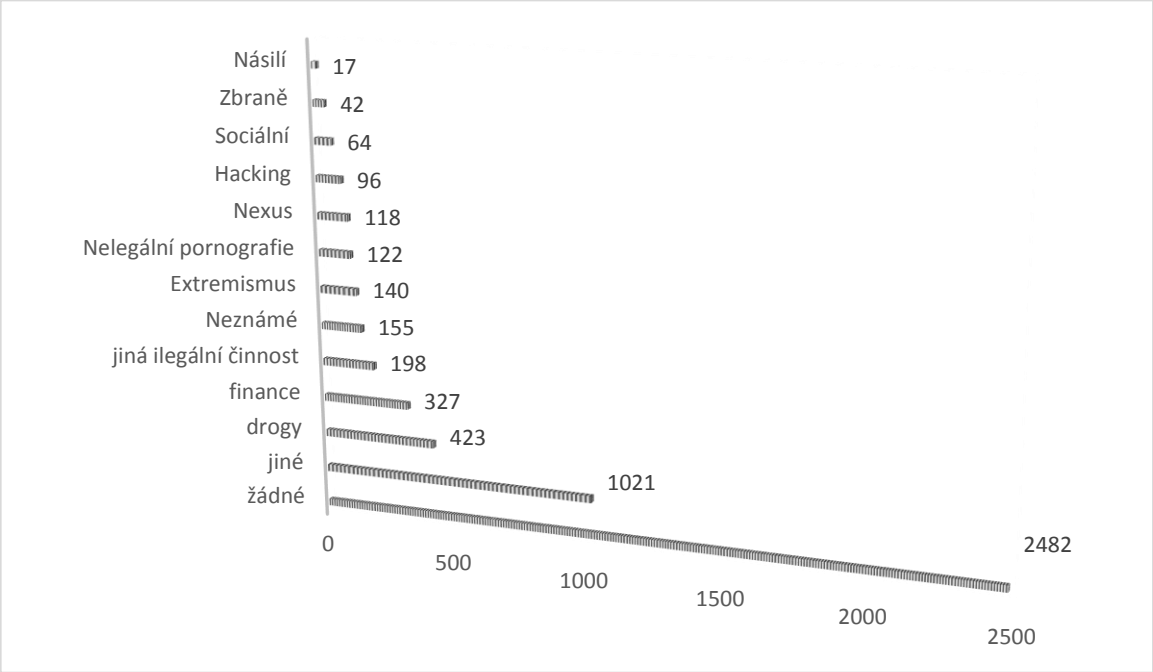
KATEGORIE	POČET SLUŽEB
Žádné	2482
Jiné	1021
Drogy	423
Finance	327
Jiná ilegální činnost	198
Neznámé	155
Extremismus	140
Nelegální pornografie	122
Nexus	118
Hacking	96
Sociální	64

[23] MOORE, Daniel a Thomas RID. Cryptopolitik and the Darknet. *Survival* [online]. 2016, **58**(1), 7-38 [cit. 2016-04-18]. DOI: 10.1080/00396338.2016.1142085. ISSN 0039-6338. Dostupné z: http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085

[24] MOORE, Daniel a Thomas RID. Cryptopolitik and the Darknet. *Survival* [online]. 2016, **58**(1), 7-38 [cit. 2016-04-18]. DOI: 10.1080/00396338.2016.1142085. ISSN 0039-6338. Dostupné z: http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085

Zbraně	42
Násilí	17
Celkem	5205
Celkem aktivních	2723
Celkem nelegálních	1547

Tabulka 3: Zastoupení kategorií počtem stránek[25]



Graf 3: Počet skrytých služeb podle náplně a zaměření, vlastní zpracování

Jak vyplývá z výsledků výzkumu (Tabulka 3, Graf 3), nejběžnější důvod využití skrytých služeb je trestní činnost, týkající se obzvláště financí a ilegální pornografie. Takové výsledky nejsou neočekávané, avšak co autoři výzkumu shledávají pozoruhodnou skutečností, je zanedbatelná, téměř nulová přítomnost islámského extremismu[26]. Na rozdíl od jiných komodit se touto studií, stejně jako žádnou další nepotvrdily domněnky o nájemných vraždách zprostředkovaných touto sítí služeb.

[25] MOORE, Daniel a Thomas RID. Cryptopolitik and the Darknet. *Survival*[online]. 2016, **58**(1), 7-38 [cit. 2016-04-18]. DOI: 10.1080/00396338.2016.1142085. ISSN 0039-6338. Dostupné z: http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085

[26] Nedávné teroristické útoky vyvolaly domněnky o používání sítě Tor teroristy jak pro komunikaci, tak pro možnost anonymních finančních transakcí. Francie zvažovala, spolu s dalšími technologickými opatřeními, zákaz užívání software Tor.
France looking at banning Tor, blocking public Wi-Fi. *Ars Technica* [online]. United Kingdom: WIRED Media, 2016 [cit. 2016-04-20]. Dostupné z: http://arstechnica.com/tech-policy/2015/12/france-looking-at-banning-tor-blocking-public-wi-fi/

Ačkoliv výsledky výzkumu zdánlivě potvrzují slova Juliana Smithe a přizvukují mediálnímu obrazu sítě Tor, taková interpretace by však představovala umné vytržení z kontextu. Skryté služby se totiž na celkovém provozu sítě podílejí zhruba z 5 %.[27] „Většina uživatelů Tor nikdy nenavštívila žádnou stránku s příponou .onion. Většina uživatelů používá software pouze k bezpečnějšímu a anonymnímu prohlížení běžných internetových adres.“[28]

Žurnalista a blogger Jamie Bartett se tématikou Dark webu a především výzkumem jeho online komunit zabývá již delší dobu. Uvědomuje si ilegální aspekty tohoto prostředí, nicméně oceňuje kreativitu a princip fungování zejména obchodu uskutečňovaného prostřednictvím skrytých služeb. Výhledově předpokládá, že se právě pro hodnoty, které anonymita ochraňuje, stane Dark web mainstreamovou záležitostí. „Dark net už není jen doupětem dealerů a úkrytem pro informátory. Už se stává mainstreamovým. (…) Internet bude zase zajímavější, více vzrušující, inovativnější, hrůznější, více destruktivní. Je to dobrá zpráva, pokud vám záleží na svobodě. Je to dobrá zpráva, pokud vám záleží na volnosti. Je to dobrá zpráva, pokud vám záleží na demokracii. Také je to dobrá zpráva, pokud si chcete prohlédnout nezákonnou pornografii a pokud chcete bez postihu nakupovat a prodávat drogy. Ne úplně temný, ne úplně světlý. Nevyhraje ani jedna, ani druhá strana, ale obě dvě.“[29]

2.4. Uživatelé Tor

Uživatelé Tor jsou běžně hromadně označováni za teroristy, drogové dealery, obchodníky se zbraněmi a pedofily. Takový obraz nastínila jednak média, jednak vládní a korporátní organizace, vůči kterým se Tor vyhraňuje. Zcestnost této domněnky bude vyvrácena v následujících řádcích.

[27] State of the Onion [32c3]. In: *Youtube* [online]. 29. 12. 2015 [vid. 2016-02-02]. Kanál uživatele CCCen. Dostupné z: https://www.youtube.com/watch?v=EXEUE__ap08

[28] MOORE, Daniel a Thomas RID. Cryptopolitik and the Darknet. *Survival* [online]. 2016, **58**(1), 7-38 [cit. 2016-04-18]. DOI: 10.1080/00396338.2016.1142085. ISSN 0039-6338. Dostupné z: http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085

[29] How the Mysterious Dark Net Is Going Mainstream. Jamie Bartlett. TED Talks. In: *Youtube* [online]. 24. 9. 2015 [vid. 2016-03-04]. Kanál uživatele TED. Dostupné z: https://www.youtube.com/watch?v=pzN4WGPC4kc

Přímo webové stránky Tor Project představují typologii svých uživatelů rozdělenou do devíti kategorií[30]: normální lidé, žurnalisté a jejich čtenáři, policie, aktivisté a informátoři, veřejné i neveřejné osoby, manažeři, blogeři, armáda, odborníci v oblasti IT.

Jako první jsou zmíněni normální lidé, lépe řečeno běžní uživatelé. Primární pohnutkou vývojářů softwaru Tor, byla ochrana uživatelů před bezohlednými praktikami obchodních korporací, stejně jako ochrana komunikace před nezodpovědnými korporacemi a jejich ledabylému zabezpečení osobních dat uživatelů. Navíc při anonymním pohybu v online prostředí je redukováno riziko odcizení identity a jako užitečný pomocník se projevuje Tor při vyhledávání citlivých informací, ať už se jedná o témata tabuizovaná kulturně, nábožensky či politicky, nebo o údaje, jejichž marketingové využití by mohlo být nepříjemné nebo je nežádané. Početnou množinou z těchto běžných uživatelů jsou pak takoví uživatelé, zabarikádováni národními firewally či stísněni cenzurou. Obecnými pohnutkami vedoucími k instalování Tor jsou v dnešní době primárně snahy limitovat dohled a udržet si určitou míru svého soukromí.

Další kategorie se dotýká žurnalistiky, a to nejen z pohledu aktivních žurnalistů, nýbrž i samotných čtenářů, kteří se tak dostávají k dalším informacím a alternativním výkladům, k názorům protichůdným ke státní propagandě apod. Novináři pak publikují svobodně a bez obav o svou bezpečnost, stejně tak disidenti a blogeři, chráněny jsou i zdroje.

Index svobody světového tisku za rok 2015[31] poukazuje na celkové zhoršení svobody informací v hodnoceném období. Klesající úroveň svobody tisku je zaznamenána na všech kontinentech, nejedná se pouze o válčící státy vedoucí též informační válku, při níž jsou právě média důležitým strategickým cílem, ať už jsou umlčována nebo zneužívána k šíření propagandy. Na znepokojujícím poklesu se podílí i rostoucí hrozba ze strany nevládních organizací, případně jiné faktory, spíše ekonomického rázu. Pohyb žurnalistů na síti Tor je rozhodně opodstatněný, často jde totiž doslova o život.

[30] THE TOR PROJECT. Tor: Anonymity Online [online]. [2012] [cit. 2015-12-29]. Dostupné z: https://www.torproject.org/index.html.en

31 2016 World Press Freedom Index: a "deep and disturbing" decline in media freedom. In: *Reporters without borders: for freedom of information* [online]. France: Reporters without borders, 2016 [cit. 2016-04-26]. Dostupné z: https://rsf.org/en/reports/2016-world-press-freedom-index-deep-and-disturbing-decline-media-freedom

A právě neustálá přítomnost takového rizika legitimuje anonymitu, v našem případě anonymitu pohybu v síti Tor. Pavla Holcová, zakladatelka Českého centra pro investigativní žurnalistiku (CCIZ), které úzce spolupracuje s Organized Crime and Corruption Reporting Project (OCCRP), považuje Tor společně s TrueCrypt za nejspolehlivější softwarová řešení[32].

Represivním složkám státu ulehčí Tor práci v případech tajných operací, při vyšetřování a odhalování zločinu, aniž by bylo potřeba zanechávat stopy, které by takovou práci mohly znemožňovat.

Mýtus týkající se uživatelů Tor představuje domněnka, že software oslovuje sofistikovanější uživatele Internetu. Od uživatelů softwaru není předpokládána žádná výraznější technická. Uživatele lze označit za sofistikovanější ve smyslu pokročilé uvědomělosti znepokojujícího sběru dat korporacemi i vládou.

3. Další projekty

Členové Tor Project se podílí na dalších projektech, které vylepšují nebo rozšiřují stávající software. TAILS, Orbot a Tor Messenger patří k těm funkčním a mezi uživateli nejrozšířenějším.

TAILS, akronym The Amnesic Incognito Live System, představuje, jak vyplývá z názvu, živý operační systém, který lze spustit na jakémkoliv počítači z DVD, USB nebo SD karty bez zanechání digitální stopy na zařízení. Tor Projekt vývoj tohoto operačního systému založeného na Debian GNU/Linux podporoval především finančně.

Obrázek 10: Logo Tails[33]

32 STROUHAL, Lukáš. Blok expertů | Rozhovor s Pavlou Holcovou. In: *Inflow: information journal* [online]. Brno: Kabinet informačních studií a knihovnictví, 2013 [cit. 2016-04-26]. Dostupné z: http://www.inflow.cz/blok-expertu-rozhovor-s-pavlou-holcovou

33 Tails: theamnesicincognitolivesystem [online]. [2015] [cit. 2016-04-22]. Dostupné z: https://tails.boum.org/news/and_the_winner_is/index.en.html

Orbot je projekt, který vznikl ve spolupráci Tor Project s The Guardian Project. Jedná se o svobodný software a otevřenou síť uzpůsobenou pro mobilní telefony s operačním systémem Android. Funkčnost systému je opět založená na budování proxy, prostřednictvím kterých je v síti Tor směrován datový tok. K dispozici je několik již nakonfigurovaných aplikací použitelných skrz Orbot, avšak většinu aplikací je potřeba nakonfigurovat manuálně.

Obrázek 11: Logo Orbot[34]

Tor Messenger je multi-platformní chatovací program, jehož provoz je kvůli zajištění bezpečnosti zase směrován přes Tor. Snadno použitelné uživatelské rozhraní v několika jazycích podporuje Jabber, Google Talk, Twitter a další komunikační služby.

Obrázek 12: Logo Tor Messenger[35]

[34] THE TOR PROJECT. Tor: Anonymity Online [online]. [2012] [cit. 2016-04-22]. Dostupné z: https://www.torproject.org/index.html.en

[35] THE TOR PROJECT. Tor: Anonymity Online [online]. [2012] [cit. 2016-04-22]. Dostupné z: https://www.torproject.org/index.html.en

III. ANONYMITA

V tomto oddíle bude nejprve nastíněn koncept anonymity v reálném světě i v online prostředí. V krátkosti bude představeno hnutí Cypherpunk, které, navzdory nespornému přínosu v oblasti informačních technologií, není v českém prostředí příliš známé. Následující kapitoly se budou problematikou zaobírat z pohledu teorie bezpečnosti systému, budou představeny snahy anonymitu změřit a na aspekty anonymity bude nahlédnuto rovněž optikou psychologie, která vyvrátí několik mýtů o chování uživatelů vystupujících v anonymitě.

4. Fenomén anonymity

Pojem anonymita[36] má kořeny v řeckém slově *anonymia*, které odpovídá významu *beze jména*, či *bezejmenný*. Dějinné ukotvení anonymity coby jakéhosi stavu, respektive možnosti pohybu bez prokázané identity, rozděluje veřejnost do dvou skupin. Jedni označují anonymitu za zbrusu nový fenomén, který se objevil až s příchodem Internetu, jiní, ačkoliv mnohdy zaměňujíce anonymitu s pseudonymitou, dokládají její přítomnost v dějinách konkrétními příklady. Za takové doklady považují jeskynní malby pravěkých lidí, hieroglyfy nebo samotnou Bibli. „Anonymní pamflety, letáky, brožury a dokonce knihy hrály důležitou roli ve vývoji lidstva.“[37] Běžnější praktikou však bylo používání pseudonymů.

Anonymita začala prosakovat do veřejné diskuze nejdříve spíše v politickém kontextu. Kupříkladu v 50. letech jurisdikce prosazovala právo NAACP (Národní asociace pro podporu barevných lidí) seznamy svých členů nezveřejňovat, toto utajení platilo i před státem a jeho zástupci. Klíčový okamžik v konceptu anonymity se však odehrál ještě později a nese označení McIntyre vs. Volební komise v Ohiu.

McIntyre vs. volební komise v Ohiu je soudní spor z roku 1994, na jehož základě došlo k anulaci právního předpisu zakazujícího anonymní literaturu podporující politickou kampaň. Na pozadí události, kdy Margaret McIntyre byla uložena pokuta místní školní radou kvůli rozdávání letáků stavějících se proti návrhu plánovaného školného v průběhu její kampaně. Tyto letáky totiž nenesly žádné údaje identifikující jejich vydavatele, neuváděly ani jiné jméno

[36] Pseudonymita se zakládá na řeckém *pseudonumom* znamenající falešně pojmenovaný.

[37] WALLACE, Jonathan D. *Nameless in cyberspace: Anonymity on the internet*. Cato Institute, 1999. Dostupné z: http://object.cato.org/sites/cato.org/files/pubs/pdf/bp54.pdf

či adresu. Hovoříme tedy o anonymitě a taková anonymní literatura byla státem Ohio považována za protiústavní. Tento spor vyvolal střet názorů jednotlivých soudců, jelikož takové právní nařízení samo o sobě odporuje Ústavě. Ke zrušení zákazu došlo v roce 1995, přičemž soud své rozhodnutí ukotvil na několika pilířích obhajujících anonymitu projevu. V zásadě se jednalo o tyto tři důvody[38]: zvýšení autority, podpora otevřené debaty a bezpečí před odplatou. „Na základě naší Ústavy, anonymní pamfletování (tedy rozšiřování nových nebo kontroverzních myšlenek prostřednictvím distribuce levných a snadno vyrobených letáků a brožur[39]) není škodlivou, podvodnou praktikou, nýbrž čestnou tradicí v naší obhajobě a nesouhlasu. Anonymita je štítem před tyranií většiny.“[40]

Jonathan Wallace, právník a vydavatel měsíčníku Ethical Spectacle, nachází paralelu mezi letáky paní McIntyer a dnešními nepodepsanými příspěvky na webu. „Přesto však lidé, kteří nedokážou vidět analogii mezi Internetem a tištěnými médii, nadále požadují zákaz anonymity v kyberprostoru.“[41]

5. Online anonymita

Východiskem pro tuto kapitolu bude anonymita chápána ve smyslu nemožnosti identifikovat uživatele určité online aktivity. Na tomto místě je vhodné připomenout původní záměr tvůrců Internetu, který neoperoval s představou implementace jeho sítě do komerčního prostředí, nemluvě o vidině jeho zpřístupnění široké veřejnosti.

Původní „Internet“ představoval síť vytvořenou za účelem přenosu a výměny dat mezi vzdálenými počítači, přístup k ní byl navíc podmíněn autentizací pomocí přihlašovacích údajů, které nebyly nutně jednoznačně identifikační. První komerční služby se na síti objevují v roce 1985, dva roky před vznikem samotného pojmu „Internet“, avšak v této době se o anonymitě ještě nehovoří, ačkoliv od 80. let již známe pojem tzv. digitálních stop. Rok 1992 je považován

[38] MCINTYRE v. OHIO ELECTIONS COMM'N. *FindLaw: For Legal Professionals* [online]. Minnesota: Thomson Reuters, 2016 [cit. 2016-02-02]. Dostupné z: http://caselaw.findlaw.com/us-supreme-court/514/334.html

[39] Pamphleteering. *Encyclopedia.com* [online]. United Kingdom: Cengage Learning, 2016 [cit. 2016-02-02]. Dostupné z: http://www.encyclopedia.com/doc/1G2-3401803143.html

[40] MCINTYRE v. OHIO ELECTIONS COMM'N. *FindLaw: For Legal Professionals* [online]. Minnesota: Thomson Reuters, 2016 [cit. 2016-02-02]. Dostupné z: http://caselaw.findlaw.com/us-supreme-court/514/334.html

[41] WALLACE, Jonathan D. *Nameless in cyberspace: Anonymity on the internet*. Cato Institute, 1999. Dostupné z: http://object.cato.org/sites/cato.org/files/pubs/pdf/bp54.pdf

za vstup vládních institucí na Internet, avšak ani připojení Bílého domu k síti nijak neodkazuje k uživatelské potřebě být anonymní.

Klíčový okamžik representuje spíše následující nástup rozsáhle komercionalizace, jež vyžadovala určitou autentizaci uživatelů. Se sílícím sociálním aspektem Internetu, na kterém se podílel vznik diskusních fór nebo e-mailových schránek, pak stoupala i úroveň a potřeba identifikace. Stručně řečeno, diskusní fóra, zpravodajské stránky a další byly financovány převážně reklamou, a proto bylo žádoucí identifikovat a spočítat návštěvníky stránky pro představu, jaký typ obsahu a další faktory se podílejí na návštěvnosti té konkrétní stránky. S hypotézou úbytku uživatelské návštěvnosti v případě vyžadování provedení autentizace jimi samotnými, bylo nutné najít alternativní, automatický způsob, což zformovalo poptávku po identifikačních technologiích. Právě propojení komerčního aspektu s tím sociálním načrtlo hrubé obrysy konceptu anonymity v tom dnešním slova smyslu, tedy nemožnosti přiřadit aktivitu subjektu v systému ke konkrétní totožnosti uživatele či skupiny uživatelů.

Na základě těchto zběžných exkurzí je možné vypozorovat nemalý časový rozestup mezi vznikem konceptu anonymity v reálném světě a v tom virtuálním. Ovšem na rozdíl od koncepce reálné anonymity, náčrtek té virtuální v dnešní době stále pozbývá konečné, ucelené formy. Naopak lze předpokládat, že do něj v příštích letech významným způsobem zasáhne očekávaný Internet věcí. Proto, vycházejíce z neúplnosti konceptu online anonymity, je příhodné o ní hovořit vždy v kontextu konkrétní operace, tj. anonymita odesílatele dat, anonymita příjemce dat, anonymita provozovatele webu apod.

5.1. Cypherpunk

První diskuze zabývající se online anonymitou se pravděpodobně odehrávaly v úzkém diskuzním kruhu, později známém jako hnutí Cypherpunk. Tato neformální skupinu aktivistů sestávala z obhájců proaktivního používání kryptografie s cílem dosáhnout bezpečnosti a ochránit své soukromí.

Kořeny cypherpunku sahají do pozdních 80. let, autorkou označení byla Jude Milhon, hackerka a jedna ze zakládajících členu tohoto hnutí. V roce 2006 byl dokonce termín zařazen do oxfordského slovníku angličtiny. Technickou základnu hnutí představuje článek Davida Chauma „Security without Identification: Transaction Systems to make Big Brother

Obsolete“[42]. Základní ideje jsou pak shrnuty v manifestu Cypherpunku, sepsaného roku 1993 Ericem Hughesem. „Soukromí je nezbytné pro otevřenou společnost v elektronické době…nemůžeme očekávat, že vlády, korporace nebo další rozsáhle organizace bez tváře nám budou dopřávat soukromí.“[43]

Původně se komunikace mezi jednotlivými členy odehrávala prostřednictvím elektronického mailing listu, který se stal záhy živým diskusním fórem, kde probíhaly debaty nejen o matematice, kryptografii či počítačově vědě, ale probíraly se i filosofické a politické otázky. Problematika soukromí a anonymity se začala projednávat v reakci na šifrovací algoritmus Skipjack, který odstartoval jakési monitorování komunikace vládními institucemi. Intenzita debat na témata jako soukromí v komunikaci a data retention zesílila. „Možnost anonymního projevu a publikování je nepochybně životně důležitá pro otevřenou společnost, esenciálním požadavkem skutečné svobody projevu.“[44]

Členové hnutí jsou často výraznými osobnostmi počítačového průmyslu. Součástí hnutí je tak např. Jacob Appelbaum, vývojář Tor, zakladatel WikiLeaks Julian Assange, Werner Koch (GNU Privacy Guard) nebo Johan Helsingius (Penet Remailer). Taková účast předpokládá spolupráci organizace na různých projektech, mimo jiné se skupina Cyphropunk podílela i na vývoji softwaru Tor.

6. Anonymita z technického hlediska

Tato kapitola se věnuje teorii z oblasti bezpečnosti. Bezpečnost systému zajišťují tyto jeho čtyři vlastnosti; anonymita, pseudonymita, nespojitelnost a nepozorovatelnost, které jsou v následujícím textu definovány, aby nedocházelo k jejich záměně.

„*Anonymita je vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb bez zjištění identity uživatele tohoto systému*.“[45] Anonymita představuje stav, kdy za žádných okolností

[42] CHAUM, David. Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM* [online].**28**(10), 1030-1044 [cit. 2016-02-06]. DOI: 10.1145/4372.4373. ISSN 00010782. Dostupné z: http://portal.acm.org/citation.cfm?doid=4372.4373

[43] HUGHES, Eric. A Cypherpunk's Manifesto (1993). Dostupné z: http://www.activism.net/cypherpunk/manifesto.html

[44] CROFTON, Isaak. *Crypto Anarchy*. 1. United States: Lulu.com, 2015. ISBN 1329059808.

[45] MATYÁŠ, Václav. Ochrana dat a informačního soukromí. (přednáška) Brno: Masarykova univerzita, 14. 9. 2014.

není možné identifikovat subjekt v rámci množiny všech uvažovaných subjektů (anonymitní množina). Dochází k naprostému odstranění všech identifikačních informací daného subjektu. Jedná se o ochranu identity uživatelů, nikoliv ochranu identity subjektů v systému.

Pseudonymitou označujeme „v*lastnost systému, který zajišťuje možnost použití zdrojů nebo služeb bez zjištění identity uživatele tohoto systému tak, že uživatel je stále zodpovědný za toto použití.*“[46] Uživatel může použít zdroj nebo službu bez nutnosti odhalení své uživatelské identity, nutnost odhalení identity stanovuje překročení určité hranice. Tu nejčastěji představují pravidla toho konkrétního systému. Pokud uživatel respektuje stanovená pravidla, pak má administrátor malou motivaci odhalit jeho identitu. V případě, kdy dojde k porušení těchto pravidel, může administrátor zjistit podrobnosti týkající se pseudonymu a jeho chování, což může vést k odhalení identity uživatele. K odhalení identity pseudonymu může dojít rovněž na základě nařízení orgánu činného v trestním řízení. Tato vlastnost je též často označována jako částečná anonymita.

Nespojitelnost (*unlinkability*) jako další bezpečnostní funkce představuje „*vlastnost systému, který zajišťuje možnost opakovaného použití zdrojů nebo služeb s tím, že ostatní si tato použití nebudou schopni spojit.*“[47] Takovým spojením chápeme vzájemnou souvislost, která nastává v případě služeb poskytovaných postupně i současně. Úkolem této funkce je zajištění možnosti použít zdroj opakovaně, aniž by byla prozrazena identita uživatele a odhalena jeho spojitost s užívanými zdroji.

Poslední z bezpečnostních funkcí systému je označována jako tzv. nepozorovatelnost (*unobservality*). Nepozorovatelnost „*zajišťuje možnost použití zdrojů nebo služeb tak, že ostatní nemohou pozorovat používání daného zdroje nebo služeb.*“[48] Na tuto vlastnost lze nazírat ze dvou pohledů. Jednak se jedná o vlastnost zaručující anonymitu subjektu, který určitý zdroj či službu využívá, a to nejen vůči pozorovatelům zvnějšku, nýbrž i vůči subjektům využívající rovněž tyto zdroje a služby. Jednak lze vlastnost nepozorovatelnosti vnímat jako záruku znemožnění detekce využívání daného zdroje nebo služby vůči takovým subjektům, které dané zdroje nepoužívají. Tato bezpečnostní funkce je specifická z hlediska hodnot, které ochraňuje. V tomto případě v ohnisku zájmu nejsou informace o uživatelích, tím chráněným jsou

[46] MATYÁŠ, Václav. Ochrana dat a informačního soukromí. (přednáška) Brno: Masarykova univerzita, 14. 9. 2014.

[47] Tamtéž.

[48] Tamtéž.

informace o využívání zdrojů a služeb. Takové vlastnosti je příhodné využít např. k ochraně proti tzv. analýze provozu (*traffic analysis*).

Pro běžnou praxi se užívá nejčastěji pseudonymity. Ačkoliv je anonymita označovaná za extrémní situaci, právě ta je stěžejní pro tuto práci. Na všechny výše zmíněné bezpečnostní funkce lze nahlížet z pohledu dvou různých směrů.

Prvním z nich je systém tzv. mixů, pojem zavedený Davidem Chaumem v 80. letech minulého století. V takovém prostředí anonymita zastupuje stav bytí neidentifikovatelným v kontextu tzv. anonymitní množiny, jíž je rozuměna množina všech takových subjektů, jež mohou být považováni za potencionální komunikační aktéry, tedy odesílatele nebo příjemce. O anonymitě subjektů hovoříme výhradně ve spojení s touto množinou, velikost množiny se používá coby metrika hodnotící míru poskytované anonymity.

Druhý možný směr nazírání na bezpečnostní funkce systému je poskytován mezinárodně významným standardem označovaným jako Společná kritéria pro hodnocení bezpečnosti, zkráceně Společná kritéria (Common Criteria for Information Technology Security Evaluation). Tento světový standard zprostředkovává hodnocení bezpečnosti systémů, srovnává je na základě specifikací požadované funkčnosti, přičemž zohledňuje velké množství aspektů, jakými jsou důvěryhodnost stanovené cesty, bezpečnost interface nebo zvolená kryptografie.

V případě anonymity je důležité zdůraznit, že standard Společných kritérií nahlíží na tuto vlastnost jako na ochranu identity uživatelů, nikoliv jako ochranu identity subjektů v systému. Úroveň anonymity pak v tomto případě reprezentuje stav, kdy specifikované entity, tedy běžní uživatelé systému, nedokážou určit souvislost mezi skutečné uživatelským jménem a specifikovanými objekty a operacemi v systému. Podúroveň představuje množina jakýchsi privilegovaných, specifikovaných subjektů, která používá specifikované služby bez toho, aby byly zjišťovány informace o jejich spojení s konkrétním uživatelem systému.

Standard Společných kritérií je mnohdy ohniskem kritiky z důvodu jakéhosi existenciálního charakteru jeho pohledu na problematiku bezpečnosti, přesněji řečeno pro skutečnost, že standard umožňuje pouze hodnocení ano/ne. Pro tuto práci je nicméně výstižnější první ze zmíněných možností náhledu na bezpečnostní funkce systému, tedy zařazení anonymity do kontextu anonymitní množiny, čehož je využíváno primárně pro měření anonymity, kterému se věnuje následující kapitola.

7. Měření anonymity

Používání nástrojů pro anonymní komunikaci na Internetu v běžné praxi odkrylo nedostatky hodnocení anonymity z pohledu Společných kritérií, tedy hodnocení ve smyslu 0 a 1, neboli ano/ne hodnocení, neboť dostatečně nezohledňuje jednotlivé aspekty podílející se na konečné anonymitě, což může vést k zavádějícím výsledkům. V současnosti není tvrzení, zda anonymity dosaženo je či není, dostačující, nýbrž je poptáváno kvantitativní hodnocení. Taková standardizovaná metrika je užitečná zejména pro uživatele jako projev míry garance systému poskytujícího anonymitu.

V této kapitole bude uveden přehled základních metrik užívaných pro měření anonymity. Některé z nich jsou sice již překonány, nicméně doposud slouží jako stavební kámen, nebo alespoň jako inspirace vedoucí k dalším způsobům měření.

Následující koncepty se zaobírají anonymitou spojení, nikoliv anonymitou přenášených dat. Měření takové anonymity analyzoval Oliver Berthold[49], který nahlíží na míru anonymity z hlediska odolávání několika typů útoků zaměřených na odkrytí obsahu posílaných zpráv, mimo jiné pracoval zejména na vývoji spolehlivých a důvěryhodných mechanismů pro vizualizaci úrovně anonymity. Ve své práci Berthold vždy zdůrazňuje potřebu uživatele být informován o míře anonymity, a tak i úrovně své ochrany při vyhledávání konkrétního obsahu na Internetu.

Všeobecně známou metrikou je bezesporu velikost anonymitní množiny (*anonymity set size)*. Anonymitní množina představuje souhrn všech subjektů potencionálně způsobilých vykazovat v rámci komunikace aktivitu, a to buď v roli odesílatele zprávy, nebo v roli jejího příjemce. Klíčový je předpoklad rovnoměrného pravděpodobnostního rozložení aktivity mezi všechny tyto subjekty, pak velikost anonymitní množiny koreluje s mírou anonymit. Takový vztah lze vyjádřit lomenou funkcí. Míra anonymity se v takovém případě může v průběhu času měnit právě v důsledku změny velikosti anonymitní množiny.

[49] BERTHOLD, Oliver, Hannes FEDERRATH a Marit KÖHNTOPP. Project "anonymity and unobservability in the Internet". In: *Proceedings of the tenth conference on Computers, freedom and privacy challenging the assumptions - CFP '00* [online]. New York, New York, USA: ACM Press, 2000, s. 57-65 [cit. 2016-03-27]. DOI: 10.1145/332186.332211. ISBN 1581132565. Dostupné z: http://portal.acm.org/citation.cfm?doid=332186.332211

Avšak předpoklad stejné míry pravděpodobnosti každého jednoho subjektu množiny je funkční pouze v teoretickém systému. Měření založené na velikosti anonymitní množiny je proto nespolehlivé a zavádějící, navzdory tomu je tato metrika stále užívanou, a to zejména pro získání jakési hrubé představy o síle anonymity nabízené systémem.

Využití Shannonovy teorie entropie coby další metriky vyjadřující míru anonymity navrhla dvojice Serjantov a Danezis[50], přičemž míra anonymity poskytované systémem se odvíjí od rozsahu nejistoty, vztažené k potencionální aktivitě účastníků systému a jejich účasti na komunikaci. Technickým problémem je i u této metriky rozdělení pravděpodobnosti[51].

Crowds-based metric[52] neboli metrika založená na systému Crowds, avšak využívána i v kontextu jiných systémů, vytvořili Reiter a Rubin přidáním třetího aspektu anonymní komunikace ke dvěma již stávajícím (prvním aspektem je anonymita z pohledu účastníků komunikace, druhým je pak pohled útočníka), a to tzv. stupeň anonymity (*degree of anonymity*). Přicházejí s modelem zobrazující anonymitu coby kontinuum (*informal continuum*), tedy spektrum nabývající hodnot od nulové anonymity až po anonymitu komplexní, přičemž se mezi těmito dvěma extrémy nachází několik dalších mezistavů. Posloupnost stupňů anonymity je následující; absolutní soukromí (*absolute privacy*), mimo podezření (*beyond suspicious*), pravděpodobná nevina (*probable innocence*), možná nevina (*possible innocence*), odhalený (*exposed*) až prokazatelné odhalený (*provably exposed*).

Jak již vyplývá z předchozího textu, metrika zakládající se na anonymitní množině není dostačující, a proto se nemalá pozornost obracela na vhodné rozšiřování tohoto konceptu. Rozdělení pravděpodobnosti aktivity účastníků anonymní komunikace se ukázalo být nevyhnutelným kritériem pro prakticky veškeré metriky usilující o kvantitativní vyjádření míry anonymity.

---

[50] COBLE, Aaron Richard. *Anonymity, information, and machine-assisted proof*. 2010. PhD Thesis. University of Cambridge.

[51] BEZZI, Michele. An entropy based method for measuring anonymity. In:*Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*. IEEE, 2007. p. 28-32.

[52] REITER, Michael K. a Aviel D. RUBIN. Crowds: anonymity for Web transactions. *ACM Transactions on Information and System Security* [online]. **1**(1), 66-92 [cit. 2016-03-27]. DOI: 10.1145/290163.290168. ISSN 10949224. Dostupné z: http://portal.acm.org/citation.cfm?doid=290163.290168

Obeznámeni s nutností této predispozice Rein Lundin a Christer Andersson[53] pracovali na vytvoření nového měřítka. Jejich práce zohledňuje množství dosavadně užívaných metrik a na tomto základě je následně vypracován koncept souboru kritérií, který by měla vhodná a spolehlivá metrika pro měření anonymity splňovat. Výstupem je návrh metriky odpovídající těmto požadavkům, kterou označili jako the scaled anonymity set size[54] (český ekvivalent by odpovídal škálovatelné velikosti anonymitní množiny).

V prvním kroku byl sestaven vzorek užívaných metrik, jejich prostudováním byl zhotoven výčet předpokladů (kritérií K) zaručujících funkčnost a spolehlivost měření.

K1 – Anonymitní metrika by měla být založena na pravděpodobnostní analýze

K2 – Anonymitní metrika musí mít jasně definované zakončení

K3 – Čím rovnoměrnější je distribuce pravděpodobnosti, tím vyšší je stupeň anonymity

K4 – Čím je větší počet uživatelů v anonymitní množině, tím vyšší je stupeň anonymity

K5 – Prvky definičního oboru hodnotící metriky musí být jasně definovány

K6 – Definiční obor metriky by měl být uspořádaný a nepříliš přibližný

Tato kritéria byla nejdříve zhodnocena každou metrikou zvlášť. Výsledky, nakolik jednotlivé metriky zohledňují stanová kritéria, znázorňuje Tabulka 4.

	K1	K2	K3	K4	K5	K6
Anonymity Set	-	-	-	+	+	+
Crowds-based metric	+	+	-	+	+	-
Entropy-based (Diaz)	+	+	+	-	+	+
Entropy-based (Serjantov, Danezis)	+	-	+	+	+	+
Source-hiding property	+	-	-	+	+	+

Tabulka 4: Evaluace metrik podle stanovených kritérií[55]

Jak vyplývá z tabulky, žádná z metrik bezvýhradně nesplňuje všechna kritéria, vycházeje z těchto poznatků, je navržena nová metrika, spojující především teorie založené na entropii s velikostí anonymitní množiny. Otestováním nové měřící metody pomocí čtyř scénářů, které

[53] ANDERSSON, Christer a Reine LUNDIN. On the Fundamentals of Anonymity Metrics. *The Future of Identity in the Information Society* [online]. Boston, MA: Springer US, 2008, s. 325 [cit. 2016-03-27]. DOI: 10.1007/978-0-387-79026-8_23. ISBN 978-1-4419-4629-4. Dostupné z: http://link.springer.com/10.1007/978-0-387-79026-8_23

[54] Tamtéž.

[55] Tamtéž.

byly použity i pro fázi sestavování kritérií, se ukázalo, že teoretický model pak skutečně naplňuje požadavky stanovené sadou kritérií.

Další nutný aspekt zohledňující tvorbu takové metriky představil Steven Murdoch ve své studii Quantifying and Measuring Anonymity[56], kde se zabývá možnostmi kvantifikace anonymity, přičemž zdůrazňuje roli útočníka, jeho strategii a znalosti systému a provozu v něm. Do této doby byl útočník považován víceméně za kritérium kvalitativního měření anonymity.

Měření anonymity a hledání vhodné metriky je živé téma netriviální povahy, obzvláště z hlediska přibývajících útoků na takové systémy a pestrostí palety jejich vlastností. S neustále se zlepšujícími znalostmi a vybaveností útočníků je důležitost takové metriky, dostatečně spolehlivé a zohledňující co největší množství aspektů, zjevná.

7.1. Míra anonymity poskytovaná Tor

Nehledě na výše zmíněné výtky vůči anonymitní množině, jedná se o pořád výrazný až klíčový aspekt hodnocení míry anonymity poskytované Tor. A právě s ohledem na výhrady této metriky, je pochopitelná neustálá snaha zapojovat do sítě Tor více uživatelů Internetu. To se odráží i na rostoucím počtu služeb, které software nabízí. Zvýšení frekvence uživatelské aktivity v síti by mělo pozitivní dopad jednak na rychlost provozu, jednak na stabilitu a míru poskytované anonymity.

Ojedinělou studií, co se týká měření anonymity, je analýza Towards measuring anonymity[57], kde je míra anonymity, poskytovaná mechanismem onion routing, zkoumána a následně srovnávána se systémem Crowds – zde je měření prováděno na základě anonymitní množiny, avšak bere v potaz rovněž rozdělení pravděpodobnosti aktivity účastníků komunikace, v tomto případě konkrétně odesílatele. Toto měření zohledňuje skutečnost, že informaci o pravděpodobnosti provedení určité operace dokáže odposlechem komunikace získat i útočník. Této metrika je vhodná především pro takové systémy, které jsou častým terčem nejrůznějších útoků.

[56] MURDOCH, Steven J. Quantifying and measuring anonymity. In: *Data Privacy Management and Autonomous Spontaneous Security*. Springer Berlin Heidelberg, 2014. p. 3-13.

[57] EDITED BY ROGER DINGLEDINE, Paul Syverson. *Privacy Enhancing Technologies Second International Workshop, PET 2002 San Francisco, CA, USA, April 1415, 2002 Revised Papers* [online]. 1. Berlin: Springer-Verlag Berlin Heidelberg, 2003 [cit. 2016-03-30]. ISBN 978-354-0364-672. Dostupné z: http://bit.ly/1S2FI3r

Každopádně k dispozici není žádná další studie zabývající se kvantitativním měřením anonymity poskytované ať už přímo softwarem Tor nebo konceptem oinon routing. Veškerá hodnocení vychází z kvalitativního a spíše vágního porovnávání. V tomto ohledu tedy sklouzneme k posouzení anonymity zprostředkovaný softwarem Tor jako dostatečné. Ve srovnání s ostatními způsoby umožňující anonymní pohyb uživatele na síti disponuje několika přednostmi, které jsme si zmínili v první kapitole u popisu Tor.

8. Psychologický aspekt anonymity

Internetová anonymity, zvláště pak anonymní online komunikace, s sebou strhla zájem především ze strany psychologie. V hojném zastoupení byly publikovány práce zaměřené především na vliv anonymity na uživatelské chování v digitálním světě. Sumativní evaluaci vypozorovaných jevů bychom mohli shrnout do následujících třech bodů, představujících tři aspekty vykazující chování jednotlivce v anonymitě, a to; minimalizace zodpovědnosti, uvolnění zábran a depersonalizace. Tyto aspekty jsou ve své podstatě neutrální, hodnot nabývají až uvedením do odpovídajícího kontextu. „Anonymita (…) je společensky zprostředkována a tak variabilní jako bezpočet sociálních kontextů, do kterých může být zasazena.“[58]

Vyhlídka na minimální zodpovědnosti může na jedné straně pokoušet k trestné činnosti, na straně druhé dovede stejně tak povzbuzovat uživatele k vyjádření svého názoru, prozkoumání nových myšlenek apod.

Chování bez zábran, neboli disinhibice, byla psychology poprvé zaznamenána v 80. letech při zkoumání verbálních vyjádření v průběhu elektronické komunikace. Takové chování je zapříčiněno zpravidla zanedbatelnou mírou reflexe sociálních norem v tomto typu komunikace. Chování tak není limitováno úzkostí, rozpačitostí či dalšími obavami, což může na jedné straně vyústit k agresivitě, v rámci diskuzí, třeba k šíření nenávisti, avšak tyto aspekty mohou v důsledku nabývat prosociálního charakteru, např. ke snadnějším navazováním vztahů.

[58] Gardner, James A., *Anonymity and Democratic Citizenship* (January 1, 2011). William & Mary Bill of Rights, Vol. 19; Buffalo Legal Studies Research Paper No. 2011-008. Available at SSRN: http://ssrn.com/abstract=1743742

Depersonalizaci chápeme optikou modelu SIDE[59] (Social Identity Explanation of Deindividuation EffectsDepersonalizaci) coby oslabení vnímání osobního-já a zároveň aktivaci sociální identity, pročež je následné chování regulováno normami uznávanými skupinou. „Anonymita slouží k posílení dopadu sociálních norem, když je osobní identita výrazná, ale je-li osobní identita výrazná, tatáž anonymita redukuje dopad sociálních norem a zvyšuje u osob věrnost k osobním normám.“[60] Tohoto aspektu je využíváno zejména v politice.

Ačkoliv je anonymitě vytýkán její domnělý anti-sociální charakter, ve skutečnosti vykazuje blahodárný psychologický efekt jakéhosi emocionálního sdílení, snad pocitu sounáležitosti, kterého lze za určitých okolností dosáhnout pouze prostřednictvím bezejmennosti. Ilustrativním příkladem je využívání anonymity při rekonvalescenci z prožitých traumat. Neboť „nejzranitelnější lidé jsou nejvíce ohroženi identifikací“[61]

Běžnou hypotézou kolující veřejností je představa o využití anonymity online uživateli za účelem lži, podvodu nebo dezinterpretace. Nicméně výsledky konkrétních výzkumů odhalily přesný opak této domněnky, ve skutečnosti jsou lidé v anonymitě sdílnější a ve svém jednání i přímější a upřímnější.

[59] LEA, M., R. SPEARS a D. DE GROOT. Knowing Me, Knowing You: Anonymity Effects on Social Identity Processes within Groups. *Personality and Social Psychology Bulletin* [online]. 2001, **27**(5), 526-537 [cit. 2016-03-15]. DOI: 10.1177/0146167201275002. ISSN 0146-1672. Dostupné z: http://psp.sagepub.com/cgi/doi/10.1177/0146167201275002

[60] Adam N . Joinson, Se lf-Disclosure in C omputer-Media ted Communication: The Ro le of SelfAwareness and Visual Anonymity, 31 Eur. J. Soc. Psych. 177 (2001).

[61] BODLE, Robert. The ethics of online anonymity or Zuckerberg vs. Moot. *ACM SIGCAS Computers and Society*, 2013, 43.1: 22-35.

IV. ETICKÉ ASPEKTY

Následující oddíl se zabývá etickými aspekty užívání softwaru Tor, potažmo etiku online anonymity. Mediální obraz anonymizérů, zejména však technologie Tor, je výrazně negativní.[62] Tor je uváděn téměř výhradně v souvislostech ilegální činností.

Obecně převládajícím přesvědčením ve společnosti je mylný dojem o nemožnosti vyřešit ilegální činnost páchanou prostřednictvím sítě Tor. Andre Lewman, tehdejší výkonný ředitel Tor Project, na obhajobu prozradil, že se naopak s policií snaží spolupracovat. Zároveň dodává, že za používáním Tor stojí vždy člověk. Lidský faktor představuje co do zranitelnosti nejslabší prvek systému. Adrian Crenshaw[63] ve svém příspěvku na 22. ročníku hackerské konference DEFCON představil čtyři konkrétní kauzy, kdy uživatelé využili Tor k nelegální činnosti a byli později dopadeni právě na základě vlastních chyb.

V každém případě nelze dvojsečnost tohoto softwaru popírat, nicméně v tomto případě se jedná o přehnanou démonizaci. V následujícím textu bude, s přihlédnutím k odpovídající legislativě, posuzováno, nakolik je užívání anonymizující technologie etické podle předem stanovených kritérií, které budou vymezeny v úvodu oddílu.

Vnímání anonymity v online prostředí je rovněž rozpačité, kontroverzní názory vzbuzuje např. téma anonymity přispěvatelů do diskuzních fór. Jedním z nejvýraznějších problémů informační společnosti je ochrana soukromí, neboť často koliduje s informačními potřebami státu a dalších institucí. Motivace pro anonymitu zůstává v průběhu času téměř neměnná, nyní je však obohacená o důvod obavy z všudypřítomného vládního nebo korporátního dohledu, jehož rozsah nemá v dějinách obdoby. Pochopitelně pokusy o hromadný dohled nad lidmi byly, nicméně díky vysokému stupni vývoje technologií dosahuje v současnosti takový dohled svého vrcholu. Na druhou stranu právě díky rychlosti rozvoje technologií, je umožněno tomuto

[62] Ministerstvo vnútra navrhuje zakázať používanie anonymizérov a uchovávať údaje používateľov verejných internetových fór. *Inet.sk* [online]. Banská Bystrica: Inet.sk, s. r. o., ©2002-2013 [cit. 2016-04-29]. Dostupné z: http://archiv.inet.sk/8135-8135ministerstvo-vnutra-navrhuje-zakazat-pouzivanie-anonymizerov-a-uchovavat-udaje-pouzivatelov-verejnych-internetovych-for.html

[63] How Tor Users Got Caught - Defcon 22. In: *Youtube* [online]. 5. 9. 2015 [vid. 2015-11-05]. Kanál uživatele Garrett Fogerlie. Dostupné z: https://www.youtube.com/watch?v=7G1LjQSYM5Q

dohledu stále více odolávat. Následující text se problematice dohledu bude věnovat v samostatné kapitole.

9. Informační etika a volba paradigmatu

O etice v informační společnosti hovoříme jako o informační etice. „Informační etika je umění a věda usilující o zvýšení citlivosti a uplatnění metod při posuzování morálních hodnot a činností v oblasti aplikace informací a informačních technologií v životě společnosti.“[64] Informační etika se týká všech fází životního cyklu informace a těch, kteří s informacemi pracují. Problematika této etiky je obsáhlá, stejně jako rámce její působnosti.

Východiskem pro etiku v dnešní informační společnosti je samozřejmě celkový etický rámec, jenž byl utvářen stovky let. Jan Činčera ve svých skriptech zastává jednoznačný postoj: „Přikláním se k názoru, že informační etika je podmnožinou obecné etiky a že soudy, které vynáší, nesmí být v rozporu s obecnými etickými postuláty. Navíc mi připadá celá diskuse poněkud akademická: proč hledat nové etické teorie, když jich tady je už tolik, že se na nich nedokážeme shodnout?”[65] Možností přístupu k disciplíně je několik a volba paradigmatu bude pochopitelně odrážet osobní postoje a hodnoty. Ve své práci pak Činčera předkládá výčet několika směrů, u nichž, po stručné charakteristice, poukazuje na silné a slabé stránky. Zmiňovanými teoriemi jsou: kodexově orientovaná morálka, teorie smlouvy, deontologické etické systémy, teleologické etické systémy, egoistické teorie, postmoderní reflexe, existenciální analýzy a ekologické analýzy.

Pro Onion routing, respektive software Tor a jím zprostředkovanou anonymitu poskytne příhodný etický rámec postmoderní filosofie. Postmoderní reflexe, se kterými jsou spojena jména Jacquese Derridy nebo Jean-Françoise Lyotarda, zpochybňují univerzální platnost etických hodnot a odmítají závaznost jejich pravidel. Víru v existenci a podporu takového fenoménu dokonce označují za neetické, neboť, optikou postmoderní filosofie, se každá taková

[64] LORENZ, Michal. Informační etika. (přednáška) Brno: Masarykova univerzita, 16. 10. 2011.

[65] *Informační etika: sylabus k bakalářskému studiu informační vědy*. 1. vyd. Brno: Masarykova univerzita, 2002, s. 20. ISBN 80-210-2981-1.

víra zakládá na určitém metanarativním příběhu, jehož legitimizující charakter[66] může nabýt až totalitní podoby. „Není univerzálně zakotvená etika, ale jen subjektivně pociťovaná morálka.“[67]

Morálku je možno definovat jako soubor nároků, požadavků a normativů na lidské jednání, které jsou určeny kulturou společnosti. Tzv. morální jednání představuje naplnění těchto požadavků v lidském konání, jedná se o chování, které společnost vnímá jako dobré či slušné. Oldřich Kužílek, poradce pro otevřenost veřejné správy a spoluautor zákona o svobodném přístupu k informacím, vidí problém ve skutečnosti, že není dostatečně jasné, co je v této oblasti (*ochrana dat a soukromí*) slušné. „Lidstvu chybí schopnost určit, co je slušné, protože teprve když víme, co je slušné, tak víme, co je neslušné, a můžeme pak říct, že to neslušné by mělo být pomocí nějak vyjádřeného práva nějakým způsobem limitováno, sankcionováno, regulováno.“[68]

Z důvodu předpokladu neexistence univerzálně platné etiky a s důrazem na morálku nebude na etické aspekty anonymitu poskytujícího softwaru Tor nahlíženo optikou konkrétního uceleného etického paradigmatu, nýbrž spíše z hlediska hodnot, které vyznává moderní demokratická společnost jako ty dobré, správné, slušné. Volba takového přístupu se zakládá na aktuálně probíhajících diskuzích nejen odborníků i široké veřejnosti zejména na téma, zda anonymita patří do demokracie. K tomuto přístupu přispěla rovněž poněkud alarmující skutečnost, že právě nejhlasitějšími odpůrci anonymity jsou státy s represivními vládami, a to především Čína, Severní Korea, Rusko a Írán.

[66] Problém: Legitimizace. LYOTARD, Jean-François. *O postmodernismu: postmoderno vysvětlované dětem: postmoderní situace*. 1. vyd. Praha: Filosofia, 1993, s. 104-106. ISBN 80-7007-047-1.

[67] *Informační etika: sylabus k bakalářskému studiu informační vědy*. 1. vyd. Brno: Masarykova univerzita, 2002, s. 20. ISBN 80-210-2981-1.

[68] Ochrana dat v éře sledování a odposlechů. In: *Youtube* [online]. 19. 2. 2014 [vid. 2015-10-06]. Kanál uživatele greensteam. Dostupné z: https://www.youtube.com/watch?v=YvEDA1nPjXU

10. Hodnoty vyznávané demokratickou společností

„V demokratické společnosti je nesmírně důležité, aby všichni občané měli volný přísun informací a svobodný přístup k informacím“[69]. „V případě neexistence práva na soukromí, nemůže existovat žádná opravdová svoboda projevu a názoru, a tudíž žádná skutečná demokracie.“[70]

I když neexistuje jednotný konsenzus, který by demokracii definoval, obecně přijatý opěrný systém demokracie je tvořen rovností před zákonem, politickými právy a právním státem. Rovnost před zákonem je ukotvena v Listině základních práv a svobody, stejně jako politická práva, v tomto případě zejména právo na informace, svobodu projevu a právo na odpor. Právní stát pak, uváděn v protikladu k diktaturám a totalitám, prezentuje důležitost zamezení zneužití politické moci proti občanům a jejich svobodě. Z hlediska těchto vyznávaných hodnot, tedy ochrany osobních údajů a soukromí, svobody slova a práva na informace, bude posuzována anonymita nabytá prostřednictvím softwaru Tor.

11. IP adresa jako osobní údaj

Vymezení osobních údajů a citlivých údajů není pro tuto část výrazněji významné. Odpovídající definice jsou snadno dohledatelné, navíc soukromí operuje se soukromými informacemi. „Soukromé informace jsou informace, které nechceme sdílet s jinými, nebo u kterých chceme osobně kontrolovat jejich pohyb, to znamená, že je sdílíme jen s někým, nikoliv s ostatními.”[71] mezi které mohou být zařazeny osobní údaje, avšak jejich výčet je širší. Takové informace mohou v určitých případech nabývat podoby identifikátoru. „Libovolná podmnožina atributů určitého jedince, která tohoto jedince jednoznačně určuje v jakékoliv množině jedinců.“[72] Člověk ani jako uživatel nedisponuje pouze jednou identitu. Identita je

[69] HURYCH, Jitka. Etika v informační společnosti. *Národní knihovna: knihovnická revue* [online]. 2003, 13(1), 3-6 [cit. 2016-03-24]. Dostupné z: http://full.nkp.cz/nkkr/NKKR0301/0301003.html

[70] Brazilian president: US surveillance a 'breach of international law':. *The Guardian* [online]. London: Guardian Media Group, 2016 [cit. 2016-04-02]. Dostupné z: http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance

[71] MATYÁŠ, Václav. Ochrana dat a informačního soukromí. (přednáška) Brno: Masarykova univerzita, 14. 9. 2014

[72] Tamtéž.

relacionistického charakteru, je různá v různém prostředí, kontextu, případně k roli, respektive k té které množině jedinců.

IP adresa je „jedinečná číselná adresa podle protokolu IP, která slouží jako identifikátor počítače nebo zařízení na síti TCP/IP. Vyjadřuje se čtveřicí čísel (32 bitů). Při zápisu se jednotlivá čísla oddělují tečkami. Každý počítač trvale připojený do internetu má přidělenu číselnou adresu, která je jednoznačná v celém internetu.“[73]

Vágní a poněkud rozpačitá definice ve směrnici Úřadu pro ochranu osobních údajů, která za osobní údaj považuje „jakákoliv informace týkající se určeného nebo určitelného subjektu údajů“ [74], ztěžuje rozhodování, zda IP adresu za osobní údaj považovat či nikoliv. Argumenty vyslovující se proti zařazení IP adresy mezi osobní údaje jsou založeny na skutečnosti, že tyto číselné adresy vedou k počítači, nikoliv k uživateli. Odkazování na technické zařízení samozřejmě nenaplňuje podstatu definice osobního údaje. S přihlédnutím k úzké provázanosti IP-adresy osobního počítače či mobilního telefonu s konkrétní osobou, je nasnadě, že číselné kombinace povedou rovněž ke koncovým uživatelům. Za přispění geografické lokace a časových údajů lze získat poměrně netriviální znalost, IP adresa tedy může reprezentovat nepřímou součást množiny dat vedoucí ke koncovému uživateli zařízení. „Pokud někde existuje informace, která může IP adresu doplnit tak, aby identifikovala konkrétní zařízení a tím jedince, je IP adresa osobním údajem. Tím spíš, že v tomto případě s jistotou víme, že takové informace existují.“[75]

Úřad pro ochranu osobních údajů IP adresu jako osobní údaj neuznává s následujícím odůvodněním „ve vztahu k IP adrese zcela chybí jednoznačně určený nebo určitelný subjekt a jako samostatný údaj tedy ani nemůže být IP adresa považována za osobní údaj.“[76] Osobním

[73] Sklenák, Vilém. IP adresa. In: KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV) [online]. Praha: Národní knihovna ČR, 2003- [cit. 2016-04-05]. Dostupné z: <http://aleph.nkp.cz/F/?func=direct&doc_number=000000620&local_base=KTD

[74] Zákon č. 101/2000 Sb., o ochraně osobních údajů. In: *ASPI* [právní informační systém]. Praha: Wolters Kluwer ČR [vid. 2016-01-04].

[75] HARAŠTA, Jakub a Jakub MÍŠEK. IP adresy v kybernetické bezpečnosti. *Revue pro právo a technologie* [online]. Brno, 2015, **6**(12), 21-42 [cit. 2016-04-17]. ISSN 1805-2797. Dostupné z: https://journals.muni.cz/revue/article/view/4091/pdf

[76] Zákon č. 101/2000 Sb., o ochraně osobních údajů. In: *ASPI* [právní informační systém]. Praha: Wolters Kluwer ČR [vid. 2016-01-04].

údajem se přece však mohou stát i takové údaj, které při vhodné kombinaci vedou k odhalení identity subjektu. Tento proces je označován jako nepřímá identifikace.

Evropská Unie přistupuje k IP adresám odlišným způsobem. Podle stanoviska Pracovní skupiny pro ochranu údajů č. 4/2007 ze dne 20. června 2007 *„pokud poskytovatel internetových služeb není schopen s naprostou jistotou odlišit údaje odpovídající uživatelům, kteří nemohou být identifikováni, bude muset pro jistotu nakládat se všemi informace o IP adresách jako s osobními údaji"*. [77] Nicméně se v obou případech jedná o stanoviska, nemají tedy charakter závazné právní normy.

Peter Hustinx z Inspektorátu Evropské ochrany dat je přesvědčen, že „anonymní data mohou být pořád osobní" [78]Vycházeje z definice identifikovatelnosti jako schopnosti osobních údajů někoho selektivně vyčlenit, má za to, že právě IP adresa ukazuje na chování jednotlivce z hlediska prováděných operací. „To nedělají počítače samy o sobě, zatím stojí jednotlivci, kteří je používají".[79]

V síti Tor, založené na dobrovolnictví a určitém altruismu, představují IP adresy fundamentální architektonické pilíře. Za problematickou oblast je ovšem stále považováno provozování koncového uzlu. „I když jsme přesvědčení, že provozování koncového uzlu je legální, je statisticky pravděpodobné, že může být použit za nelegálním účelem, což může přitáhnout pozornost orgánů činných v trestním řízení."[80] Takovou situaci ilustruje případ kolem Williama Webera[81], jenž byl na podzim roku 2012 obviněn z šíření dětské pornografie na základě jeho IP adresy, která byla přiřazena ke zprávě obsahující nezákonný pornografický obsah.

[77] *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. ledna 2015*. In: *ASPI* [právní informační systém]. Praha: Wolters Kluwer ČR [vid. 2016-01-03].

[78] Hustinx: nameless data can still be personal: Legal news and guidance from Pinsent Masons. In: Out-Law.com [online]. UK: Pinsent Masons, 2008 [cit. 2016-04-18]. Dostupné z: http://www.out-law.com/page-9563

[79] Hustinx: nameless data can still be personal: Legal news and guidance from Pinsent Masons. In: Out-Law.com [online]. UK: Pinsent Masons, 2008 [cit. 2016-04-18]. Dostupné z: http://www.out-law.com/page-9563

[80] *Tor: The Legal FAQ for Tor Relay Operators.* [online]. 2016 [cit. 2016-03-11]. Dostupné z: https://www.torproject.org/eff/tor-legal-faq.html.en

[81] JANOUŠ, Marek. Provozoval uzel sítě Tor, a obvinili jej z šíření dětské pornografie. In: *Lupa.cz: Server o českém Internetu* [online]. Praha: Internet Info s.r.o., 2012 [cit. 2016-04-17]. Dostupné z: http://www.lupa.cz/clanky/tor-zasah/

Prostřednictvím zařízení s touto IP adresou byl provozován koncový uzel a vlastník zařízení, ke kterému číselný identifikátor odkazoval, neměl o této aktivitě tušení.

Otázkou je, jak by se uzákonění IP adresy coby osobního údaje odrazilo na provozování těchto uzlů. Zařazení IP adres mezi osobní údaje by se promítlo zejména v rámci ochrany osobních údajů, musely by se tedy upravit praktiky zacházení s těmito daty, ve smyslu sběru, uchovávání i užívání. Síťový odposlech těchto kódů by se tedy ocitl mimo rámec zákon, což by upevnilo anonymitu poskytovanou Tor, na druhou stranu zároveň ztížilo odhalování trestné činnosti.

12. Soukromí

Jakkoliv se ve společnosti objevují hlasy označující soukromí za přežitek nebo považující soukromí uměle vytvořenou anomálii, je soukromí považováno za jeden z nosných pilířů osobní svobody. Soukromí je živě diskutovaný aspekt společnosti, ať už se hovoří o potřebě soukromí, nebo přímo právu na soukromí, o jeho narušování i zároveň požadavku na jeho ochranu. Obzvláště v poslední půlstoleté etapě bylo publikováno velké množství vědeckých pojednání hledající příhodné vymezení konceptu soukromí a vše, co k tomu náleží. Právě soukromí se ukázalo být jedním z nejvýraznějších problémů informační společnosti, neboť často koliduje s informačními potřebami státu a dalších institucí.

„Dobrá zpráva co se týká soukromí, že 84 % z nás má obavy o své soukromí. Ta špatná zpráva je, že přesně nevíme, co tím myslíme.“[82], zpravila své čtenáře Anne Branscomb, když se zabývala otázkou vlastnictví informace v rámci současné legislativy.

V tomto okamžiku je nezbytné upozornit na absenci obecně přijímaného vymezení pojmu soukromí, ba dokonce není stanoven ani konečný výčet toho, co můžeme do oblasti soukromí zahrnout. Na této skutečnosti staví i světově významný odborník na informační soukromí Daniel J. Solove[83] zdůrazňuje skutečnost, že nelze nalézt jednotící znak vymezující soukromí.

[82] BRANSCOMB, Anne Wells. *Who owns information?*. New York: Basic Books, 1994. xii , 241 s. ISBN 0-465-09175-X.

[83] SOLOVE, Daniel J. *Understanding privacy*. Cambridge, Mass.: Harvard University Press, 2008. ISBN 978-0-674-02772-5.

12.1. Legislativní ukotvení soukromí

O soukromí jako legálním právu v moderním smyslu mluvíme od konce 19. století. Warren a Brandeis[84] definovali soukromí jako právo „to be alone“, respektive jako pasivní možnost „to be left alone“. Takové soukromí se řešilo především v souvislosti s rozmáhajícím se tiskem, neboť původní záměr média zpravovat občany o aktuálním dění, politickém i kulturním, se v důsledku rostoucí konkurence proměnila v senzacechtivé, bulvární zpravodaje. V modernějším pojetí pak jako soukromí chápeme možnost života bez zásahu vlády a hromadných sdělovacích prostředků, která vznikla rovněž v důsledku rostoucího individualismu. V informační společnosti by soukromí analogicky odpovídalo právu „not to be identified“, tj. nebýt identifikován.

Roku 1973 United States Department of Health Education and Welfare zveřejnili příspěvek “Records, Computers, and the Rights of Citizens”[85], ve kterém se zabývají počítačovým zpracováním informací a neustále se rozšiřujícími úložišti osobních údajů, kterými disponují vládní agentury. „Jednotlivec musí stále častěji poskytovat informace o sobě velkým a relativně anonymním institucím, kde je používají cizí lidé – neznámí, neviditelní a často též nekomunikující. Někdy jednotlivci dokonce ani netuší, že o nich organizace uchovává záznamy. Běžně záznamy nevidí, natož aby zpochybnil jejich přesnost, kontroloval jejich následné šíření nebo napadl jejich užívání ostatními.“[86] Součástí tohoto příspěvku bylo doporučení „Fair Information Practices“[87], které sehrálo významnou roli v případě vytváření legislativního rámce pro informační soukromí ve Spojených státech, nýbrž jeho působnost je patrná v patřičné legislativě po celém světě., jak zdůrazňuje Marc Rotenberg[88], prezident a výkonný ředitel Electronic Privacy Information Center (EPIC).

---

[84] WARREN, Samuel D. a Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review* [online]. 1890, **4**(5), 193- [cit. 2016-04-10]. DOI: 10.2307/1321160. ISSN 0017811x. Dostupné z: http://www.jstor.org/stable/1321160?origin=crossref

[85] *Records, computers, and the rights of citizens: report* [online]. 1. [Cambridge? Mass.: MIT Press, 1973] [cit. 2016-04-10]. ISBN 02-620-8070-2. Dostupné z: https://www.justice.gov/opcl/docs/rec-com-rights.pdf

[86] Solove, Daniel J., *A Brief History of Information Privacy Law*. PROSKAUER ON PRIVACY, PLI, 2006; GWU Law School Public Law Research Paper No. 215. Dostupné z: http://ssrn.com/abstract=914271

[87] The Code of Fair Information Practices. *Epic.org: Electronic Privacy Information Center* [online]. Washington: EPIC, ©1994-2016 [cit. 2016-04-29]. Dostupné z: https://www.epic.org/privacy/consumer/code_fair_info.html

[88] ROTENBERG, Marc. Preserving privacy in the information society. In:*International Forum on Information and Documentation*. INTERNATIONAL FEDERATION FOR, 1998. p. 11-18.

V českém prostředí představuje jeden z pilířů legislativního uchopení soukromí EU Data Protection Directive, sestavený v roce 1995, jenž zakládá fundamentální principy legislativy zabývající se soukromím, platné pro členské země Evropské unie. V reakci na implementaci tohoto právního předpisu poukazuje Joel Reidenberg[89], odborník na soukromí a informační technologie v kontextu práva, na klíčový rozdíl přístupu evropské legislativy k soukromí a té americké. Zatímco tedy Spojené státy řeší soukromí více než z právního hlediska tržní optikou, Evropa, přesněji řečeno Evropská Unie zachází se soukromím jako s politickým imperativem zakořeněným v základních lidských právech. Tento přístup byl zachován i v případě European General Data Protection Regulation, které před čtyřmi lety nahradilo stávající směrnici.

12.2. Privacy by design

Úprava European General Data Protection Regulation nově operuje se dvěma principy, označovanými jako „privacy by design" a „privacy by default". Privacy by default je označení pro nastavení týkající se soukromí v rámci nového produktu či služby na tu nejpřísnější hodnotu, uživatel pak není nucen manuálně měnit nastavené svého soukromí. Termín *privacy by design* nemá ustálený český ekvivalent, neboť se jedná o téma v českém prostředí poměrně nové. Úřad pro ochranu osobních údajů[90] navrhuje termíny „ochrana soukromí jako aspekt návrhu" nebo „naprojektovaná ochrana soukromí". Jedná se o takový přístup k ochraně soukromí, jenž vyžaduje zakotvení zásad ochrany soukromí již do samotných návrhů různých technologií.

12.3. PET

Russell Shank, americký knihovník a prezident American Library Association uvědoměle již před třiceti lety upozorňuje, že „některé společenské ideály nemohou být přeloženy do srozumitelné právní teorie."[91]. Skutečnost, že ochrana soukromí nelze vyřešit pouze cestou

[89] Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 Hous. L. Rev. 717 (2001-2002) Dostupné z: http://ir.lawnet.fordham.edu/faculty_scholarship/38

[90] Úřad pro ochranu osobních údajů [online]. [cit. 2016-04-10]. Dostupný z: https://www.uoou.cz/privacy-by-design/ds-2307/p1=2307

[91] SHANK, Russell. Privacy: History, legal, social, and ethical aspects. *Library Trends*, 1986, 35.1: 7-18. Dostupné z: https://www.ideals.illinois.edu/bitstream/handle/2142/7457/librarytrendsv35i1c_opt.pdf?sequence=1

práva, si uvědomuje i Jan Holvast[92], který nachází další možnost v technické řešení problému, zmiňuje právě anonymizéry, nástroje určené pro využívání služeb v rámci ICT sítí bez zanechání digitálních stop, které by mohly vést k identifikaci uživatele. Tedy i Tor. Tyto nástroje tvoří množinu zaštítěnou označením PET.

PET je zkratka označující Privacy enhancing technologies, tj. technologie zajišťující soukromí. Handbook of Privacy and Privacy-Enhancing Technologies definuje PET jako „technologie zajišťující soukromí představují systém ICT opatření, chránící informační soukromí skrze eliminaci či minimalizaci použití osobních dat, čímž předchází zbytečnému či nechtěnému zpracování osobních dat, aniž by byla narušena funkčnost informačního systému.“[93] PET je tedy souhrnné označení pro množinu počítačových nástrojů a mechanismů, které, integrovány v počítačových službách či aplikacích či využívány v součinnosti s nimi, umožňují uživatelům chránit osobní údaje, které těmto aplikacím či službám svěřují a s nimiž tyto aplikace nakládají.

13. Společnost pod dohledem

Charakteristickým rysem současné informační společnosti je všudypřítomný dohled státu a jiných institucí pod záminkou bezpečnosti občanů a potlačení případné trestné činnosti, v extrémním případě zamezení terorismu. Technologie umožňující dohled nad internetem však nejsou problematické pouze v zemích s diktátorským režimem, k porušování lidských práv v souvislosti s užíváním informačních a komunikačních technologií činí potíže i v demokratických zemích. Trendem je podávat takový obraz o dění ve společnosti, který má za následek nejen smíření, ba dokonce aktivní žádost o takový dohled i za cenu podstoupení části svého soukromí.

Dozor státu nad svými občany probíhá většinou pod záštitou jejich bezpečnosti, ochrany před terorismem, monitoring má posílit boj proti korupci, chránit děti před škodlivým obsahem apod. Dnes a denně jsou lidé přesvědčování o tom, že cenzura je nutná. Hromadný sběr dat dělá z každého subjektu dat potencionálního podezřelého. Otřepaným argumentem je sousloví „nic

[92] History of Privacy. In: *The Future of Identity in the Information Society* [online]. Brno: Springer Berlin Heidelberg, 2009, s. 13-42 [cit. 2016-04-10]. DOI: 10.1007/978-3-642-03315-5_2. ISBN 978-3-642-03315-5. ISSN 1868-4238. Dostupné z: http://link.springer.com/10.1007/978-3-642-03315-5_2

[93] PISA CONSORTIUM. Handbook of Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents. [online]. Haag: TNO-FEL, 2003. ISBN 90-74087-33-7. [cit. 2016-03-04]. Dostupné z: http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf

špatného nedělám, nemám co skrývat[94]“, což vytváří nejen iluzi legitimity takových zásahů do soukromí, ale úplně zneškodňuje princip, který je označován jako presumpce neviny a který je právě jedním ze základů v úvodu zmíněné vyznávané hodnoty právního státu.

Skutečnost, že současná míra dozoru státu, státními agenturami a jinými institucemi není kompatibilní se základními lidskými právy, si uvědomuje stále více a více lidí, pročež jejich nejběžnější reakce se omezuje na poněkud vágní požadavek omezení přístupu ke shromážděným datům, což je evidentně poněkud neefektivní, řečeno bez skrupulí naprosto zbytečné. Richard Stallmann[95], zakladatel svobodného softwaru, projektu GNU, vývojář, lektor a hacker v jedné osobě, považuje neustálý digitální dozor nad společností za jakési společenské znečištění, které připodobňuje ke znečištění životního prostředí. S touto paralelou pracuje, když si pokládá otázku, jakou míru takového dohledu demokratické společnost unese. Stallmann vysvětluje naléhavou a okamžitou potřebu limitovat nežádoucí dopad na společnost s každou další implementací digitálního systému. Nenaléhavější je však jeho apel směrem k jednotlivým uživatelům, neboť u nich celý proces začíná.

Skutečnou hrozbu pro naše soukromí, respektive pro naši osobní svobodu jako takovou, představuje zcela jednostranná, asymetrická ztráta soukromí vůči moci. Na tomto místě je důležité zmínit původní motivaci mechanismu Tor. Tento software byl navržen takovým způsobem, aby zabránit uživatelům, ve smyslu nejen korporací ale i jednotlivců, určit polohu uživatele a zároveň zamezit pozorování našich uživatelských návyků v rámci internetových prohlížečů. Důraz byl kladen primárně na soukromí uživatelů před marketingovými společnostmi, nikoliv před těmi vládními. „Chtěli jsme poskytnout kontrolu nad tvými informacemi tobě, uživateli, nikoliv implicitně všem těm společnostem. Na tobě jsme chtěli nechat rozhodnutí, zda důvěřuješ Googlu, zda důvěřuješ Amazonu, zda důvěřuješ BBC, komukoliv.“[96]

---

[94] SOLOVE, Daniel J. "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. *San Diego Law Review* [online]. 2007, **44**(4), 745-772 [cit. 2016-02-11]. ISSN 00364037. Dostupné z: http://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?sid=dd651e5c-6219-41bc-8dd3-df53b8e6f099%40sessionmgr120&vid=2&hid=113

[95] Stallman: How Much Surveillance Can Democracy Withstand? *WIRED* [online]. New York: WIRED, 2016 [cit. 2016-02-27]. Dostupné z: http://www.wired.com/2013/10/a-necessary-evil-what-it-takes-for-democracy-to-survive-surveillance/

[96] What is Tor? A beginner's guide to the privacy tool. *The Guardian* [online]. London: Guardian Media Group, 2016 [cit. 2016-04-02]. Dostupné z: http://www.rogerclarke.com/DV/Dredge-131105-WhatIsTor.pdf

Právě takové aspekty mechanismu Tor převažují na etických miskách vah. Motivace uživatelů Tor, která byla představena v jedné z prvních kapitol, naprosto legitimizuje používání softwaru Tor, stejně jako hovoří ve prospěch anonymního pohybu v online prostředí. Anonymita a Tor. Thomas Cooley, významný právník, advokát a profesor práv na Univerzitě v Michiganu, měl již v roce 1868 velmi jasný názor na potřebu a důležitost soukromí, když se, a pro náš případ velmi trefně, vyslovuje: „*Je častokrát lepší nechat zločin nepotrestán, než napadnout prostor občana, jeho truhlice vylomené a jeho knihy, soukromé dokumenty a dopisy vystavené všetečné zvědavosti*.“[97]

14. Tor proniká do mainstreamu

Stránky New Yorkeru upozorňující na páchání nepravostí, knihovny s kopiemi často nedostupných knih či blogy politických aktivistů se nenacházejí v zorném poli senzacechtivých médií toužících po bizarních, kontroverzních a skandálních zprávách. Lákavější je nedbalé zpracování kauzy Silk road[98] nebo nepodložené obvinění technologie z nedávných teroristických útoků[99].

Lidé z Tor Project si dobře uvědomují negativní konotaci, se kterou se o tomto softwaru na veřejnosti hovoří, a proto se snaží neustále navazovat nové kontakty, publikovat a šířit tak osvětu nejen o Tor, ale potažmo o významu anonymity na Internetu obecně. V říjnu 2014 si zástupci Tor Project najali dokonce PR firmu Thomson Communications s konkrétní objednávkou, a to změnit negativní slovník, který je ve spojitosti s Tor užíván. Doprovázeno bouřlivou mediální publicitou společné snažení bylo úspěšné. Nejpřesvědčivějším výsledkem je navýšení nevládních zdrojů financování projektu.

Neustále také stoupá počet firem, které jednají s lidmi z Tor Project s cílem zahrnout přístup do sítě Tor do svých produktů. Jednou konkrétní představou do budoucna je nahrazení dosavadního soukromého režimu běžných prohlížečům přístupem k této síti. Jak známo

[97] Cooley, Thomas McIntyre. *A Treatise on the Constitutional Limitations Which Rest Upon the Legislative Powers of the States of the American Union*. Boston: Little, Brown, 1868, p. 306.

[98] Umožnil prodej tvrdých drog. Provozovatel portálu Silk Road dostal doživotí. In: *Lidovky.cz* [online]. Praha: MAFRA, a.s, 2015 [cit. 2016-04-21]. Dostupné z: http://www.lidovky.cz/pres-americky-webovy-portal-se-prodavaly-drogy-jeho-sef-dostal-dozivoti-14g-/zpravy-svet.aspx?c=A150529_223636_ln_zahranici_ELE

[99] France looking at banning Tor, blocking public Wi-Fi. In: *Arstechnica* [online]. Cambridge: WIRED Media: Ars Technica and WIRED, 2015 [cit. 2016-04-21]. Dostupné z: http://arstechnica.com/tech-policy/2015/12/france-looking-at-banning-tor-blocking-public-wi-fi/

vývojáři Tor úzce spolupracují zejména s Firefoxem, ohniskem jejich kooperace je zejména oblast bezpečnosti a použitelnosti.

To, že užívání softwaru Tor se stává mainstreamovou záležitostí, si můžeme ilustrovat na Richardu Jamesonovi, známého pod uměleckým jménem Aphex Twin, který před dvěma roky způsobil poprask tím, když na svých sociálních sítích zveřejnil odkaz s adresou *.onion,* který vedl ke skryté službě v síti Tor, na které zveřejnil název a seznam písniček svého nově připraveného alba.

Spolupráci organizace Tor Project s veřejností znázorňuje konkrétní koncept, který, alespoň optikou našeho oboru, lze označit za zajímavý, snad odvážný.

14.1. Tor v knihovnách

Knihovny v dnešní době musí neustále obhajovat svůj význam a přínos společnosti. Argumentujíce zejména skutečností, že oporný pilíř takových institucí představují knihovní výpůjčky, je naštěstí překonanou domněnkou, jsou s velkým důrazem vyzdvihovaný služby jako přístup k Internetu a jiné způsoby zprostředkování informací. Ovšem tyto služby limituje praxe obchodníků a vlády dohlížejících na digitální prostředí a pohyb v něm.

Vyznávanými hodnotami knihoven jsou lidská práva a jejich ochrana, svobodný přístup k informacím, svoboda slova, tisku apod. Diskutovaná je ovšem skutečnost, jak lze tuto ochranu zaručit vzhledem k technologiím, které jsou v knihovnách užívány a jejichž politika je naprosto v rozporu s vyznávanými hodnotami. Jako ilustrativní příklad poslouží odhalení praktik osvojených společností Adobe[100] a jeho nástroje pro digitální úpravy dokumentů.

Na jedné straně zde máme aktivní participaci knihoven na plnění slíbených záruk ochrany soukromí, které mohou mít např. podobu minimální rozsah a omezená časové období uchovávaných záznamů o výpůjčkách, nebo přístup k počítači bez potřeby identifikátoru ve smyslu uživatelského účtu, jména apod. Na straně druhé zde však stojí takové digitální zdroje, které jsou dostupné prostřednictvím korporací sbírajících a zpracovávajících data uživatelů. Projekt svobodných knihoven se snaží do této oblasti zasáhnout.

[100] Adobe Spyware Reveals (Again) the Price of DRM: our Privacy and Security. *Electronic Frontier Foundation* [online]. San Francisco: EFF, 2016 [cit. 2016-02-15]. Dostupné z: https://web.archive.org/web/20150321222721/https:/www.eff.org/deeplinks/2014/10/adobe-spyware-reveals-again-price-drm-your-privacy-and-security

Library Freedom Project představuje úzkou spolupráci knihovníků, techniků, právníků a obhájců soukromí za účelem vytvoření skutečné intelektuální svobody v knihovnách. Projekt představila jeho zakladatelka, knihovnice a aktivistka v oblasti soukromí, Alison Macrina, začátkem února 2015.

Obrázek 13: logo Library Freedom Project[101]

Původní podoba a způsob naplňování tohoto cíle se omezovala na šíření osvěty. Zástupci projektu kontaktovali knihovny s vzdělávacími programy, pořádali workshopy a konference. Účelem bylo vzdělat knihovníky ve třech klíčových oblastech, a to informovat je o hrozbách digitálního dohledu, proškolit je v oblasti soukromí a ochrany dat, seznámit je a naučit je pracovat s anonymizačními nástroji. V dalším kroku pak vychází větší aktivita ze stran knihoven, které instalují software Tor na své počítače a zároveň pak poskytnou své IP adresy.

Důvodem, proč byly pro spolupráci zvoleny právě knihovny, cíleno na ty veřejné, je souhrn několika faktorů specifických právě pro tyto instituce. Jednak je to jejich významné aktivistické působí v boji za lidská práva v historii i hodnoty vyznávané v současnosti, jednak je to pak technické zázemí knihoven, tedy přístup k počítači a k Internetu. Klíčovou hodnotu do tohoto projektu vnáší úzký vztah knihoven k místním komunitám. Zároveň Tyto skutečnosti činí z knihoven ideální prostředí rozšiřovat povědomí o síti Tor, ale i o dalších nástrojích anonymizace, respektive o fenoménu anonymity vůbec.

První knihovnou, která se aktivně zapojila a v níž byla implementována i druhá fáze, tedy nainstalování Tor Browser a poskytnutí IP adresy, byla Kiltonská veřejná knihovna v New Hampshire. Není překvapením, že tato událost vzbudila zájem i u místní policie a knihovna

[101] *The Library Freedom Project* [online]. Dostupné z: https://libraryfreedomproject.org/

pod nátlakem celou operaci anulovala. Nicméně v následujících dnech se zvedla vlna masivní podpory veřejnosti, která dodala instituci odvahu ke znovuvybudování uzlu pro síť Tor.

Projekt se ztotožňuje s tezí The Freedom to Read Statement[102], kterou představila American Library Association (ALA) v květnu roku 1953. Prohlášení zakončené tvrzením, že „svoboda je sama o sobě nebezpečný způsobem života, ale je naše.“[103], hovoří ve prospěch tohoto projektu navzdory vyvolávající kontroverzi zapříčiněnou primárně volbou konkrétního nástroje. „I když se zaměřujeme na knihovny Spojených států, horlivě hovoříme s našimi kolegy z dalších států, jelikož soukromí je právo pro každého v každé zemi (a je všude ohrožováno).“[104] Výhled do budoucnosti, mimo plánované internacionální rozšíření projektu, představuje inkorporace dalších služeb, které Tor nabízí, představitelé projektu se nebrání ani možnosti provozovat skryté služby na serverech knihovny. V květu tohoto roku byl Library Freedom Project dokonce získal cenu Free Software Award for Projects of Social Benefit at MIT institucí Free Software Foundation´s[105].

Oldřich Kužílek, poradce pro otevřenost veřejné správy a ochranu soukromí a autor zákona o svobodném přístupu k informacím, v panelové diskusi Ochrana dat v éře sledování a odposlechů[106] v rámci projektu Zelená pro budoucnost Evropy a Česka, snažícího se mimo jiné zapojit veřejnost do debat o aktuálních evropských tématech, zmiňuje potřebu množiny takových úředníků, jež by byli proškoleni v oblasti ochrany soukromí a osobních údajů, aby byli připraveni a schopni občanům srozumitelným způsobem vysvětlit důsledky jejich konkrétního projevu v digitálním světě. Podle mého názoru, projekt svobodných knihoven v jistém smyslu koresponduje s touto jeho výzvou.

---

[102] The Freedom to Read Statement. *ALA: American Library Association* [online]. Chicago: ALA, 2016 [cit. 2016-02-13]. Dostupné z: http://www.ala.org/advocacy/intfreedom/statementspols/freedomreadstatement

[103] The Freedom to Read Statement. *ALA: American Library Association* [online]. Chicago: ALA, 2016 [cit. 2016-02-13]. Dostupné z: http://www.ala.org/advocacy/intfreedom/statementspols/freedomreadstatement

[104] Guest Post: The Library Freedom Project: Bringing privacy and anonymity to libraries. In: *Tor Project Blog* [online]. 2015 [cit. 2016-02-14]. Dostupné z: https://blog.torproject.org/blog/guest-post-library-freedom-project-bringing-privacy-and-anonymity-libraries

[105] Library Freedom Project and Werner Koch are 2015 Free Software Awards winners. *Free Software Foundation* [online]. Boston: Free Software Foundation, ©2004-2016 [cit. 2016-02-15]. Dostupné z: https://www.fsf.org/news/library-freedom-project-and-werner-koch-are-2015-free-software-awards-winners

[106] Ochrana dat v éře sledování a odposlechů. In: *Youtube* [online]. 19. 2. 2014 [vid. 2015-10-06]. Kanál uživatele greensteam. Dostupné z: https://www.youtube.com/watch?v=YvEDA1nPjXU

V. Závěr

V této práci byl uveden přehled anonymizace softwarem Tor z technického hlediska a bylo představeno několik etických problémů v současné společnosti, které by mohly být řešeny použitím této technologie.

V prvním oddílu práce jsem představila koncept Onion routingu a jeho zdařilé implementace Tor. Pokusila jsem se vysvětlit, na jakém principu software pracuje a co síť Tor obnáší. Větší prostor byl věnován skrytým službám, neboť se jedná právě o ten aspekt, na základě kterého je Tor démonizován.

V druhém oddílu byl vykreslen koncept anonymity. Do této části jsem se pokusila zařadit především takové aspekty, které nejsou v českém prostředí příliš známé, nebo výrazněji rozšířené. Anonymita je zde uvedena z hlediska bezpečnostní teorie systému a jsou představeny její psychologické aspekty, které ukazují, že ve společnosti přetrvávají mylné představy, pro které je stav anonymity obávaný.

Třetí oddíl věnující se etickým aspektům poukazuje na některé problémy současné informační společnosti. Je dokladem o nutnosti začít problémy, kterými se informační etika zabývá, řešit úpravou stávající legislativy, avšak naléhavěji se jeví potřeba řešení technického charakteru, ve smyslu rozšíření užívání technologií zajišťujících soukromí, třeba právě instalováním softwaru Tor a využíváním jeho sítě i pro běžné surfování. Zjednodušeně, motto této části by znělo „Za svobodnější Internet.“.

Anonymity i pseudonymity bylo celou řadu let využíváno v literatuře i umění a využívá se jich dodnes. Od jeskynních maleb pravěkých lidí přes samotnou Bibli až do dnešní doby je anonymity využíváno. Anonymita je předpokladem pro fungující demokratickou společnost, od samotného způsobu voleb až po právo na soukromí a svobodu projevu.

Z předložené bakalářské práce by mělo vyplývat především to, že Tor je pouze nástroj, který anonymizuje spojení s prohlížečem, a nepřisuzovat mu zázračné vlastnosti, a to jak v pozitivním slova smyslu, tedy že zaručuje bezpečnost uživatelů, tak v tom negativním vyznění o napomáhání trestné činnosti. Pochopitelně lze Tor označit jako vynález zkázy, jenže každý užitečný a dobrý vynález byl dříve či později zneužit.

Anonymita zprostředkovaná softwarem Tor prokazuje svou užitečnost v rámci práce s drogově závislými, při řešení krizových situací, v průběhu rekonvalescence z prožitých traumat nebo v případech choulostivých zdravotních problémů. Taková anonymita je též vhodná pro informátory, koresponduje se žurnalistickou etikou, je nápomocna policii i armádě. Na druhé straně nelze přehlížet možný ilegální obsah či nápomoc k trestným činům, avšak ve srovnání s „dobrem“, které přináší, jde o výrazný nepoměr.

Tor se ukázal být vhodným nástrojem pro častější používání vyžadující vyšší bezpečnost. Samozřejmě není dostačující pouhá instalace takového anonymizačního nástroje, a, ačkoliv poskytuje uživateli dostatečnou míru anonymity, je i nadále od uživatele vyžadována obezřetnost. Problematika anonymizérů vyžaduje osvětu a související vzdělání, v našem konkrétním případě jakousi Tor-gramotnost. Inspiraci nám předkládán v závěru zmíněný Library Freddom Project.

VI. Seznam použitých zdrojů

ABLON, Lillian;Libicki. Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data. *Defense Counsel Journal* [online]. 2015, **82**(2), 143-152 [cit. 2016-04-28]. ISSN 08950016. Dostupné z: http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?sid=4abe1479-2a2d-4705-bd21-bdc6d08e1287%40sessionmgr4001&vid=2&hid=4105

ALQAHTANI, Abdullah A. a El-Sayed M. EL-ALFY. Anonymous Connections Based on Onion Routing: A Review and a Visualization Tool. *Procedia Computer Science* [online]. 2015, **52**, 121-128 [cit. 2016-04-28]. DOI: 10.1016/j.procs.2015.05.040. ISSN 18770509. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1877050915008406

ANDERSSON, Christer a Reine LUNDIN. On the Fundamentals of Anonymity Metrics. *The Future of Identity in the Information Society* [online]. Boston, MA: Springer US, 2008, s. 325 [cit. 2016-04-28]. DOI: 10.1007/978-0-387-79026-8_23. ISBN 978-1-4419-4629-4. Dostupné z: http://link.springer.com/10.1007/978-0-387-79026-8_23

Anonymous Connections and Onion Routing. *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS* [online]. 1998, **16**(4), 482-494 [cit. 2016-04-28]. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=668972

BACKES, Michael, Ian GOLDBERG, Aniket KATE a Esfandiar MOHAMMADI. Provably Secure and Practical Onion Routing. In: *2012 IEEE 25th Computer Security Foundations Symposium* [online]. IEEE, 2012, s. 369-385 [cit. 2016-04-28]. DOI: 10.1109/CSF.2012.32. ISBN 978-1-4673-1918-8. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6266172

BAE, Mikyeung. The effects of anonymity on computer-mediated communication: The case of independent versus interdependent self-construal influence. *Computers in Human Behavior* [online]. 2016, **55**, 300-309 [cit. 2016-04-28]. DOI: 10.1016/j.chb.2015.09.026. ISSN 07475632. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0747563215301576

BERTHOLD, Oliver; FEDERRATH, Hannes; KÖHNTOPP, Marit. Project "anonymity and unobservability in the Internet". In: *Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions*. ACM, 2000. p. 57-65.

BEZZI, Michele. An entropy based method for measuring anonymity. In:*Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*. IEEE, 2007. p. 28-32.

BODLE, Robert. The ethics of online anonymity or Zuckerberg vs. Moot. *ACM SIGCAS Computers and Society*, 2013, 43.1: 22-35.

BRANSCOMB, Anne Wells. *Who owns information?*. New York: Basic Books, 1994. xii , 241 s. ISBN 0-465-09175-X.

ÇALIŞKAN, Emin, Tomáš MINÁRIK a Anna-Maria OSULA. *Technical and Legal Overview of the Tor Anonymity Network* [online]. Tallinn, 2015 [cit. 2016-01-20]. Dostupné z: https://ccdcoe.org/sites/default/files/multimedia/pdf/TOR_Anonymity_Network.pdf

COBLE, Aaron Richard. *Anonymity, information, and machine-assisted proof*. 2010. PhD Thesis. University of Cambridge.

CROFTON, Isaak. *Crypto Anarchy*. 1. United States: Lulu.com, 2015. ISBN 1329059808.

DÍAZ, Claudia, Stefaan SEYS, Joris CLAESSENS a Bart PRENEEL.*Towards Measuring Anonymity* [online]. s. 54 [cit. 2016-04-28]. DOI: 10.1007/3-540-36467-6_5. Dostupné z: http://link.springer.com/10.1007/3-540-36467-6_5

DINGLEDINE, Roger; MATHEWSON, Nick; SYVERSON, Paul. Challenges in deploying low-latency anonymity (DRAFT). *Unpublished Manuscript. http://tor. eff. org/cvs/tor/doc/design-paper/challenges. pdf*, 2005.

DINGLEDINE, Roger a Paul SYVERSON. *Privacy enhancing technologies: second International Workshop, PET 2002 : San Francisco, CA, USA, April 14-15, 2002 : revised papers*. Berlin: Springer, c2003. Lecture notes in computer science. ISBN 3-540-00565-X.

FEIGENBAUM, Joan, Aaron JOHNSON a Paul SYVERSON. *A Model of Onion Routing with Provable Anonymity* [online]. s. 57 [cit. 2016-04-28]. DOI: 10.1007/978-3-540-77366-5_9. Dostupné z: http://link.springer.com/10.1007/978-3-540-77366-5_9

FEIGENBAUM, JOAN;FORD. Seeking Anonymity in an Internet Panopticon. *Communications of the ACM* [online]. 2015, **58**(10), 58-69 [cit. 2016-04-28]. DOI: 10.1145/2714561. ISSN 00010782. Dostupné z: http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?sid=41123018-5261-495d-a1e4-6c5838442c0f%40sessionmgr4002&vid=3&hid=4105

FindLaw: For Legal Professionals [online]. Minnesota: Thomson Reuters, 2016 [cit. 2016-04-28]. Dostupné z: http://lp.findlaw.com/

FORTIER, Alexandre a Jacquelyn BURKELL. Hidden Online Surveillance: What Librarians Should Know to Protect Their Own Privacy and That of Their Patrons. *Information Technology and Libraries* [online]. 2015, **3**(34), 59-72 [cit. 2016-04-28]. ISSN 2163-5226. Dostupné z: http://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?sid=06ee6d13-8d28-4ed9-8e0c-bd0bc7ce5c73%40sessionmgr103&vid=2&hid=113

GELLER, Tom. In Privacy Law, It's the U.S. vs. the World. *Communications of the ACM* [online]. 2016, **59**(2), 21-23 [cit. 2016-04-28]. DOI: 10.1145/2852233. ISSN 00010782. Dostupné z: http://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?sid=3d905c0e-da86-4f6a-a468-79c19868ca7f%40sessionmgr103&vid=2&hid=113

GOLDBERG, Ian. *Privacy-Enhancing Technologies for the Internet, II: Five Years Later* [online]. s. 1 [cit. 2016-04-28]. DOI: 10.1007/3-540-36467-6_1. Dostupné z: http://link.springer.com/10.1007/3-540-36467-6_1

GOLDSCHLAG, David M., Michael G. REED a Paul F. SYVERSON. *Hiding Routing information* [online]. s. 137 [cit. 2016-04-28]. DOI: 10.1007/3-540-61996-8_37. Dostupné z: http://link.springer.com/10.1007/3-540-61996-8_37

HARAŠTA, Jakub;Míšek. IP adresy v kybernetické bezpečnosti. *Revue pro právo a technologie* [online]. 2015, **6**(12), 21-42 [cit. 2016-04-28]. Dostupné z: https://journals.muni.cz/revue/article/viewFile/4091/pdf

HAUGHEY, Hamish, Gregory EPIPHANIOU a Haider M AL-KHATEEB. Anonymity networks and the fragile cyber ecosystem. *Network Security* [online]. 2016, **2016**(3), 10-18 [cit. 2016-04-28]. DOI: 10.1016/S1353-4858(16)30028-9. ISSN 13534858. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1353485816300289

HEURIX, Johannes, Peter ZIMMERMANN, Thomas NEUBAUER a Stefan FENZ. A taxonomy for privacy enhancing technologies. *Computers & Security* [online]. 2015, **53**, 1-17 [cit. 2016-04-28]. DOI: 10.1016/j.cose.2015.05.002. ISSN 01674048. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0167404815000668

History of Privacy. In: *The Future of Identity in the Information Society* [online]. Brno: Springer Berlin Heidelberg, 2009, s. 13-42 [cit. 2016-04-10]. DOI: 10.1007/978-3-642-03315-5_2. ISBN 978-3-642-03315-5. ISSN 1868-4238. Dostupné z: http://link.springer.com/10.1007/978-3-642-03315-5_2

HURYCH, Jitka. Etika v informační společnosti. *Národní knihovna: knihovnická revue* [online]. 2003, 13(1), 3-6 [cit. 2016-02-11]. Dostupné z: http://full.nkp.cz/nkkr/NKKR0301/0301003.html

Informační etika: sylabus k bakalářskému studiu informační vědy. 1. vyd. Brno: Masarykova univerzita, 2002. ISBN 80-210-2981-1.

JARDINE, E. Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. *New Media & Society*[online]. [cit. 2016-04-28]. DOI: 10.1177/1461444816639976. ISSN 1461-4448. Dostupné z: http://nms.sagepub.com/cgi/doi/10.1177/1461444816639976

LORENZ, Michal. Informační etika. (přednáška) Brno: Masarykova univerzita, 16. 10. 2011.

MACRINA, Alison. The Tor Browser and Intellectual Freedom in the Digital Age. *Reference* [online]. 2015, **54**(4), 17-20 [cit. 2016-04-28]. ISSN 10949054. Dostupné z: http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?sid=e5746497-ee45-44ab-8cf5-2a89f19299d5%40sessionmgr4004&vid=2&hid=4105

MATYÁŠ, Václav. Ochrana dat a informačního soukromí. (přednáška) Brno: Masarykova univerzita, 14. 9. 2014

MILAJERDI, Sadegh Momeni a Mehdi KHARRAZI. A composite-metric based path selection technique for the Tor anonymity network.*Journal of Systems and Software* [online]. 2015, **103**, 53-61 [cit. 2016-04-28]. DOI: 10.1016/j.jss.2015.01.002. ISSN 01641212. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0164121215000035

MINÁRIK, Tomáš a Anna-Maria OSULA. Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law.*Computer Law & Security Review* [online]. 2016, **32**(1), 111-127 [cit. 2016-04-28]. DOI: 10.1016/j.clsr.2015.12.002. ISSN 02673649. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0267364915001673

MOORE, Daniel a Thomas RID. Cryptopolitik and the Darknet. *Survival* [online]. 2016, **58**(1), 7-38 [cit. 2016-04-18]. DOI: 10.1080/00396338.2016.1142085. ISSN 0039-6338. Dostupné z: http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085

MÜLLER, Sebastian;Brecht. Distributed Performance Measurement and Usability Assessment of the Tor Anonymization Network. *Future Internet* [online]. 2012, **4**(2), 488-513 [cit. 2016-04-28]. ISSN 19995903. Dostupné z: http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?sid=ef06b095-e89b-41b1-854b-62336a3ec21e%40sessionmgr4005&vid=2&hid=4105

OWEN, Michael. Fun with onion routing. *Network Security* [online]. 2007, **2007**(4), 8-12 [cit. 2016-04-28]. DOI: 10.1016/S1353-4858(07)70044-2. ISSN 13534858. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1353485807700442

PHELPS, Amy a Allan WATT. I shop online – recreationally! Internet anonymity and Silk Road enabling drug use in Australia. *Digital Investigation* [online]. 2014, **11**(4), 261-272 [cit. 2016-04-28]. DOI: 10.1016/j.diin.2014.08.001. ISSN 17422876. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1742287614000930

PISA CONSORTIUM. Handbook of Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents. [online]. Haag: TNO-FEL, 2003. ISBN 90-74087-33-7. [cit. 2016-04-28]. Dostupné z: http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf

POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012. 388 s. ISBN 9788087284223.

Records, computers, and the rights of citizens: report [online]. 1. [Cambridge Mass.: MIT Press, 1973] [cit. 2016-04-10]. ISBN 02-620-8070-2. Dostupné z: https://www.justice.gov/opcl/docs/rec-com-rights.pdf

REITER, Michael K. a Aviel D. RUBIN. Crowds: anonymity for Web transactions. *ACM Transactions on Information and System Security* [online]. **1**(1), 66-92 [cit. 2016-03-27]. DOI: 10.1145/290163.290168. ISSN 10949224. Dostupné z: http://portal.acm.org/citation.cfm?doid=290163.290168

ROTENBERG, Marc. Preserving privacy in the information society. In:*International Forum on Information and Documentation*. INTERNATIONAL FEDERATION FOR, 1998. p. 11-18.

SERJANTOV, Andrei a George DANEZIS. *Towards an Information Theoretic Metric for Anonymity* [online]. s. 41 [cit. 2016-04-28]. DOI: 10.1007/3-540-36467-6_4. Dostupné z: http://link.springer.com/10.1007/3-540-36467-6_4

SHANK, Russell. Privacy: History, legal, social, and ethical aspects. *Library Trends*, 1986, 35.1: 7-18. Dostupné z: https://www.ideals.illinois.edu/bitstream/handle/2142/7457/librarytrendsv35i1c_opt.pdf?sequence=1

SCHUBERT, Christoph. Unidentified speakers in news discourse: A pragmatic approach to anonymity. *Journal of Pragmatics* [online]. 2015, **89**, 1-13 [cit. 2016-04-28]. DOI: 10.1016/j.pragma.2015.09.003. ISSN 03782166. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0378216615002520

SOLOVE, Daniel J. *Nothing to hide: the false tradeoff between privacy and security*. New Haven: Yale University Press, 2011. ISBN 978-0-300-17233-1.

SOLOVE, Daniel J. "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. *San Diego Law Review* [online]. 2007, **44**(4), 745-772 [cit. 2016-04-28]. ISSN 00364037. Dostupné z: http://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?sid=dd651e5c-6219-41bc-8dd3-df53b8e6f099%40sessionmgr120&vid=2&hid=113

SOLOVE, Daniel J. *Understanding privacy*. Cambridge, Mass.: Harvard University Press, 2008. ISBN 978-0-674-02772-5.

The Freedom to Read Statement. *ALA: American Library Association* [online]. Chicago: ALA, 2016 [cit. 2016-04-28]. Dostupné z: http://www.ala.org/advocacy/intfreedom/statementspols/freedomreadstatement

THE TOR PROJECT. Tor: Anonymity Online [online]. [2012] [cit. 2016-04-28]. Dostupné z: https://www.torproject.org/index.html.en

Tor: The Second-Generation Onion Router. *Proceedings of the 13th conference on USENIX Security Symposium* [online]. 2004, **13**(1), 21-39 [cit. 2016-04-28]. ISSN 0006E2EF. Dostupné z: https://www.usenix.org/legacy/publications/library/proceedings/sec04/tech/full_papers/dingledine/dingledine.pdf?CFID=767814377&CFTOKEN=95122783

WALLACE, Jonathan D. *Nameless in cyberspace: Anonymity on the internet*. Cato Institute, 1999. Dostupné z: http://object.cato.org/sites/cato.org/files/pubs/pdf/bp54.pdf

WARREN, Samuel D. a Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review* [online]. 1890, **4**(5), 193- [cit. 2016-04-10]. DOI: 10.2307/1321160. ISSN 0017811x. Dostupné z: http://www.jstor.org/stable/1321160?origin=crossref

Zákon č. 101/2000 Sb., o ochraně osobních údajů. In: *ASPI* [právní informační systém]. Praha: Wolters Kluwer ČR [vid. 2016-04-28].

VII. Seznam obrázků, tabulek a grafů