Uloga knjižnice u zaštiti privatnosti na internetu i borbi protiv masovnog nadziranja

Džapo, Paula

Sveučilište u Zadru

Odjel za informacijske znanosti
Diplomski sveučilišni studij Informacijske znanosti - knjižničarstvo

Paula Džapo

Uloga knjižnica u zaštiti privatnosti na internetu i borbi protiv masovnog nadziranja

Diplomski rad

Zadar, 2016.

Sveučilište u Zadru

Odjel za informacijske znanosti
Diplomski sveučilišni studij Informacijske znanosti - knjižničarstvo

Uloga knjižnica u zaštiti privatnosti na internetu i borbi protiv masovnog nadziranja

Diplomski rad

Student/ica:
Paula Džapo

Mentor/ica:
doc. dr. sc. Martina Dragija Ivanović

Zadar, 2016.

Izjava o akademskoj čestitosti

Ja, **Paula Džapo,** ovime izjavljujem da je moj **diplomski** rad pod naslovom **Uloga knjižnica u zaštiti privatnosti na internetu i borbi protiv masovnog nadziranja** rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Ni jedan dio mojega rada nije napisan na nedopušten način, odnosno nije prepisan iz necitiranih radova i ne krši bilo čija autorska prava.

Izjavljujem da ni jedan dio ovoga rada nije iskorišten u kojem drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Zadar, 30. rujan 2016.

Sadržaj

Sažetak

Ovaj rad se bavi temom zaštite privatnosti na internetu i ulozi knjižnica u tome te borbi protiv masovnog nadziranja. Rad je podijeljen u dva dijela, teorijski dio koji se temelji na literaturi i istraživački dio. Teorijski dio se bavi pojmovima i definicijama privatnosti i zaštite privatnosti na internetu te knjižničnoj ulozi u toj zaštiti kao i pojmom masovnog nadziranja koje su provodile vlade i obavještajne agencije, poput američke Nacionalne sigurnosne agencije (eng. NSA) i njihovim programima za nadziranje milijuna ljudi diljem svijeta. Također, teorijski dio se bavi knjižničnom borbom protiv masovnog nadziranja i alatima koje knjižničari koriste i edukacijama koje provode kako bi zaštitili privatnost korisnika na internetu. Istraživački dio rada prikazuje istraživanje provedeno metodom ankete među studentima Informacijskih znanosti na Sveučilištu u Zadru čiji cilj je bio saznati na koji način studenti štite privatnost na internetu te doznati njihova mišljenja o ulozi knjižnica u zaštiti privatnosti na internetu te borbi protiv masovnog nadziranja. Istraživanjem se želi osvijestiti buduće knjižničare o opasnostima kršenja privatnosti na internetu i masovnog nadziranja kojima se ugrožava njihova i privatnost knjižničnih korisnika. Ovaj rad je namjenjen kao temelj za daljnja istraživanja o navedenoj temi i moguću provedbu edukacija u knjižnicama kao i ukazivanje na probleme koji prijete privatnosti na internetu.

Ključne riječi: privatnost, internet, knjižnice, masovno nadziranje

1. Uvod

U vrijeme kada su tehnologije dio svakodnevice i mnoge osobe koriste barem jednu društvenu mrežu i svakodnevno pretražuju internet u potrazi za informacijama i drugim podacima koji ih zanimaju, privatnost na internetu je važnija no ikada. Korisnici društvenih mreža na svojim profilima ostavljaju veliku količinu osobnih podataka, od imena i prezimena, slika do broja mobitela, kao i raznih mišljenja i objava koje dijele s drugima. Kada pojedinac svjesno i svojom voljom dijeli te informacije, to radi jer to želi, no postoji mnogo slučajeva kada se njegova privatnost narušava jer su podaci koje je ta osoba željela zadržati za sebe ili podijeliti samo s određenim brojem ljudi, završili u krivim rukama. Danas pojam privatnosti obuhvaća ne samo privatnost koju pojedinac ima u svome domu, onu koja je „opipljiva“, već i privatnost na internetu. Uzevši u obzir činjenicu da privatnosti na internetu skoro pa nema, ovaj rad se bavi zaštitom privatnosti na internetu, ulozi knjižnica u zaštiti te njihovoj borbi protiv masovnog nadziranja.

U radu su prikazani pojmovi privatnosti i načini zaštite, uloga knjižnica u zaštiti privatnosti na internetu i borbi protiv masovnog nadziranja. Prvi dio rada bavi se različitim definicijama i podijelama privatnosti te zašto osobe žele zaštiti svoju privatnost, privatnosti na internetu i prijetnjama koje se tamo nalaze. Drugi dio rada se bavi pojmom masovnog nadziranja posebno nadziranjem koje su provodile američka vlada i obavještajne agencije poput Nacionalne sigurnosne agencije (NSA) koje je razotkrio Edward Snowden i programi kojima su se služili kako bi došli do podataka milijuna osoba diljem svijeta. Treći dio rada se bavio knjižnicama i knjižničarima i kako se oni bore protiv masovnog nadziranja i zaštite privatnosti korisnika na internetu, kako u sadašnjosti tako i u prošlosti te problemi s kojima su se susretali. Također, rad se bavio i projektima koji se u SAD-u provode u knjižnicama kao dio edukacije u zaštiti privatnosti na internetu te alatima koji se koriste kao dio te edukacije i zaštite. Literatura se uglavnom sastojala od jedinica na engleskom jeziku, jer domaće literature koja se bavi ovom temom nema dovoljno te su opisivani projekti bili usmjereni na američke projekte jer su knjižničari iz tog dijela svijeta započeli s detaljnijom zaštitom privatnosti korisnika na internetu u knjižnicama.

Provedeno je istraživanje kako bi se saznalo kako i na koji način studenti Informacijskih znanosti u Zadru štite privatnost na internetu te koje je njihovo mišljenje o ulozi knjižnica u

zaštiti privatnosti na internetu te borbi protiv masovnog nadziranja. Rezultati istraživanja mogu poslužiti kao temelj na kojem će se provoditi daljnja istraživanja o istim i sličnim temama te možda potaknuti i hrvatske knjižnice da počnu s provedbom edukacija knjižničara i korisnika o zaštiti privatnosti na internetu.

2. Privatnost

2.1. Definicija privatnosti

Svaki pojedinac ima pravo na privatnost. Svaki pojedinac ima pravo na kontrolu onoga što dijeli s drugima, kao što su informacije, činjenice i druge osobne stvari koje mogu biti privatne. Osim što pojedinci imaju pravo na kontrolu, imaju i pravo na odluku kako će se privatne informacije koristiti. Pojedinci odlučuju i kontroliraju ono što žele dijeliti s drugima, primjerice, neke informacije te osobe žele učiniti javnima, dok druge sasvim privatne, zadržavaju za sebe ili dijele s malim brojem ljudi. Privatnost također označava i pravo na tjelesnu privatnost ili pravo pristupa nekom mjestu, kao na primjer mjestu stanovanja osobe. Privatnost označava ono što je osobno, što nije javno i što pojedinac želi zadržati za sebe ili u krajnjem slučaju napraviti javnim no do određene granice.

Pojam privatnosti se ne može definirati na samo jedan način, svatko može dati svoju verziju definicije privatnosti koja može biti točna i primjenjiva na različite situacije u kojima se razmatra pojam privatnosti. To znači da postoje višestruke definicije i pogledi na privatnost. Prema Warrenu i Brandeisu[1], koji su 1890. godine objavili članak pod nazivom "Pravo na privatnost", privatnost se treba promatrati kao opće pravo na imunitet osobe. Pravo na privatnost, kao dio općenitijeg prava na imunitet osobe, je povezano s pravom na nečiju osobnost, pravo osobe da ima svoj mir.

Međunarodni savez knjižničarskih društava i ustanova (eng. International Federation of Library Associations and Institutions – IFLA) navodi kako je privatnost definirana kao ljudsko pravo u članku 12 Opće deklaracije,

> „Nitko ne smije biti podvrgnut samovoljnom miješanju u privatni život, obitelj, dom ili dopisivanje, niti napadima na čast ili ugled."

Privatnost je potrebna kako bi se omogućio pristup informacijama i njihovom korištenju bez straha od posljedica.[2]

[1] Usp. Buitelaara, J. C. Privacy and Narrativity in the Internet Era. // The Information Society: An International Journal, 30:4. Str. 267.
[2] Usp. IFLA-ina Izjava o privatnosti u knjižnici. URL: http://www.hkdrustvo.hr/clanovi/alib/datoteke/file/IFLA-ina%20Izjava%20o%20privatnosti.pdf (2016-04-03)

Boban[3] navodi kako je pravo na privatnost osnovno čovjekovo pravo, što uključuje međunarodno, ustavno pravo i osobno pravo te označava nezamjenjiv element koji štiti čovjeka od prekomjernih posezanja državne vlasti, javnosti i drugih pojedinaca u pojedinčevu duševnu, prostornu i informacijsku privatnost. To znači da je pravo na privatnost ljudsko pravo, koje je međunarodno priznato i zaštićeno ustavom dok je osobno pravo zaštićeno instrumentima građanskog prava. Boban govori i o pojmu *protupravnosti*, koji označava granicu koju pojedinac ne smije prijeći u zadiranju u privatnost drugog pojedinca, gdje kršenje prava na privatnost predstavlja interes pojedinca za očuvanje vlastite privatnosti te je prvenstveno riječ o osobi i osobnim podacima, a osoba se štiti zaštitom podataka od neodgovarajuće uporabe.[4]

A.R. Miller objašnjava važnost informacijskog samoodređenja za očuvanje privatnosti i navodi kako osnovno svojstvo učinkovitog prava na privatnost je sposobnost pojedinca da kontrolira cirkulaciju informacija koje se odnose na sebe, a to je moć koja je često neophodna za održavanje društvenih odnosa i osobnih sloboda. U slučaju da pojedinac više ne može utvrditi u kojoj mjeri se otkriva svijetu, tada je privatnost opljačkana temeljne vrijednosti, a to je prilika da slobodno odlučujemo za sebe.[5]

Dakle, pravo na privatnost je pravo svake osobe koje je priznato i zaštićeno, kako je Boban navela u svom radu, privatnost štiti osobu i time se odvaja ono što je privatno i ono što je javno. Svatko privatnost koristi na svoj način jer je to pravo pojedinca te svatko dijeli s drugima pojedinosti o sebi koje smatra da pripadaju u javnosti, no bilo kakvo drugo dijeljenje koje nema odobrenje osobe se smatra kršenjem privatnosti, samim time i kršenjem zakona. Zbog činjenice da je privatnost zaštićena ustavom, to znači da i državne institucije te ostale institucije trebaju zaštititi pravo na privatnost pojedinca, a među tim institucijama su i knjižnice koje godinama rade na zaštiti privatnosti, čak i više od drugih institucija, ponajprije državnih, koje bi trebale više vremena posvetiti temi privatnosti i zaštiti iste.

[3] Usp. Boban, Marija. Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu. // Zbornik radova Pravnog fakulteta u Splitu 49, 3(2013). Str. 582-583.
[4] Usp. Isto. Str. 583.
[5] Usp. Buitelaara, J. C. Nav. dj.

Nadalje, Horvat[6] navodi kako pravo na osobnost podrazumijeva pravo da pojedinac bude sam kada to izabere i da sam odluči s kim će se družiti te da ono uključuje i pravo pojedinca da ga se ne nadzire. Također navodi kako je za knjižničare relevantan Zakon o zaštiti tajnosti podataka, koji utvrđuje da postoje tajni podaci, koje dalje dijeli na državne, vojne, službene, poslovne i profesionalne. Profesionalnu tajnu zatim definira kao podatke o osobnom ili obiteljskom životu stranaka koje saznaju svećenici, odvjetnici, zdravstveni i socijalni djelatnici, te druge službene osobe u obavljanju svojega poziva. Iako knjižničari nisu posebno spomenuti, oni se svakako mogu ubrojiti u „druge službene osobe“, koje tijekom obavljanja svojega posla saznaju ne samo osobne podatke o svojim korisnicima, poput imena, adrese, telefonskoga broja i sl., koje su korisnici dužni dati pri upisu u knjižnicu, već i mnogo podataka o njihovim sklonostima, interesima i čitalačkim navikama. Ti, pak, podaci pripadaju domeni privatnosti, i otkrivaju mnogo o samoj osobi.

Svaka država u svom Ustavu ima propisan zakon koji se odnosi na privatnost i pravo pojedinca na privatnost. To uključuje i Republiku Hrvatsku koja u svom Ustavu[7] koji se odnosi na Zaštitu ljudskih prava i temeljnih sloboda, u odjeljku 2. Osobne i političke slobode i prava članak 35. navodi,

> „Svakom se jamči štovanje i pravna zaštita njegova osobnog i obiteljskog života, dostojanstva, ugleda i časti.“

Time se pojednicima osigurava pravo na privatnost od same države odnosno njihovih vlada, javnih tvrtki ili bilo kojih drugih javnih ustanova koje na neki način mogu kršiti privatnost osoba, bez obzira da li je ta osoba javna ličnost, kao što su glumci, pjevači, političari ili osobna ličnost koja nije izložena očima javnosti kao popularne osobe.

Možemo zaključiti da osoba želi zaštititi privatnost zbog sljedećih razloga[8]:

- *Psihološki* – pojedincima je potreban osobni prostor, kako u javnosti, tako i u vlastitom domu.

---

[6] Horvat, Aleksandra. Javno i tajno u knjižničarskoj struci. URL: http://dzs.ffzg.unizg.hr/text/jit_u_%20knjiz.htm (2016-04-10)

[7] Hrvatski Sabor. Ustav Republike Hrvatske. URL: http://www.sabor.hr/Default.aspx?art=1841 (2016-04-01)

[8] Usp. Gledec, Gordan; Mikuc, Miljenko; Kos, Mladen. Sigurnost u privatnim komunikacijskim mrežama. // MIPRO 2008 - HEP Informatička i komunikacijska tehnologija (ICT) u vođenju elektroenergetskog sustava / uredio Josip Kljajić. Rijeka: Denona Ltd., Zagreb, 2008. Str. 35. URL: https://www.fer.unizg.hr/_download/repository/Sigurnost_u_privatnim_komunikacijskim_mrezama.pdf (2016-04-08)

- *Društveni* – pojedinci moraju biti slobodni kako bi nesputano komunicirali s drugima i otvoreno izražavali svoje mišljenje, bez osjećaja da ih netko promatra i nadgleda.
- *Ekonomski* – pojedinci moraju biti slobodni kako bi mogli biti inovativni.
- *Politički* – pojedinci moraju imati slobodu razmišljati, raspravljati i djelovati, a nadzor nad njima sputava njihovo ponašanje i izražavanje te ugrožava demokraciju.

Privatnost je složen pojam, koji uključuje osobno, društveno, etičko i drugo sudjelovanje u pitanjima zakona i prava na privatnost. Pojedinci trebaju biti zaštićeni od kršenja privatnosti, bilo od strane države ili drugog pojedinca, što je i propisano u mnogim zakonima i ustavima država diljem svijeta. Pojedinci žele zaštititi privatnosti iz nekolicine razloga, kao što su psihološki ili društveni, žele imati opciju odluke onoga što hoće i što neće dijeliti s drugima, što će zadržati za sebe i imati pravo da ih se pusti na miru. Pravo na privatnosti je fundamentalno pravo svake osobe i treba se zaštititi, na bilo koji način.

2.2. Podjela privatnosti

Autor koji zauzima posebno mjesto u teoriji privatnosti je Alan Westin. Svojim radovima iz 60-ih godina prošlog stoljeća koji su se bavili privatnošću i pravom na privatnost, potaknuo je zemlje i pokrete koji su se bavili temom privatnosti prema boljoj zaštiti iste. Njegova teorija privatnosti se bavi činjenicom da ljudi sami sebe štite tako što privremeno ograniče pristup drugima sebi. Za Westina privatnost je tvrdnja pojedinaca, skupina ili institucija kako bi se utvrdilo kada, kako i do koje mjere se informacije o njima predstavljaju drugima. Također, privatnost je dobrovoljno i privremeno povlačenje osobe iz društva putem tjelesnih ili duševnih sredstava. Westin[9] navodi četiri funkcije privatnosti:

- *Osobna autonomija* se odnosi na želje kojima se izbjegava manipulacija, dominacija ili izloženost od strane drugih;
- *Emocionalno izdanje* se odnosi na oslobađanje od napetosti društvenog života, kao što su zahtjevi uloga, emocionalna stanja, manja odstupanja i upravljanje gubitaka i

[9] Usp. Privacy Online: perspectives on privacy and self-disclosure in the social web. Berlin. Springer, 2011. Str. 10.

tjelesnih funkcija. Privatnost, bilo kada smo sami ili s drugima, daje pauzu od socijalnih zahtjeva te nam tako daje mogućnost za emocionalno oslobađanje;

- *Samovrednovanje* se odnosi na integriranje iskustva u smislene obrasce i izvršavanje individualnosti na događaje;
- Konačna funkcija, *ograničena i zaštićena komunikacija*, ima dva aspekta: ograničena komunikacija postavlja međusobne granice dok zaštićena komunikacija omogućuje dijeljenje osobnih informacija sa pouzdanim osobama;

Druga teorija privatnosti koja je opće prihvaćena je ona Irwina Altmana[10] koja se usredotočuje na individualnu i grupnu privatnost i ponašanje koje djeluje kao koherentan sustav. Privatnost za Altmana je selektivna kontrola pristupa sebi. Privatnost ima pet svojstava:

- privatnost uključuje dinamičan proces međuljudske granice kontrole;
- postoje dvije razine privatnosti – željena i stvarna;
- privatnost je ne-monotona funkcija, s optimalnom razinom privatnosti i mogućnosti da je imamo previše ili premalo;
- privatnost je dvosmjerna, uključuje komunikaciju između dvije ili više osoba;
- privatnost djeluje na individualnoj i grupnoj razini;

Svojstva i funkcije privatnosti naglašavaju činjenicu da pojedinci trebaju imati pravo na izbjegavanje manipulacije od drugih, privatnost daje mogućnost osobi da bude sama i ima mjesto na kojem joj drugi neće smetati, posjedovanje individualnosti je važno i pripadanje nekoj zajednici je sastavni dio života no saznanje o samome sebi i svojoj privatnosti je također bitno. Privatnost se može čuvati samo za sebe ili dijeliti s drugima, no samo one dijelove koje osoba odluči da su vrijedni dijeljenja, one osobne i najintimnije osoba možda ne želi dijeliti već zadržati za sebe, što je i apsolutno pravo koje posjeduje.

Boban[11] dijeli privatnost osobe na:

- *Prostorna privatnost* – aspekt privatnosti koji se odnosi na dom i drugi prostor u kojem osoba vodi život zasebno od drugih.

[10] Usp. Isto. Str. 11.
[11] Usp. Boban, Marija. Nav. dj. Str. 584-586.

- *Informacijska privatnost* – aspekt privatnosti koji se odnosi na prikupljanje podataka o osobi, upravljanje tim podacima i njihovo korištenje.
- *Komunikacijska privatnost* – aspekt privatnosti koji se odnosi na osobne zapise te dopisivanje odnosno bilo koji drugi oblik komuniciranja.

Gledec, Mikuc i Kos[12] privatnost dijele na:

- *Privatnost osobe* – vezana je uz integritet tijela osobe, pa se često naziva i tjelesnom privatnošću, a problemi vezani uz ovu vrstu privatnosti često su zdravstvene prirode.
- *Privatnost ponašanja* – odnosi se na sve pojavnosti ponašanja, posebice na spolne navike i orijentaciju, političku aktivnost, religioznu pripadnost.
- *Privatnost osobne komunikacije* – pojedinci imaju interes za međusobnom komunikacijom koristeći različite komunikacijske medije te ne žele da ta komunikacija bude pod nadzorom drugih osoba ili organizacija.
- *Privatnost osobnih podataka* – pojedinci ne žele da podaci o njima budu dostupni ostalim pojedincima i organizacijama, a čak i kad podatke posjeduju drugi, osoba mora imati određeni stupanj nadzora nad tim podacima i načinom njihova korištenja.
- *Privatnost informacije* – porastom tehnologija, posljednje dvije privatnosti se isprepliću te kombinacijom dimenzija privatnosti osobne komunikacije i privatnosti osobnih podataka nastaje nova privatnost, privatnost informacije.

Privatnost osobe se može podijeliti na privatnost u prostoru koja se odnosi na činjenicu da pojedinac u svome vlastitom domu ima privatnost koju ne želi dijeliti s drugima bez pristanka, što se iskazuje kroz nekoliko činjenica kao što su postavljanje zastora na prozor ili zaključavanje vrata čime se iskazuje želja za privatnom sferom u kojoj mogu sudjelovati samo odabrani, a ne većina. To je povezano i s privatnosti osobe koja svoju intimu dijeli samo s osobama koje poznaje ili vjeruje te pruža uvid u osobne stvari kao što su npr. spolna orijentacija, koja je osobna i taj pojedinac ne želi da druge osobe ili organizacije znaju za to. Pravo na zaštitu osobnih podataka je također važna, knjižničarstvo kao profesija radi na tome da u svojim ustanovama štiti osobne podatke korisnika, nudi edukacije koje uče korisnike informacijskoj pismenosti i kako zaštititi sebe i svoju privatnost od uplitanja drugih ili organizacija. Knjižnice i knjižničari se bore za zaštitu privatnosti i intelektualne slobode, informacija i autonomije korisnika i drugih pojedinaca, savjetovanjem o čuvanju podataka i

[12] Usp. Gledec, Gordan; Mikuc, Miljenko; Kos, Mladen. Nav. dj. Str. 35.

nadzorom nad njima. Pojedinci trebaju imati kontrolu nad tim podacima, a ne korporacije ili vlasti, koje su do tih podataka došli na ilegalan način odnosno bez pristanka pojedinca.

Prostorna ili fizička privatnost koju pojedinci imaju je pod velikom zaštitom, primjerice provala u stan ili auto je kažnjiva zakonom te se smatra povredom privatnosti osobe, dok se u mislima većine privatnosti koja se tiče tehnologije ili interneta, odnosno informacijskoj privatnosti, pridodaje manje važnosti, iako je i ono podložno kažnjavanju ako se prekrši, o čemu će se pisati u nastavku rada.

3. Privatnost na internetu

Dok je fizička privatnost pojedinca koja se temelji na „opipljivim“ stvarima više zaštićena i društvo na nju općenito obraća pozornost, privatnost na internetu je još uvijek tema kojoj se ne pridaje prevelika važnost, odnosno nije dovoljno razvijena svijest da se privatnost koju prakticiramo u stvarnom životu odnosi i na privatnost na internetu. Danas, kada velika većina ljudi svakodnevno koristi tehnologiju za različite svrhe, privatnost se proširila i na takve medije. Pojedinci sve više svojih osobnih podataka i informacija dijele preko interneta, posebno se proširilo nakon što su različite društvene mreže, poput Facebooka, Twittera, MySpacea i drugih, postale popularne te se društvena sfera komunikacije preoblikovala u nešto novo, gdje je sve manje komunikacije u živo, licem u lice, već se sve više komunicira preko ekrana. Zato je važno da se definicija privatnosti širi te obuhvati tehnologije i internet. Pojedinci nisu ni svjesni koliko je važna zaštita privatnosti na internetu, gdje velika količina podataka koju osobe nisu htjele podijeliti ni s kim završe u rukama kompanija, koje putem rudarenja podataka dolaze do raznih informacija o pojedincima. Jednostavno i svakodnevno pretraživanje web tražilice kao što su na primjer Google ili Yahoo!, zainteresiranim pojedincima mogu proslijediti naše podatke o stranicama koje posjećujemo, stvarima koje kupujemo, glazbi koju smo slušali. Oglasi koji se pojavljuju na stranicama su povezani s onim što osoba pretražuje. Na primjer, ako netko pomoću tražilice pretražuje hranu za kućne ljubimce, oglasi koji će se nakon toga prikazivati bit će povezani s tim upitom. Upravo na taj način Google prikuplja informacije o web pretragama i stvara profil korisnika koji toga u najviše slučajeva nije niti svjestan. Sve je to dovelo do stvaranja termina „privatnost je mrtva“, koja opisuje da u današnjem tehnološkom svijetu u kojem se nalazimo, privatnosti nema te sve što dijelimo ili pretražujemo zapravo dijelimo s drugima, često bez ikakvog znanja da smo to napravili.

S druge strane, pojedinci samovoljno odaju svoje osobne podatke, bez prisile kompanija ili vlada. Pojedinci imaju po nekoliko društvenih mreža na kojima iznose podatke, svjesno ili nesvjesno, što vladama i korporacijama koje se bave prikupljanjem podataka u marketinške ili druge svrhe olakšava posao. Jednim klikom mogu saznati informacije o osobama koje mogu iskoristiti za svoje potrebe.

3.1. Prijetnje privatnosti na internetu

Iako su mnoge online usluge besplatne, neke od najvećih su financirane oglasima koji nastaju na temelju korisničkih podataka. Što se više podataka prikupi o online aktivnostima to će oglasi biti učinkovitiji. Korištenje podataka, profila, financijskih statusa i drugih informacija je bitno u marketinškim strategijama online biznisa te sve više raste s pojavom novih osobnih podataka. Na primjer, tvrtka AVG prodaje podatke o pretraživanju oglašivačima kako bi zaradili od svog besplatnog antivirusnog programa. Koristeći se uslugom, pojedinci dobiju besplatni antivirusni program i zaštitu u zamjenu za njihove osobne podatke koji se prikupljaju i prodaju za zaradu. Količina osobnih podataka se proširila kao rezultat pojave društvenih mreža, koje su otvorile nove mogućnosti komunikacije i potakle prikupljanje osobnih podataka za velike tvrtke.[13]

Razne web stranice prikupljaju podatke poput datuma i vremena posjeta toj stranici, grada, države, IP adrese, operacijskog sustava koji se koristi, web preglednika i verzije preglednika, rezolucije ekrana, jezika, je li osoba došla na tu stranicu preko računala ili telefona, koji je internetski pružatelj usluge (ISP) koji osoba koristi, koliko se zadržala na toj stranici i koje sadržaje je pregledala. Takve podatke svakodnevno ostavljaju milijuni korisnika interneta, često bez znanja da su takvi podaci sada dostupni drugima. Na prvi pogled možda ne izgleda kao velika količina podataka, no zapravo se puno toga sazna o osobi koja je posjetila stranicu koja ima ugrađene parametre koji otkrivaju nabrojane informacije, a da osoba nije ni svjesna da je toliko otkriveno o njoj samo jednim klikom.

Dalje u tekstu će se pisati o opasnostima koje prijete privatnosti na internetu, preko kolačića, web preglednika i tražilica, društvenih mreža do phishinga i spywarea. Važno je pisati o tome, jer mnogi korisnici nisu svjesni da se preko toga prikuplja ogromna količina podataka o njima i o onome što pregledavaju na internetu. Rad dalje objašnjava neke od najčešćih načina preko kojih se prijeti privatnosti na internetu.

[13] Usp. Clark, IJ. The digital divide in the post-Snowden era. // Journal of Radical Librarianship, 2(2016). URL: http://infoism.co.uk/digitial-divide-snowden.pdf (2016-03-20). Str. 6.

3.1.1. Kolačići

Kolačići (eng. Cookies) su naziv za podatke koje web poslužitelj prosljeđuje pregledniku kad korisnik pristupi mrežnom mjestu. Nakon primitka podataka, preglednik spremi te podatke na disk te svaki put kada računalo pristupi tom istom mrežnom mjestu, preglednik tu pohranjenu informaciju šalje na sjedište. Najčešće korišteni preglednici podržavaju korištenje kolačića. Budući da protokol HTTP ne čuva stanja, tj. nije moguće pratiti ponašanje korisnika samo na temelju podataka koji su dostupni putem protokola HTTP, koristi se tehnologija kolačića kako bi se moglo identificirati svako računalo pri ponovljenom zahtjevu za dohvatom nekog resursa na web poslužitelju. Pomoću kolačića web sjedište korisničkom pregledniku dodjeljuje jedinstveni identifikator pomoću kojeg će ga moći prepoznati u kasnijim zahtjevima. Iako kolačić ne može identificirati korisnika, moguće je pomoću njega povezati različite informacije o korisniku i tako stvoriti svojevrsni korisnički profil koji se može zloupotrijebiti prilikom na primjer oglašavanja ili prodaje. No, preglednici omogućuju kontrolu korisnika nad načinom na koji se kolačići pohranjuju na računalo, iako većina korisnika to ne zna i time ostavlja otvorenom mogućnost narušavanja njihove privatnosti. [14]

Kolačići se po porijeklu mogu podijeliti u skupine: obični kolačići (eng. First-party cookies), kolačići trećih strana (eng. Third-party cookies), kolačići za praćenje (eng. Tracking cookies) i flash kolačići. Glavna osobina običnih kolačića je da su nastali na istom web poslužitelju na kojem se nalazi stranica koju korisnik trenutno pregledava. Obične kolačiće može koristiti samo poslužitelj koji ih je i napravio pa su jedine točke rizika web poslužitelj i korisničko računalo. Budući da nisu posebno zaštićeni (npr. kriptiranjem), zlonamjerni korisnik mora samo pronaći način kako pristupiti podacima na disku korisnika te naravno, mora znati koji kolačić sadrži tražene informacije. Složena web stranica se sastoji od velikog broja elemenata. Svi elementi jedne web stranice se ne moraju nužno nalaziti na istom poslužitelju, nego se dohvaćaju s nekoliko poslužitelja. Primjer su reklame ili flash elementi na web stranici, a kako bi ti elementi bili ispravno prikazani, nekada je potrebno koristiti kolačiće koji se zovu kolačići trećih strana. Kolačići za praćenje je naziv za kolačiće s kojima je moguće saznati točno kojim redoslijedom je korisnik otvarao web stranice. Pomoću identifikatora kojeg je korisnik dobio kada prvi put posjeti web stranicu i zapisa u web poslužitelju moguće je odrediti točno kada je korisnik pristupio nekoj stranici. Kolačići za praćenje na poslužitelju se

[14] Usp. Gledec, Gordan; Mikuc, Miljenko; Kos, Mladen. Nav. dj. Str. 37.

najčešće koriste kako bi se dobila statistika pristupa pojedinim stranicama i ne predstavlja sigurnosni rizik jer se podaci koriste samo na tom web poslužitelju. Ako su kolačići za praćenje ujedno i kolačići trećih strana, onda sigurnosni rizik postoji jer su informacije o korisnikovim navikama dostupne i drugim poslužiteljima. Takve informacije se najčešće koriste u marketinške svrhe kako bi se procijenile navike potrošača i prema tome izradila strategija promocije nekog proizvoda. Međutim, te informacije se mogu koristiti i kako bi se korisniku na neki način naudilo (krađa identiteta, otkrivanje osjetljivih informacija, zlonamjerni napad na korisnikovo računalo itd.), a ne samo u promidžbene svrhe.[15]

Sve češći sigurnosni rizik su flash kolačići koje stvara program Adobe Flash Player prilikom prikaza flash animacija i objekata. Flash kolačići se koriste za prikupljanje podataka svaki puta kada korisnik otvori web stranicu s flash elementom (jer je svakom korisniku s flash kolačićem dodijeljen jedinstveni identifikator). Na taj način se mogu bilježiti sve stranice s flash elementom koje je korisnik posjetio. Predstavljaju isti sigurnosni rizik kao i prije spomenuti kolačići, ali njih preglednici ne mogu zabraniti niti nadgledati. Zbog toga flash kolačići ostaju na korisnikovom računalu duže od običnih, a njihovo trajno brisanje je složeniji postupak od brisanja običnih kolačića čak i uz upotrebu dodatne programske podrške jer neki flash kolačići stvaraju pričuvnu kopiju kojom se obrisani flash kolačić ponovo vraća na korisnikovo računalo. [16]

3.1.2. Web preglednici i tražilice

Preko web preglednika[17] korisnik komunicira s web poslužiteljima te je preglednik taj koji prosljeđuje informacije o korisniku do web poslužitelja. Što manje podataka preglednik šalje, manje podataka će se moći saznati o korisniku. Web preglednik uvijek šalje korisnikovu IP adresu iz koje se može saznati cijeli niz informacija, od ISP-a, države pa čak i mjesta gdje se korisnik nalazi. Sve više preglednika pruža mogućnost privatnog pretraživanja, a korištenjem preglednika na ovaj način, preglednik ograničava ili mijenja informacije o korisniku koje šalje kako bi povećao korisnikovu privatnost. Također, automatski se zabranjuju kolačići i izvođenje skripti koje bi mogle pristupiti korisnikovim informacijama. Po završetku

[15] Usp. Privatnost na internetu. URL: http://security.lss.hr/images/dokumenti/lss-pubdoc-2010-10-002.pdf (2016-04-08). Str. 7-9.
[16] Usp. Isto.
[17] Usp. Isto. Str. 10-11.

pretraživanja, podaci o tom pretraživanju se brišu. Problem koji se stvara je nemogućnost korištenja web stranica za internet bankarstvo ili kupovinu koje ipak zahtijevaju informacije o korisniku kako bi ih on mogao koristiti, no pravi problem je što preglednik ne može nikada ostvariti potpunu anonimnost korisnika te se ova mogućnost mora koristiti u kombinaciji sa servisima za postizanje anonimnosti poput anonimnih proxy poslužitelja ili s nekim drugim servisima.

Unatoč uslugama poput privatnog pretraživanja, preglednici tijekom svog rada prikupe značajnu količinu podataka o korisniku. Ti podaci se u pravilu ne prikazuju trećim stranama, ali treće strane mogu do njih doći iskorištavajući sigurnosne propuste u korisnikovom pregledniku ili operacijskom sustavu. Jedan način pristupanja tim podacima je preko dodataka koji se instaliraju u web preglednik (eng. plug-in ili add-on). Autori dodataka nemaju privatnost korisnika na umu dok stvaraju dodatak, a dodaci nisu podvrgnuti istim strogim testovima kojima se provjerava sigurnost i čuvanje privatnosti kao oni kroz koje moraju proći sami preglednici. Zbog toga, svaki instalirani dodatak predstavlja sigurnosni rizik. U samim preglednicima kroz zadnjih nekoliko godina otkriveni su brojni sigurnosni propusti koji omogućuju ovakve napade. Kako u relativno kratkom roku od otkrivanja propusta proizvođači web preglednika objavljuju zakrpe kojima se propusti ispravljaju te ih implementiraju u nove inačice preglednika, korisnicima se preporuča da svoje preglednike redovito ažuriraju (instaliraju zakrpe ili nadograđuju na nove inačice).[18]

Svi korisnici tijekom svog rada koriste tražilice kako bi pronašli neki podatak na internetu. Pri tome, tražilica može zabilježiti korisnikovu IP adresu, vrijeme i pojam koji se pretraživao. Prikupljanjem podataka o svim korisnikovim pretraživanjima mogu se dobiti ključne informacije o korisniku, a sam korisnik može nehotice otkriti informacije koje se mogu iskoristiti protiv njega, kao na primjer u sudskim postupcima. Ako korisnik u tražilicu upiše svoje ime, želeći provjeriti koliko se o njemu može saznati preko interneta, njegovo ime i prezime se može povezati s IP adresom koju koristi. Prateći daljnja korisnikova pretraživanja i skupljajući dodatne podatke, moguće je zaključiti da je ime upisano u tražilicu zaista korisnikovo ime. Jednom kada se ime poveže s IP adresom, a time i s mjestom stanovanja (tj. pružateljem internetskih usluga), moguće je saznati odakle je korisnik, možda čak i njegovu adresu stanovanja. Sve tražilice bilježe korisničke upite, a kao razlog navode pružanje bolje

[18] Usp. Privatnost na internetu. Str. 10.

usluge korisnicima jer na temelju prijašnjih pretraga mogu bolje odrediti što korisnika zanima i tako pružiti bolji odgovor na upit. [19]

Problem je što je vremenski period u kojem tražilice bilježe korisničke pretrage i dulji nego što je to potrebno za razloge koje su naveli. Tri najveće internetske tražilice (Google, Yahoo!, Bing) čuvaju podatke o korisnikovoj IP adresi i njegovim pretraživanjima, gdje Yahoo! čuva podatke 90 dana, Bing 6 mjeseci, a Google čak 9 mjeseci.[20] Nakon isteka ovog vremena, korisnička IP adresa povezana s upitima briše se iz baze podataka. Do tada, postoje zapisi u kojima su zabilježeni svi korisnikovi upiti i moguće je na temelju pojmova koje je pretraživao saznati čime se bavio u to vrijeme. Korisnikova privatnost se dodatno može narušiti ako se koriste tražilica i poslužitelj elektroničke pošte kod istog ISP-a (npr. Google tražilica i Gmail). Tada se korisnikova elektronička pošta može povezati s pretraživanjima i dobiti još više informacija. Korištenjem dodatnih usluga povećava se količina informacija koje stoje na raspolaganju tom pružatelju usluga. Korisnik ne može biti siguran koliko dobro pružatelj usluga čuva njegove podatke i prikazuje li ih nekim drugim stranama s kojima ima ugovor. Država može sudskim nalogom zatražiti podatke o korisnikovim pretraživanjima ako se sumnja da bi u njima mogli postojati dokazi koji povezuju korisnika s nekom nezakonitom radnjom. Takvi slučajevi su rijetki, ali ipak postoje i zbog toga postoji opravdana zabrinutost korisnika za njihovu privatnost dok se koriste tražilicama.[21]

3.1.3. Društvene mreže

Društvene mreže su danas bez sumnje najraširenija pojava na internetu, s više od milijardu korisnika i preko dvadeset, ako ne i više, različitih društvenih mreža koje se koriste svakodnevno diljem svijeta. Strauß i Nentwich[22] navode kako su Boyd i Ellison definirali društvene mreže kao „web bazirane usluge koje omogućuju pojedincima da osmisle javni ili polu - javni profil unutar omeđenog sustava, artikuliraju popis drugih korisnika s kojima dijele vezu i pregledavaju njihov popis.“ U skladu s društvenom potrebom za komunikacijom, društvene mreže pružaju širok spektar mogućnosti za dijeljenje, razmjenu, stvaranje sadržaja i

[19] Usp. Isto.
[20] Usp. Privatnost na internetu. URL: http://security.lss.hr/images/dokumenti/lss-pubdoc-2010-10-002.pdf (2016-04-08). Str. 11.
[21] Usp. Isto.
[22] Usp. Strauß, Stefan; Nentwich, Michael. Social networking sites, privacy and the blurring boundary between public and private spaces. // Science and Public Policy 4(2013). Str. 724-725.

suradnju s drugima. Jedna od glavnih karakteristika društvenih mreža je dijeljenje osobnih podataka i informacija, jer svaki oblik društvene interakcije zahtijeva određenu količinu informacija o uključenim stranama. Društvene mreže su uglavnom dizajnirane kako bi potakle interakciju i navele korisnika na otkrivanje osobnih podataka. Društvene mreže su povezane s Web 2.0. koji omogućava širok opseg komunikacije i interakcije. Prve društvene mreže su se razvile u kasnim 90-im godinama, raširile su se 2003., a danas najpoznatija društvena mreža, Facebook, nastao je 2004., a Twitter 2006. godine. Veliki dio društvenih mreža su korisnički osobni profili s informacijama koje korisnici navedu o sebi, kao što su interesi i aktivnosti, koji se nalaze u digitalnom prostoru kojem se obično može pristupiti samo uz registraciju. Najpoznatije društvene mreže su Facebook, Twitter, MySpace, Tumblr, Google+, a među poznatijima su još i Bebo, LinkedIn, Badoo, Vkontakte i druge.

Svim društvenim mrežama je zajedničko da korisnik prijavom na neku od njih stvara svoj profil koji sadrži određene informacije o korisniku. Podaci o korisniku se ne pohranjuju na korisnikovom računalu nego na udaljenim poslužiteljima, što predstavlja određeni sigurnosni rizik jer korisnik tim podacima ne pristupa izravno pa ih ne može niti izravno obrisati. Nakon prijave, korisnik može pregledavati profile ostalih korisnika te mreže. Kao što korisnik može pregledavati tuđe profile, tako i njegov profil može biti pregledan. Za korisnikov profil nisu zainteresirani samo prijatelji, rodbina i ostali poznanici već njegov profil mogu pregledavati osobe koje skupljaju informacije o korisnicima kako bi pronašli način da ih prevare (npr. ukradu identitet), ili su to korporacije koje skupljaju podatke o navikama korisnika u svrhu poboljšanja marketinške kampanje. Clark upozorava da tvrtke vlasnice društvenih mreža također skupljaju podatke kako bi poboljšali uslugu koju pružaju, ali nerijetko i prodaju te informacije oglašivačima. Upotreba društvenih mreža je besplatna, tako da je oglašavanje glavni izvor zarade za vlasnike socijalnih mreža i zbog toga se često prodaju podaci o navikama korisnika kako bi se ostvario dodatni profit. Oglašivačima su ove informacije korisne jer mogu bolje usmjeriti marketinšku kampanju i time ostvariti bolju prodaju. U ovakvom načinu oglašavanja nema nikakvih ograničenja u informacijama koje se sakupljaju. Korisnici ne znaju koje informacije o njima koriste oglašivači, često se sakupljaju informacije i o maloljetnim osobama, a informacije nisu na poseban način zaštićene zbog čega zlonamjerni korisnici mogu doći do njih. Clarkova je teza da društvene mreže prate, nadziru i povezuju individualce s drugim osobama, potkopavajući nastojanja korisnika u zadržavanju privatnosti. Ova vrsta nadziranja se razlikuje od one koju provodi vlada jer se čini kako je sporazumna. Korisnici se ne promatraju tajno niti su njihovi podaci prikupljeni bez njihovog

znanja, već su sami korisnici dobrovoljno dali podatke. Umjesto panoptikona koji se nameće bez pristanka, korisnici društvenih mreža su dio dobrovoljne vrste panoptikona. Dobrovoljni panoptikon rezultira predajom osobnih podataka u korist korisniku, bilo zbog besplatnih usluga ili povećanja društvenog statusa. Kao dio neoliberalizma koji pretvara građane u potrošače, društvene mreže igraju važnu ulogu u pretvaranju svih dijelova života vidljivim i pristupačnim za marketinške sile.[23]

Na društvenim mrežama korisnik u svojem profilu objavljuje podatke o sebi kako bi bili vidljivi ostalim korisnicima. Podaci koje korisnik objavljuje mogu biti ime i prezime, dob i spol, datum rođenja, mjesto stanovanja, broj mobitela, svoje fotografije, informacije o obrazovanju, zaposlenju, adresu na kojoj se korisnik nalazi i drugo. Korisnik može ograničiti tko može vidjeti ove podatke. Najnesigurnije je ako pristup svojim informacijama dopusti svima (informacije postaju javne). Često je ovo podrazumijevani način prikaza korisnikovog profila koji ostaje takav dok ga korisnik ne promijeni. Zbog toga je preporučljivo odmah nakon otvaranja profila promijeniti postavke privatnosti na neku od viših razina sigurnosti kako bi korisnikove informacije mogli vidjeti samo njegovi prijatelji ili nitko osim korisnika. Međutim, mijenjanje postavki privatnosti tako da informacije postanu privatne ne jamči čuvanje privatnosti i toga većina korisnika nije svjesna. Razlozi tome mogu biti sigurnosni propusti unutar samog servisa, postojanje malware programa na korisnikovom računalu, nesavjesno ponašanje nekoga kome je dozvoljen pristup informacijama i slično. Jedan od načina osiguravanja privatnosti je objavljivanje samo nužnih podataka, dok se svi ostali skrivaju ili uopće ne navode. Korisnici, često nesvjesno, objavljuju statuse iz kojih se mogu saznati osjetljive informacije (npr. trenutna lokacija, tvrtka u kojoj su se zaposlili, planove putovanja itd.). Osim statusa, korisnici mogu objavljivati slike i video materijale na kojima se nalaze oni ili njihovi prijatelji. Prilikom objavljivanja slika i videa potrebno je pripaziti tko ih može vidjeti jer su česti slučajevi u kojima su fotografije vidjele osobe kojima one nisu bile namijenjene. Informacije o korisniku se mogu dobiti iz grupa u kojima se korisnik nalazi i profila koje prati. Mogu se saznati korisnikovi interesi, hobiji, koji mobilni uređaj koristi ili planira kupiti i još mnogo toga. Sakupljanjem i analizom ovih naizgled nevažnih informacija može se saznati jako puno o korisniku i njegovim navikama.

[23] Usp. Clark, IJ. Nav. dj. Str. 6.

Korisnik može utjecati na količinu informacija koje svjesno objavljuje o sebi. Ali na društvenim mrežama se do njegovih podataka može doći i na druge načine. Korisnikovi prijatelji mogu dalje širiti korisnikove informacije bez njegovog znanja i dopuštenja. Poznati su slučajevi kada je korisnika na slici neprimjerenog sadržaja označio neki njegov prijatelj. Zbog toga što je slika bila vidljiva svima, nju su mogle vidjeti i osobe za koje korisnik nije htio da ju vide (poput šefova na poslu). Društvena mreža zadržava pravo promjene postavki privatnosti u bilo koje vrijeme čime privatne informacije mogu postati javne. Zbog toga je poželjno često provjeravati postavke privatnosti kako bi se provjerilo tko može vidjeti pojedine informacije. Dodavanjem programa nepoznatih autora omogućen je pristup korisnikovim privatnim informacijama bez njegova znanja (npr. igre koje korisnik igra na mrežama). Dodavanjem programa, korisnik dopušta uvid samo u neke informacije, ali ne zna što točno program može vidjeti, tj. koje informacije o korisniku program može proslijediti nekim zainteresiranim skupinama. Neki programi ne poštuju sigurnosne politike društvene mreže te čitaju i bilježe informacije koje nisu potrebne za njihov rad. Te informacije se kasnije mogu koristiti za razne napade. Društvene mreže, u svojim politikama privatnosti, naglašavaju kako nisu odgovorne za takve programe niti za curenje informacija njihovom upotrebom.[24]

Kolačići za praćenje se povezuju s korisnikovim profilom na društvenoj mreži te na taj način mogu se saznati korisnikove privatne informacije i njegove internetske navike. Kako bi se korištenje kolačića onemogućilo, poželjno je obrisati sve kolačiće nakon upotrebe društvenih mreža. Kao još jedan problem se navodi činjenica da korisnikov profil se ne briše u potpunosti kada korisnik odluči napustiti mrežu, nego se često postavlja u stanje hibernacije, a to znači da profil neće moći pregledavati drugi korisnici, ali se sve informacije u njemu čuvaju. Ako korisnik ponovo poželi koristiti tu društvenu mrežu, moći će ponovo aktivirati svoj stari profil. Nažalost, do tada se podaci o korisniku čuvaju na udaljenim poslužiteljima i korisnik ne može biti siguran na koji način se oni koriste.[25]

[24] Usp. Privatnost na internetu. URL: http://security.lss.hr/images/dokumenti/lss-pubdoc-2010-10-002.pdf (2016-04-08). Str. 11-14.
[25] Usp. Isto. Str. 14.

3.1.4. Phishing

Phishing[26] (mrežna krađa identiteta) je jedan od oblika prijevare koji podrazumijeva skup aktivnosti kojima neovlašteni korisnici korištenjem lažnih poruka elektroničke pošte i lažnih web stranica, koje su većinom financijske organizacije, pokušavaju korisnika navesti na otkrivanje povjerljivih osobnih podataka kao što su OIB, JMBG, korisnička imena i zaporke, PIN-brojevi, brojevi kreditnih kartica i slično. Velik broj korisnika nije upoznat s ovim tipom prijevare, a kada dođu do ovih informacija, zlonamjerni korisnici se ili sami njima koriste ili ih prodaju kako bi došli do podataka o drugim osobama. Elektroničke poruke se obično oslanjaju na lažne web stranice koje izgledom sasvim odgovaraju web stranicama legitimnih tvrtki.

Najčešći primjeri phishinga su:

- Lažna upozorenja banaka ili drugih financijskih organizacija u kojima se od korisnika traži upisivanje osobnih podataka kako u suprotnom ne bi došlo do ukidanja računa.
- Prijevare s aukcijskim web stranicama kao što je eBay, u kojima se korisnika nagovora na uplatu određene novčane svote kako bi se kupio neki proizvod, čime korisnik zapravo, misleći da kupuje proizvod, vrši uplatu na lažni račun.
- Lažne poruke od administratora u kojima se traže korisnički podaci kao što su lozinke.
- Poruke u kojima se korisnika pokušava namamiti da uplati određenu svotu novaca na lažni račun.
- Poruke koje se pozivaju na sigurnost i zahtijevaju od korisnika otkrivanje osobnih informacija (korisnički račun, lozinku itd.) ili zahtijevaju instalaciju programa za kojeg se tvrdi da će pomoći pri sigurnosnom propustu.
- Poruke koje korisnika obavještavaju da je dobio dobitak na lutriji i da trebaju njegove osobne podatke kako bi mogao podići dobitak.[27]

Kada prevaranti dođu do osobnih informacija korisnika, oni će ih koristiti na različite načine, a većina će iz ovih informacija pokušati izvući financijsku korist. Ako se prevarant domogne informacija o brojevima kreditnih kartica ili bankovnih računa, može to sam iskoristiti ili prodati informacije drugima. Također se i manje osjetljive informacije (poput e-mailova, imena, JMBG broja) mogu iskoristiti i prodati zainteresiranim stranama, a opasno je kada

[26] Usp. Gledec, Gordan; Mikuc, Miljenko; Kos, Mladen. Nav. dj. Str. 37.
[27] Usp. Isto. Str. 37-38.

prevaranti dođu do informacija o korisničkim računima i lozinkama korisnika, jer se tada u ime prevarenih korisnika mogu činiti razne kriminalne aktivnosti na internetu.

Moguće preventivne mjere protiv phishinga su:

- Nikad ne odgovarati na elektroničke poruke koje traže osobne podatke - financijske institucije imaju podatke, a i mala je vjerojatnost da bi bilo koja renomirana tvrtka zatražila osobne podatke putem maila.
- Nikad ne slijediti sumnjive linkove - najčešće se takvi linkovi nalaze unutar sumnjivih e-mail poruka te nikada slijediti linkove ako primatelj nije siguran u identitet pošiljatelja - za ovu svrhu dobro je koristiti digitalne potpise.
- Koristiti antivirusni softver - ova vrsta programa prepoznaje maliciozni softver koji se također može koristiti za prikupljanje osobnih informacija.
- Koristiti osobni vatrozid (eng. firewall) kako bi se moglo pratiti promet prema internetu i uočiti moguće sumnjive aktivnosti te također koristiti antispyware softver.
- Koristiti dobre lozinke i često ih mijenjati - dobre lozinke sastoje se od kombinacije velikih i malih slova, brojeva i simbola što ih čini vrlo teškim za probijanje.
- Provjeriti koristi li web stranica protokol HTTPS – web adresa financijskih institucija trebala bi počinjati s https:// umjesto s http://, a dvostrukim klikom na ikonu lokota moguće je provjeriti digitalni certifikat.[28]

3.1.5. Spyware i Adware

Spyware je računalni program iz kategorije malwarea koji skuplja osobne informacije korisnika bez svjesnog pristanka, u situaciji kad korisnik nije upoznat s činjenicama i implikacijama koje akcije spywarea mogu izazvati. Osobni podaci korisnika se tajno prikupljaju koristeći razne metode, kao što su nadzor pritisnutih tipki na tastaturi, pohranjivanje web adresa koje korisnik posjećuje ili analiza dokumenata na tvrdom disku korisnika. Ciljevi napada mogu biti kriminalni poput krađe lozinki i financijskih podataka, npr. brojeva kreditnih kartica ili se mogu bilježiti pretraživani pojmovi na internetu za potrebe oglašavanja. Tako prikupljeni podaci često se i preprodaju, a sve veće širenje spywarea dovelo je do razvoja antispyware-softvera. Takvi programi uklanjaju ili onemogućuju rad spywarea na napadnutom računalu i onemogućuju njegovu instalaciju. No, dio računalnih

[28] Usp. Isto. Str. 39.

tvrtki namjerno u svoje programske proizvode ugrađuje spyware, kako bi prikupili podatke o ponašanju korisnika za marketinške potrebe. Korisnici najčešće nisu ni svjesni da su takvi programi instalirani i pokrenuti na njihovom računalu i da im narušavaju privatnost. Dodatni problem spywarea je da, uz narušavanje privatnosti, koristi resurse računala (memoriju, procesor, disk) bez znanja i dopuštenja korisnika.[29]

Adware (eng. advertising-supported software) je programski paket koji nakon instalacije i pokretanja korisniku automatski (bez njegove intervencije i eksplicitnog zahtjeva) prikazuje ili dohvaća s mreže reklamne materijale. Adware je modularno integriran u legitimne programske pakete ili je kao nezavisna aplikacija njihov sastavni dio. Obično se koristi kao način povrata financijskih sredstava uloženih u razvoj glavnog programskog proizvoda ili za snižavanje ili eliminaciju troškova korištenja programskog paketa u kojeg je integriran. Adware često poprima karakteristike spywarea, tako da za njih korisnici često koriste nazive spyware ili čak malware.[30]

[29] Usp. Isto. Str. 40.
[30] Usp. Isto. Str. 41.

4. Masovno nadziranje

Masovno nadziranje pojedinaca ili građana nije novi koncept, postoji duži niz godina te je bio u centru popularnih medija. Jedan od primjera je i knjiga Georgea Orwella *Tisuću devetsto osamdeset četvrta* u kojoj se radnja odvija u distopijskom svijetu gdje se pomoću tehnologije nadzire stanovništvo. Knjiga je izvor inspiracija koje se koriste u modernom dobu, poput Velikog Brata, koji nadzire sve i gleda 24 sata dnevno što stanovništvo radi i čiji je slogan Veliki Brat te gleda. Osim što je bila inspiracija za emisiju Big Brother u kojoj su osobe pod cjelodnevnim nadzorom kamera, povlači se paralela i s današnjim svijetom, gdje je na svakom koraku kamera, bilo na ulici, banci, supermarketu, pošti, knjižnici, školama, vladinim institucijama, javnom prijevozu i raznim drugim mjestima, kamere snimaju i spremaju lica osoba koje su zabilježile kako bi kasnije služile za identifikaciju u slučaju zločina, terorističkog napada ili drugog. Prema priopćenju britanskog udruženja industrije zaštite (BSIA)[31] iz 2013., samo u Velikoj Britaniji na javnim i drugim površinama, nalazi se između 4 i 6 milijuna kamera odnosno video nadzor (eng. CCTV), dok je procjena na globalnoj razini preko 246 milijuna kamera, od čega je preko 30 milijuna u Sjedinjenim Američkim Državama.[32] Broj kamera i video nadzora se naglo povećao nakon napada 11. rujna u New Yorku i Washingtonu, te kasnijih napada u Londonu i Madridu, a pristup video nadzoru imaju razne tajne agencije država. Danas je taj broj još i veći, gdje se svakodnevno dodaju kamere na javne površine, što je slučaj i u Hrvatskoj, gdje hrvatska Sigurnosno-obavještajna služba (SOA) ima pristup kamerama i video nadzoru diljem Hrvatske, a broj iznosi preko 300 kamera koje se nalaze u gradovima[33], dok drugi navode da samo u Zagrebu ima preko 4000 nadzornih kamera, a video nadzor se nalazi i po autocestama.[34]

Video nadzor se također koristi i u knjižnicama, koji su uvele mnoge knjižnice diljem svijeta, od SAD-a do Velike Britanije. Video nadzor u knjižnicama može biti prijetnja privatnosti knjižničnih korisnika i djelatnika, a što se krši s knjižničnim nastojanjima očuvanja

[31] Usp. Reeve, Tom. BSIA attempts to clarify question of how many CCTV cameras are there in the UK, 2013. URL: http://www.securitynewsdesk.com/bsia-attempts-to-clarify-question-of-how-many-cctv-cameras-in-the-uk/ (2016-04-03)
[32] Usp. Ingram, Philip. How many CCTV camers are there globally? URL: http://www.securitynewsdesk.com/how-many-cctv-cameras-are-there-globally/ (2016-04-03)
[33] Usp. Velika promjena: SOA dobiva pristup gradskim nadzornim kamerama. URL: http://www.telegram.hr/politika-kriminal/velika-promjena-soa-dobiva-pristup-gradskim-nadzornim-kamerama/ (2014-04-03)
[34] Usp. Zagreb pokriven s četiri tisuće nadzornih kamera. URL: http://www.poslovni.hr/hrvatska/zagreb-pokriven-s-cetiri-tisuce-nadzornih-kamera-299781 (2016-04-03)

privatnosti i intelektualne slobode. Video nadzor u knjižnicama se, kao i u drugim ustanovama, može zloupotrijebiti i koristiti za diskriminaciju i kršenje privatnosti korisnika, a odluke o digitalnim sustavima nadziranja u knjižnicama bi se trebale bazirati na razlozima koji su dokazani.[35] Knjižnice se smatraju mjestima u kojima se štite intelektualna sloboda, sloboda govora i privatnost, stoga uvođenje video nadzora u knjižnice može biti u sukobu s tim ciljevima. Pravne osnove za video nadzor na javnim mjestima, uključujući knjižnice, se temelji na pretpostavki da pojedinci ne očekuju privatnost na javnim mjestima te da ovi sustavi predstavljaju opravdano korištenje moći kako bi se zaštitilo javno dobro. Protivnici ovog sustava navode kako bi građani trebali imati pravo anonimnosti na javnim mjestima i tako zabraniti vladi video nadzor i praćenje bez opravdanog razloga.[36] Američko knjižničarsko društvo (eng. American Library Association – ALA) za video nadzor u knjižnicama navodi kako je oprema za nadziranje u mogućnosti snimiti korisnikove čitateljske navike na način koji otkriva o korisniku na isti način kao i zapisi o posuđenim knjigama koje knjižnice čuvaju od očiju javnosti, no ako knjižnica odluči da je video nadzor zaista potreban, važno je da knjižnica razvije i provede smjernice koje štite korisničku privatnost i povjerljivost.[37] Zbog činjenice da su osobne informacije osjetljive i podložne zlouporabi, prikupljanje nadzornih podataka može imati ozbiljne posljedice za knjižnično poslovanje.[38] Osim korisnika, ugrožena je privatnosti i djelatnika knjižnice, čija privatnost nije osigurana te čije radnje zabilježene na video snimkama mogu biti iskorištene kao dokazni materijal ako policija ili obavještajne agencije uzmu te snimke. [39]

Kao još jedan primjer pojma masovnog nadziranja u popularnoj kulturi je američka serija *Person of Interest* čija radnja se zasniva na video nadzoru i masovnom nadziranju stanovništva, gdje je u centru Stroj (eng. The Machine), umjetna inteligencija koja putem video nadzora i drugih tehnologija, poput Velikog Brata, nadzire građane i predviđa zločine koji će se dogoditi. Kao i u stvarnosti, kada se povećao broj nadzornih kamera nakon 11.

[35] Usp. Newell, Bryce Clayton; Randall, David P. Video surveillance in public libraries: a case of unintended consequences? // IEEE, 2012. URL: http://www.computer.org/csdl/proceedings/hicss/2013/4892/00/4892b932.pdf (2016-01-16). Str. 1932.
[36] Usp. Isto. Str. 1934.
[37] Usp. Isto.

[38] Usp. Randall, David P.; Newell, Bryce Clayton. The panoptic librarian: the role of video surveillance in the modern public library. URL: https://www.ideals.illinois.edu/bitstream/handle/2142/47307/132_ready.pdf?sequence=2 (2016-01-13). Str. 509.

[39] Usp. Newell, Bryce Clayton; Randall, David P. Nav. dj. Str. 1935.

rujna, tako je i u seriji umjetna inteligencija nastala nakon napada i nakon nekog vremena prodana američkoj vladi koja ju je koristila za nadziranje građana i sprječavanje terorističkih napada, dok su drugi protagonisti uz pomoć Stroja sprječavali razne zločine i spašavali nevine. Kao jedna od tema u seriji su i vladine agencije, poput Nacionalne sigurnosne agencije (eng. National Security Agency - NSA), koje špijuniraju građane i njihove telefonske pozive, internetsku aktivnost te narušavaju njihovu privatnost.

4.1. NSA nadziranje

Upravo se američka NSA našla pod pritiskom nakon što je u lipnju 2013. godine Edward Snowden izašao u javnost i objavio dokumente u kojima se otkriva kako je NSA od 2001. godine špijunirala građane, ne samo SAD-a, već i građane diljem svijeta.

U kasnoj 2012. i ranoj 2013. godini, Edward Snowden, koji je tada radio za NSA preko agencije Booz Allen Hamilton, kontaktirao je dvoje novinara, Lauru Poitras i Glenna Greenwalda, s informacijama o programima masovnog nadziranja koje je provodila američka vlada. NSA je prikupljala velike količine podataka koji su se odnosili na korištenje interneta i prikupljanje metapodatka.[40] Snowden, Poitras, Greenwald i novinar Ewen MacAskill iz The Guardiana našli su se 1. lipnja 2013. godine u hotelu u Hong Kongu, gdje su vodili intervju sa Snowdenom i razgovarali o dokumentima koje je prikupio u NSA.[41] Prvi dokument koji je Edward Snowden otkrio 5. lipnja 2013. kojeg je objavio britanski The Guardian se bavio činjenicom da je NSA, pomoću naloga suda za protuobavještajni nadzor (eng. Foreign Intelligence Surveillance Court - FISC), zahtjevala od teleoperatera Verizona metapodatke koji su uključivali telefonske pozive i internetske zapise. Verizonu je bilo zabranjeno otkrivati javnosti o zahtjevu za korisničke podatke. Idući dan, članci u Washington Postu i The Guardianu su opisali kako je program PRISM dao NSA direktan pristup serverima nekih od najvećih tehnoloških kompanija, koje uključuju Apple, Facebook, Google, Microsoft, Skype, Yahoo i YouTube. Enkripcija i kontrole privatnosti su zaobiđene uz pomoć navedenih kompanija.[42] PRISM je usmjeren na internetsku komunikaciju i podatke osoba koje nisu

[40] Usp. Clark, IJ. Nav. dj. Str. 1.
[41] The Guardian. Edward Snowden and the NSA files – timeline. URL: http://www.immagic.com/eLibrary/ARCHIVES/GENERAL/GMGP_UK/G130623S.pdf (2016-05-03)
[42] Usp. Lyon, David. Surveillance, Snowden, and big data: capacities, consequences, critique. // Big Data & Society, 2014. Str. 2.

američki državljani i koji žive izvan SAD-a i osoba koje su u kontaktu s njima. Uslijedilo je objavljivanje novih dokumenta, koji su govorili o programima poput XKeyscore i Tempora. Objavljeni su detalji o tome kako je američka vlada špijunirala računala u Kini kao i detalji o NSA i britanskoj agenciji GCHQ koji su prisluškivali komunikacije političkih vođa tijekom sumita G20 2009. u Londonu te da je NSA prikupljala metapodatke o internetskim komunikacijama.[43] U Velikoj Britaniji je na snazi bio program Tempora, koji je dao pristup britanskoj agenciji GCHQ, koja je radila u suradnji s NSA, a Upstream se odnosi na spajanje na kabele i mreže koji onda presreće sav internetski promet. Baza podataka koja omogućava prikupljanje informacija u stvarnom vremenu se zove XKeyscore. Podaci o nadziranju koje je iznio Snowden pokazuju kako vlade, posebno američka, britanska, kanadska te moguće i druge, provode nevjerojatnu razinu nadziranja stanovništva te na koji način to rade. NSA zapošljava izvođače radova koji prikupljaju korisničke podatke od drugih korporacija, posebno telefonske, internetske i web kompanije. Ova vrsta nadziranja znači da NSA i ostale agencije koriste informacije poput kolačića i log-in podataka. Koriste podatke koji su proizašli iz korištenja uređaja kao što su mobiteli ili društvene mreže koje mogu geolocirati korisnike. Ono što korisnici napišu na medijima poput Facebooka ili Twittera ili korištenjem svojih telefona, može se smatrati iskoristivim podacima za svrhe nacionalne sigurnosti. Metapodaci koji su povezani s korisnicima se prikupljaju bez njihovog znanja samo zato što koriste te uređaje. Metapodaci, koji se opisuju kao podaci o podacima, se odnose na IP adrese, identitet osobe, lokaciju poziva ili poruke te vrijeme kontakta. Nakon što je Snowden izašao u javnost s dokumentima, vlade i agencije su odbacivale i smanjivale važnost metapodataka, no Bruce Schneier navodi kako su metapodaci sami po sebi dovoljni za nadziranje. [44]

Nadziranje se proširilo toliko da, iako nije sveprisutno, prisutnost nadziranja postao je normalan i opće prihvaćen dio modernog života. Iako se neki dijelovi nadziranja mogu opravdati, kao na primjer kada su nadzirane osobe povezane s terorizmom, implementacije masovnog nadziranja izazivaju ozbiljnu zabrinutost. Michel Foucault je interpretirao panoptikon Jeremyja Benthama, a ta interpretacija se često koristi kao polazna točka shvaćanja utjecaja nadziranja na individualca.[45] Bentham je predložio dizajn zatvora sa središnjim tornjem koji bi omogućio nadzornicima pogled prema svim ćelijama u bilo koje

[43] Usp. Landau, Susan. Making sense from Snowden: what's significant in the NSA surveillance revelations. // IEEE, 2013. URL: http://www.cs.siue.edu/~wwhite/IS376/ReadingAssignments/0930_MakingSenseFromSnowden.pdf (2016-05-04) Str. 54.
[44] Usp. Lyon, David. Nav. dj. Str. 2-3.
[45] Usp. Clark, IJ. Nav. dj. Str. 3.

vrijeme bez da ih zatvorenici mogu vidjeti, a taj dizajn se zadržao do danas. Foucault je iskoristio Benthamovu ideju kao primjer automatske funkcije moći, navodeći kako je nadziranje najučinkovitije kada je trajno u svojim učincima, čak ako i nije stalno u svojim akcijama. Za Foucaulta, učinkovita moć mora biti vidljiva i neprovjerljiva, a oni koji se nadziru moraju vidjeti ili biti svjesni mehanizama koji se koriste kako bi ih se nadziralo, no u isto vrijeme ne biti u mogućnosti odrediti jesu li nadzirani u bilo kojem trenutku. Nadziranje je najučinkovitije kada ne zahtjeva korištenje moći, individualci se kontroliraju tako što su svjesni da ih se može promatrati. Upravlja i kontrolira individualcima te tako potkopava autonomiju na bazi postojanja, više nego pretvaranja.[46]

Masovno nadziranje rezultira ograničenom intelektualnom privatnosti, spriječavanjem mogućnosti traženja novih ideja koji se krše s dosadašnjim stanjem i na taj način spriječava autonomiju. Sloboda traženja novih ideja, kritika i neslaganje s dosadašnjim stanjem je jedna od glavnih elemenata demokratskog procesa.[47] Iako se na nadziranje gleda kao mehanizam države, razvilo se i korporativno nadziranje. Ove dvije forme nadziranja se mogu doimati posebne, no obe komuniciraju s informacijama koje se nalaze među njima, u formi „tekućeg nadziranja“.[48] Tekuće nadziranje se pojavilo kao posljedica svođenja običnih građana na potrošače i pretvaranja građana u sumnjivce, omogućujući osobnim podacima da teku kao da su tekućina. Korporativno nadziranje se više ne može smatrati odvojenim, a suradnja između vlade i kompanija u prikupljanju informacija onih koji prijete dosadašnjem stanju nije nova pojava, posebno u Velikoj Britaniji. Podaci koje su korporacije prikupile nisu samo prodani oglašivačima za zaradu, ostajući samo u korporativnoj domeni, već, kako su Snowdenovi dokumenti otkrili, tim podacima može pristupiti i vlada. Privatne kompanije zarađuju od osobnih podataka, prikupljaju ih i prodaju, a zauzvrat nude „besplatne“ usluge. Brza komercijalizacija interneta od 1995. do danas bila je važna u potvrđivanju pojma da je informacija roba, a osobni podaci su postali roba za velike korporacije koje zarađuju od njih.[49]

Agencije poput NSA i GCHQ su namjerno dizajnirali programe za nadziranje kako bi iskoristili takozvane 'backdoors' na medijima za privatnu komunikaciju, poput Googlea i Facebooka. Uz to, kao i tehnologije koje prepoznaju lica i glas, analize jezika, izvedbene alate baza podataka, pretraživanje videa te alate koji analiziraju ponašanje u stvarnome svijetu,

[46] Usp. Isto.
[47] Usp. Isto. Str. 5.
[48] Usp. Isto.
[49] Usp. Isto.

preko takvih medija, aktivnosti postaju podaci koje NSA prikuplja kao profil ljudske interakcije preko stalnog nadziranja.[50] Hogan i Shepherd pišu o NSA i ukazuju na ogromni kompleks u državi Utah, tzv. Data Center, koji služi za prikupljanje i čuvanje podataka koje agencija prikupi tijekom nadziranja, ne samo u SAD-u, već i diljem svijeta. Svrha kompleksa je presretanje, dešifriranje, analiziranje i čuvanje ogromnih podataka izvučenih iz komunikacija koje se odvijaju u svijetu. Pretpostavka je da kompleks može čuvati i do 12 exabajta (exabajt je trilijun terabajta) informacija. Neke od tih informacija su podaci o telefonskim razgovorima, podaci prikupljeni preko web platformi poput Facebooka i Googlea, a NSA prikuplja i sadržaj i metapodatke, vremenske i lokacijske informacije korisnika, onih koji šalju sadržaj kao i onih koji primaju. Programi poput XKeyscorea su dizajnirani kako bi prikupili informacije u stvarnom vremenu, bez odgode, a koji iskorištavaju ne samo „stražnja vrata" tj. „backdoors" već i rupe u zakonu. Iako je kompleks ogroman, prema Mooreovom zakonu, koji navodi kako se računalni podaci dvostruko povećaju svakih dvanaest do osamnaest mjeseci, ovaj prostor za nekoliko godina neće biti dovoljan. Sam XKeyscore, kako navodi Greenwald, prikuplja preko dvadeset terabajta dnevno, što ne ostavlja mnogo prostora za daljnje čuvanje.[51]

SAD nije jedina država koja koristi nadziranje za kontroliranje i praćenje svakog koraka svojih građana. Britanska vlada je jedna od vodećih predlagača nadziranja, u tolikoj mjeri da se Velika Britanija smatra jednom od najnadziranijih demokratskih država. 2008. godine britanska vlada je pokrenula program masovnog digitalnog nadziranja (kodno ime KARMA POLICE) bez javne rasprave ili propitivanja.[52] Cilj programa je bio zabilježiti navike pretraživanja svakog vidljivog korisnika na internetu. Podaci koji su prikupljeni uključivali su pristup web stranicama s vijestima, društvenim mrežama, web tražilicama, chat forumima, time kršeći intelektualnu privatnost onih koji se nisu mogli zaštititi. The Guardian je nakon Snowdenovih otkrića objavio podatke o GCHQ programu Tempora. Zbog postavljenih presretača podataka na kablove s podacima između Europe i Amerike, program Tempora je omogućio agenciji analizu komunikacija, koje su uključivale sadržaje elektoničke pošte, Facebook objava i telefonskih poziva.[53] Takve aktivnosti izazivaju ozbiljnu zabrinutost za knjižnice i knjižničare koji se brinu za intelektualnu slobodu i privatnost, posebno o tome

[50] Usp. Hogan, Mel; Shepherd, Tamara. Information ownership and materiality in the age of big data surveillance. // Journal of Information Policy, 5(2015). Str. 8.
[51] Usp. Isto. Str. 9-11.
[52] Usp. Clark, IJ. Nav. dj. Str. 9.
[53] Usp. Isto.

kako knjižničari mogu zaštititi privatnost korisnika i osigurati njihovu autonomiju u pristupu internetu, posebno u Velikoj Britaniji. Prije nego je Snowden izašao u javnosti, britanska vlada je pokušala usvojiti Zakon o nacrtu komunikacijskih podataka (eng. Draft Communications Data Bill) kako bi nadzirali online komunikacije. O tome kako se zakon „razvijao“ pisao je Clark, a zakon je trebao prisiliti tehnološke tvrtke i teleoperatere na prikupljanje i čuvanje metapodataka godinu dana i učiniti ih dostupnima vlasti bez naloga. Zakon je kasnije preimenovan u Zakon o istražnim moćima (eng. Investigatory Powers Bill), a on navodi da pružatelji internetskih usluga čuvaju podatke, kako bi im vlada kasnije mogla pristupiti. Zakon je imao posljedice za knjižnične usluge, u narodnim i sveučilišnim knjižnicama, jer zahtjeva od knjižnica čuvanje podataka o korištenju interneta koje bi vlada mogla uzeti bez naloga, čime se krši autonomnost korisnika. Suradnja između NSA i GCHQ nije nova, ECHELON sustav je omogućio Five Eyes (suradnju između obavještajnih agencija iz SAD-a, Velike Britanije, Kanade, Australije i Novog Zelanda) presijecanje svih satelitskih komunikacija, dopuštajući pristup kabelskim i radio komunikacijama diljem svijeta.[54]

4.2. Programi za nadziranje komunikacije na internetu

4.2.1. PRISM

PRISM je kratica od Planning Tool for Resource Integration, Synchronization, and Management, programa za nadziranje obavještajne agencije NSA, a svrha programa je prikupljanje i analiziranje podataka koje iz drugih zemalja prolaze preko američkih servera.[55] PRISM dozvoljava NSA prikupljanje, pregledavanje i analiziranje različitih vrsta podataka koje se nalaze u internetskim kompanijama smještenima u SAD-u. Iako NSA ne bi smjela pristupati podacima američkih građana, ne mogu biti sigurni koji su podaci od stranih državljana, a koji od američkih. Kompanije koje su bile uključene u PRISM program su Google, Yahoo, Microsoft, AOL, Facebook, Apple, YouTube, Skype i PalTalk. Korisnički podaci koje je NSA prikupljala iz navedenih kompanija su e-mailovi, razgovori, video

[54] Usp. Isto. Str. 10.
[55] Usp. Dreyfuss, Benjamin; Dreyfuss, Emily. What is the NSA's PRISM program? (FAQ), 2013. URL: http://www.cnet.com/news/what-is-the-nsas-prism-program-faq/ (2016-05-23)

materijali, slike, spremljeni podaci, VoIP, korisničke aktivnosti, log-in podaci, podaci s društvenih medija i drugo.[56]

Nakon što se prikupe podaci i informacije, dalje se analiziraju preko posebnih sustava koji se bave glasovnim informacijama, tekstom i videom, a koji uključuju lokacije i uređaje koje koriste nadzirane osobe. Sustavi koji se bave time su Printaura, Scissors, Protocol Exploitation, Nucleon (glas), Pinwale (video), Mainway (telefonski zapisi) i Marina (internetski zapisi). NSA je mogla i u stvarnom vremenu nadzirati kada netko pošalje ili primi e-mail ili kada pretražuje nešto na internetu. Prva kompanija koja je bila dio PRISM programa je bio Microsoft, nakon čega su uslijedili Yahoo, Google i Facebook, a Apple je bila posljednja kompanija koja se pridružila PRISM.[57]

4.2.2. XKeyscore

Tajni NSA program pod nazivom XKeyscore[58] omogućava analistima da pretražuju kroz ogromne baze podataka koje sadrže e-mailove, online chatove i povijesti pretraživanja milijuna pojedinaca. Na prezentaciji koju je u javnost pustio Snowden, XKeyscore obuhvaća područje Srednje Amerike, Afrike, Bliskog Istoka i Azije, Australije te posebno Europu, posebice Istočnu Europu, na otprilike 150 mjesta sveukupno i preko 700 servera. XKeyscore je program koji pokriva skoro sve što tipičan korisnik radi na internetu, što uključuje sadržaje e-maila, posjećenih stranica i pretraživanja, kao i metapodatke. Plug-inovi izvlače i indeksiraju metapodatke u tablice, koji uključuju e-mail adrese, HTTP parser, broj telefona, internetsku aktivnost i drugo. Analisti mogu koristiti program kako bi u stvarnom vremenu presreli internetske aktivnosti pojedinca. Svrha XKeyescorea je pretraživanje metapodataka i sadržaja e-maila, kao i pretraživanje prema imenu, broju telefona, IP adresi, ključnim riječima, jeziku po kojem se pretraživalo ili vrsti web pretraživača koji se koristio. XKeyscore omogućava i analiziranje aktivnosti unutar društvenih mreža, gdje NSA analist može čitati sadržaje Facebook chata i privatnih poruka.[59]

---

[56] Usp. NSA slides explain the PRISM data-collection program, 2013. URL: http://cyber-peace.org/wp-content/uploads/2013/06/NSA-slides-explain-the-PRISM-data-collection-program-The-Washington-Post.pdf (2016-05-23)

[57] Usp. Isto.

[58] Usp. Greenwald, Glenn. XKeyscore: NSA tool collects nearly everything a user does on the internet, 2013. URL: http://www.tietotori.fi/Keskustelualueet/Muu%20maailma/Yhdysvallat/I00470F08.0/Sinisilm%C3%A4isille%20mietitt%C3%A4v%C3%A4%C3%A4.pdf (2016-05-23)

[59] Usp. Isto.

4.2.3. Tempora

Tempora je program britanske agencije GCHQ-a, koji radi na sličnoj bazi kao XKeyscore te je ujedno i najveći svjetski XKeyscore program koji je u suradnji s ostalim NSA programima za nadziranje. Tempora je prikupljala podatke s Bliskog Istoka, Sjeverne Afrike i iz Europe, a korišteno je preko 1000 strojeva koji su analizirali i procesirali preko 40 milijardi podataka na dan. Podaci su se spremali u repozitorij koji je čuvao podatke, 3 dana za običan sadržaj, a 30 dana za metapodatke.[60]

Tempora je presretala podatke koji su prolazili kroz optičke kablove kako bi GCHQ imao pristup ogromnim količinama podataka korisnika interneta. Presretači su bili postavljeni u Velikoj Britaniji i u drugim zemljama, a kompanije koje su omogućile postavljanje presretača su bile svjesne što mogu napraviti. Tempora je prikupljala podatke kao što su telefonski pozivi, sadržaje e-mail poruka, Facebook podatke i povijesti pretraživanja interneta. GCHQ je prikupljene podatke dijelio s NSA.[61]

[60] Usp. Tempora: the world's largest XKeyscore is now available to qualified NSA users, 2012. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHc5f6.dir/doc.pdf (2016-05-23)
[61] Usp. Isto.

5. Knjižnice i borba za privatnost korisnika

5.1. Knjižnice protiv masovnog nadziranja

Nakon što je Edward Snowden izašao s dokumentima koji razotkrivaju špijuniranje i nadziranje koje je NSA provodila diljem svijeta, pojedinci su postali svjesniji problema s privatnosti. Međutim, svijest o ovom problemu, davno prije Edwarda Snowdena i ostalih, bili su - knjižničari.

Jedna od glavnih uloga knjižnica i knjižničara je omogućiti korisnicima pristup informacijama, osigurati slobodu govora, intelektualnu slobodu, kao i ne provođenje cenzure u knjižnici. Knjižnice su uvijek bile na strani korisnika i štitile njihovu privatnost i prava, jer je to jedna od glavnih uloga knjižnica i knjižničara, omogućiti korisnicima pristup informacijama, slobodu govora, intelektualne slobode. Knjižnice su među prvima stale iza korisnika u slučaju NSA nadziranja[62] te to nije bila prva borba knjižničara za prava svojih korisnika. Povijest je puna slučajeva u kojima su knjižnice bile glavni borci, no imale su i one trenutke u kojima je većina nadglasala manjinu, tako da su prava korisnika na privatnost bila ugrožena i u knjižnicama.

5.1.1. Problemi u čuvanju privatnosti korisnika u knjižnicama

U prošlosti kada bi vlada trebala pomoć, pozvali bi knjižničare, no zbog toga bi knjižnična profesija i sami knjižničari osjećali tenzije jer se nalaze u ulogama čuvara javnog dobra i zaštitnika intelektualnih sloboda, dok s druge strane vlada od njih očekuje da javno dobro nekih osoba stave u drugi plan kako bi se zaštitili drugi. Zbog tih tenzija neke su knjižnice posustale i odustale od svojih etičkih načela.

Početkom Prvog svjetskog rata, tek nedavno osnovano Američko knjižničarsko društvo – ALA (1876. godine) je pružalo standarde za knjižnični menadžment i profesionalne aktivnosti, kao što je razvoj zbirki. Tada je rat predstavljao pravu priliku za knjižničare jer su

[62] Usp. NSA surveillance: how libraries have been on the front line to protect privacy. URL: http://www.theguardian.com/world/2015/jun/05/nsa-surveillance-librarians-privacy (2016-01-10)

mogli razviti svoju profesiju tako što bi preobrazili svoje ustanove u centar ratne podrške u zajednici. Nakon rata, ALA je ustanovila Knjižnični odbor za ratne usluge, a usluge su bile mobilne dostave knjiga, prodaja obveznica i kampanje štednje hrane. U sklopu mobilne dostave knjiga, dostavljeno je više od deset milijuna knjiga i časopisa na pet tisuća lokacija, koje su uključivale i 36 novo-sagrađenih knjižnica. No tijekom godina, donešeni su zakoni koji su ograničavali slobodu govora te je bilo ilegalno govoriti, pisati ili objavljivati bilo što protiv vlade SAD-a, a tijekom tog vremena od knjižničara se također tražilo da nadziru korisnike.[63] 1918. poslana je naredba da se iz knjižnica uklone svi materijali o eksplozivima te da se imena osoba koje su tražile takve materijale prijave vojsci. Većina knjižnica su poslušale, a neke koje su bile protiv toga su se dosjetile inovativnih načina sprječavanja kršenja korisničke privatnosti tako što su smanjile broj materijala i pristupa istima. Knjižnični odbori su promicali micanje knjiga na njemačkom, dok su neki knjižničari čak i zapalili materijale na njemačkom. Objavom popisa knjiga za uklanjanje iz narodnih knjižnica diljem zemlje, dovelo je knjižničare u situaciju u kojoj nisu htjeli sukobe s vlasti i građanima, a zbog te situacije knjižnična zajednica je u potpunosti odbacila nekoliko hrabrih knjižničara koji su se suprostavili vladi i njihovim zahtjevima te su htjeli zaštititi privatnost korisnika. Starr navodi kako se između dva rata pojavila debata o slobodi pristupa u knjižnicama, gdje su tradicionalisti podržavali zaštitu vrijednosti zajednice kroz restriktivne politike knjižnične nabave, dok su progresivne mase podržavale razvoj nabave koja je neutralna i predstavlja sva gledišta. Tijekom 1938. knjižničari su bili pozvani da budu protiv cenzure, a Archibald MacLeish je 1940. zatražio od knjižničara da prihvate odgovornosti za opstanak demokracije. ALA je podržala taj stav, te je pet dana nakon napada na Pearl Harbor poslala deklaraciju u kojoj poziva sve knjižnice da postanu ratni informativni centri. [64]

Cenzura knjiga i ostalih knjižničnih materijala događala se ne samo u SAD-u, već i diljem svijeta, a u knjižnicama Sovjetskog saveza cenzura se nije odnosila samo na knjige, već i na filmove, predstave i druge umjetnosti. Razlozi za cenzuru su uključivali anti-sovjetsku propagandu, misticizam, kršenje službenih tajni i drugo, a sastavljeni su i popisi knjiga koje nisu smjele u knjižnice.[65]

[63] Usp. Starr, Joan. Libraries and national security: an historical review. // First Monday 9, 12(2004). URL: http://firstmonday.org/ojs/index.php/fm/article/view/1198/1118 (2016-03-17)
[64] Usp. Isto.
[65] Usp. Rogers, Robert A. Censorship and libraries in the Soviet Union. // Journal of library history, philosophy, and comparative librarianship 8, 1(1973). Str. 26.

U SAD-u se 1942. zahtjevalo od knjižnica da uklone materijale o naoružanju i kriptografiji te da FBI-u prijave imena osoba koje su tražile te materijale. ALA je proslijedila zahtjev prema 187 knjižnica za koje su smatrali da imaju takve materijale, a knjižničari koji su preispitivali zahtjev su to činili prema praktičnim, a ne etičkim načelima te su se knjižničari koji nisu dobili zahtjev žalili vlastima što su bili izostavljeni. Iako je ALA 1939. objavila etički kodeks u kojem se ističe pravo korisnika na privatnost, u stvarnosti su knjižničari tretirali privatnosti kao luksuz namjenjen za vrijeme mira, koji će se vratiti tek s pobjedom.[66]

5.1.2. Borba za privatnost korisnika nakon Drugog svjetskog rata

Poslije Drugog svjetskog rata i pojačanih tenzija između Sovjeta i SAD-a, američke vlasti su poduzele akcije koje su izazivale strah i pritisak na knjižnice, knjižničare i druge javne djelatnike. Počelo je kao anti-sovjetsko i anti-komunističko pročišćavanje knjiga no ubrzo se proširilo na sav materijal koji je bio anti-američki, a zaposleni knjižničari su morali odlučiti kako će se nositi s tim te su raspravljali o uklanjanju knjiga, premještanju i drugačijem označavanju. S druge strane, sovjetske vlasti su koristile knjižnice kao sredstvo koje promovira propagandu i koje je upozoravalo na opasnosti američkog kapitalizma. Sovjeti su također strahovali da će se američke informacijske tehnologije uvući u socijalističko društvo.[67]

ALA je donijela dvije odluke, jednu 1948. i drugu 1953. godine kojima su se podržavale intelektualne slobode i protivilo cenzuri te koje su podržavale knjižničare. To je bio prvi korak u stvarnoj borbi, koja je dala priliku knjižničarima da budu borci za demokratsku slobodu i slobodu čitanja. Carpenter navodi kako je prva knjižničarka koja je završila u zatvoru jer je branila privatnost i intelektualnu slobodu bila Zoia Horn, koja je provela tri tjedna u zatvoru 1972. godine jer je odbila svjedočiti protiv aktivista koji su se protivili Vijetnamskom ratu.[68] Kongres je 1978. godine prihvatio zakon o protuobavještajnom nadzoru

[66] Usp. Starr, Joan. Nav. dj.
[67] Usp. Richards, Pamela Spence. Cold war librarianship: Soviet and American library activities in support of National Foreign Policy. //Libraries and Culture 36, 1(2001). Str. 195-197.
[68] Usp. Carpenter, Zöe. Librarians versus the NSA: your local library is on the front lines against government surveillance, 2015. URL: http://www.thenation.com/article/librarians-versus-nsa/ (2016-01-16)

(eng. Foreign Intelligence Surveillance Act – FISA), a zakon obuhvaća ograničenja pod kojima bi agencije mogle prikupiti informacije bez nadzora.

Starr piše kako su se 1987. FBI agenti u knjižnici na Sveučilištu u Columbiji raspitivali o stranim korisnicima knjižnice, no zbog knjižničarke Paule Kaufman koja ih je odbila i prijavila IFC-u, Odboru za intelektualnu slobodu (eng. Intelectual Freedom Committee) nisu uspjeli u svom naumu. FBI je naveo da je taj zahtjev naredba knjižničarima da prijave knjižnične korisnike koji mogu biti diplomati stranih sila koji regrutiraju agente ili prikupljaju informacije o potencijalnim opasnostima za sigurnost. IFC je pozvao knjižničare da prijave slične incidente i objavio sažetak onoga što FBI smatra sumnjivim, kao razmjena dokumenata s drugim knjižničnim korisnicima, pričanje na stranom jeziku ili traženje materijala o podzemnim tunelima, vojnim instalacijama ili tehnološkom napretku. Kasniji pregledi u FBI-ev program nadziranja knjižnica je otkrio da je program djelovao tijekom 1973. i kasnije tijekom 1985., te iako je FBI rekao da je program ograničen na područje New Yorka, istraživanje je pokazalo kako je nadziranje bilo prošireno s prijavljenim incidentima od Marylanda, Virginije, Floride, Pennsylvanije, Ohioa, Wisconsina, Michigana, Utaha, Teksasa do Kalifornije. IFC je izdao izjavu u kojoj upozorava knjižničare na upletanje vlade bez naloga na osobnu privatnost i pozvao knjižničare da zaštite privatnost korisnika.[69] 1988. predsjednik IFC-a je na sudu izjavio kako je Library Awareness Program opasnost za fundamentalnu slobodu. Iduće godine je objavljena informacija kako je FBI proveo više od sto provjera podataka o knjižničarima ili njihovim suradnicima, od kojih su većinom bili oni koji su bili protiv Library Awareness Programa, također, iako je FBI objavio da je program ugašen 1987. informacije su pokazale kako su se istraživanja nastavila i tijekom 1989., a Judith Krug, ALA-ina direktorica ureda za intelektualne slobode je izjavila kako su knjižničari vjerovali što im je rečeno, no da su ih nastavili pozivati nakon 1987., da su osobe koje su se protivile bile istraživane te da zapravo nisu sigurni koliko su mislili da jesu. [70]

Miješanje vlade i države u posao knjižnica nije ograničen samo na SAD, već su se slične stvari događale i u Hrvatskoj i hrvatskim knjižnicama gdje je prije 90-ih godina policija bila vrlo zainteresirana saznati tko, na primjer, čita emigrantski tisak i više je hrvatskih knjižničara bilo suočeno s dvojbom otkriti ili ne otkriti imena čitatelja.[71]

[69] Usp. Starr, Joan. Nav. dj.
[70] Usp. Isto.
[71] Usp. Horvat, Aleksandra. Nav. dj.

5.1.3. Domovinski zakon (Patriot Act) i Zakon o slobodi (FREEDOM Act)

Nakon terorističkih napada 11. rujna u New Yorku, vlada SAD-a u listopadu 2001. je donijela novi zakon, Domovinski zakon (eng. USA Patriot Act, kratica od Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act).[72] Domovinski zakon je omogućio upletanje vlade u mnoge aspekte običnog života, pa tako i u korištenje knjižnice.

Kao rezultat promjena koje je donio Domovinski zakon, svaka obavještajna istraga koja se dogodi u knjižnici može biti opsežnija nego prije. Prije zakona, obavještajne informacije su trebale biti glavni dio istrage, no nakon donošenja zakona informacije trebaju biti važne za istragu, što olakšava nadziranje u knjižnicama. Podaci koji su mogli biti pretraženi u knjižnici uključivali su tiskane ili elektroničke knjige, zapise, dokumente, a zapisi mogu uključivati transakcije, koje se odnose na korisnike i djelatnike, korisničke zapise, podatke o posudbi, podatke o korištenju računala i podatke o pretraživanju.[73] Domovinski zakon je također omogućio nadziranje elektroničkih i telefonskih razgovora, koje uključuju podrijetlo, sadržaj i odredište telefonskog poziva, glasovne poruke, elektroničke pošte i drugih oblika komunikacije korisnika i djelatnika u knjižnici. Zakon je također omogućio dijeljenje informacija između agencija, što je značilo da sve informacije koje su prikupljene mogu koristiti različite agencije. Četiri elementa Domovinskog zakona se odnose na knjižnice i istraživače: 1) zakon proširuje okolnosti pod kojima se nadzor i pretresi mogu dogoditi u knjižnicama te zabranjuje diskusije o istrazi; 2) zakon stvara širu definiciju onoga što agencije mogu pretražiti i uzeti iz knjižnica; 3) zakon omogućuje praćenje i pretraživanje komunikacija koje su se odvijale putem elektroničke pošte; 4) zakon mijenja legalne mehanizme preko kojih agencije traže informacije.[74] Dio Domovinskog zakona pod nadzivom sekcija 215 imala je naziv 'odredba knjižničnih podataka', jer je od knjižničara zahtjevala da podatke o posuđenim knjigama korisnika, kao i o njihovim računalnim podacima predaju agencijama te

[72] The USA Patriot Act: preserving life and liberty. URL: https://www.justice.gov/archive/ll/highlights.htm (2016-07-25)
[73] Usp. Jaeger, Paul T... [et al]. The USA Patriot Act, the Foreign Intelligence Surveillance Act, and Information Policy Research in Libraries: issues, impacts, and questions for libraries and researchers. // The Library Quarterly: information, community, policy 74, 2(2004). Str. 100 - 104.
[74] Usp. Isto.

su nalogom zabranili knjižničarima spominjanje korisnicima da su njihovi podaci sada u rukama vlade.[75]

2002. godine ALA-in ured za intelektualnu slobodu (eng. Office of Intellectual Freedom – OIF) je evaluirao implikacije Domovinskog zakona i objavio dokument pod nazivom Domovinski zakon u knjižnici: analiza Domovinskog zakona povezanog s knjižnicama (eng. *The USA Patriot Act in the Library: Analysis of the USA Patriot Act Related to Libraries*)[76], a dokument je sadržavao objašnjenja relevantnih sekcija zakona bez savjeta knjižničarima kako se nositi u slučaju da se nađu pod istragom. Dva mjeseca kasnije ALA je prihvatila zakon o privatnosti u kojem stoji da u knjižnici (fizičkoj ili virtualnoj) pravo na privatnost je pravo pojedinca bez da se njegovi interesi pregledavaju ili ispitivaju od strane drugih. Povjerljivost postoji kada knjižnica posjeduje osobne informacije o korisnicima i čuva te informacije kao privatne.[77]

2003. ALA je donijela odluku kao odgovor na Domovinski zakon; poticala je učenje o zakonu i opasnostima koje prijete intelektualnoj slobodi te da knjižnice trebaju prihvatiti i implementirati privatnost korisnika i politiku zadržavanja podataka, tako što bi prikupljale samo informacije koje su potrebne za knjižnični rad. Odluka je povezala ALA-u s drugim ustanovama s istim ciljem, a to je zaštita prava na upite i slobodu izražavanja. Također, odluka je uključivala dio koji nalaže da će nabaviti i objaviti javnosti informacije o nadziranju knjižnica i korisnika knjižnice od strane raznih agencija. ALA je pokrenula nekoliko projekata koji pomažu knjižničarima i ravnateljima knjižnica kod problema koji mogu nastati tijekom svakodnevnog knjižničnog poslovanja. Na svojim web stranicama nude edukativne materijale koji informiraju djelatnike i članove zajednice o tim problemima te o razvijanju lokalne politike za zadržavanje zapisa i odgovor na naloge za pretraživanje. ALA je također inicirala kampanje u kojima prikuplja potpise za suzbijanje sekcije 215, a 2003. u javnost je izašla informacija da je FBI kontaktirao oko 50 knjižnica kao dio istrage.[78]

Mediji su izvjestili o mnogobrojnim odgovorima na Domovinski zakon od strane knjižničara i knjižnica, a uključivali su svakodnevno uništavanje internetskih pristupnih lozinki,

[75] Usp. Glaser, April. Long before Snowden, librarians were anti-surveillance heroes, 2015. URL: http://www.slate.com/blogs/future_tense/2015/06/03/usa_freedom_act_before_snowden_librarians_were_the_anti_surveillance_heroes.html (2016-01-15)
[76] Analysis of the USA Patriot Act related to libraries. URL: http://www.ala.org/offices/oif/ifissues/issuesrelatedlinks/usapatriotactanalysis (2016-07-25)
[77] Usp. Starr, Joan. Nav. dj
[78] Usp. Isto.

postavljanje znakova koji upozoravaju na gubitak privatnosti te educiranje korisnika. Leigh Estabrook i suradnici sa Sveučilišta u Illinoisu su proveli istraživanje među knjižničarima, gdje su istraživali knjižničare u mjesecima nakon napada te godinu dana kasnije. Nešto više od polovice ispitanika su odgovorili kako nisu surađivali s agencijama i zahtjevima za korisničkim podacima i internetskim navikama, a nekoliko knjižnica je promijenilo postojeće politike pristupa. Većina je educirala djelatnike o Domovinskom zakonu i knjižničnim politikama privatnosti. U suprotnosti onome što je objavila vlada, istraživanje je pokazalo kako su agencije posjetile najmanje 545 knjižnica, a smatraju kako je taj broj i niži od stvarnog zbog zabrane otkrivanja činjenice da su knjižnice bile pod nadzorom. Istraživanje je također pokazalo kako su knjižničari za razliku od javnosti, spremniji suprostaviti vladi zbog uklanjanja informacija s web stranica.[79] Zabrane o informiranju korisnika su utjecale na sve vrste knjižnica, a također su utjecale na interakciju knjižničara s korisnicima što je moglo dovesti do toga da neki korisnici promijene svoje ponašanje pri traženju informacija u knjižnici, a zabrana je utjecala i na usluge, sredstva i načina rada u knjižnicama te je povezano s problemima sigurnosti, privatnosti, slobode govora i akademske slobode.[80]

Carpenter upozorava na problem odnosa prema osobama muslimanske vjere koje koriste računalo u knjižnici kako bi razgovarali s obitelji u inozemstvu ili aktivisti koji planiraju protest protiv policijske brutalnosti, njihovi digitalni tragovi su podložni nadziranju, kao i tragovi ostalih ljudi. U tjednima nakon 11. rujna FBI je objavio kako su neki od terorista koristili knjižnice u Floridi kako bi isplanirali napad. Iako je agencija prikupila podatke o njihovim posjetima preko normalnih naloga, počela su nagađanja da su knjižnice postale sigurna utočista za teroriste.[81] Knjižničari su se susreli s činjenicom da je svaka osoba koja je ušla u knjižnicu potencijalna meta FISA istrage, a sve aktivnosti unutar knjižnice dio istrage, što je značilo da su svi knjižnični korisnici potencijalni sumnjivci. Problemi koji su nastali s ovim zakonom su veza između knjižničara, knjižnice i korisnika, dok su drugi problemi ograničenja onoga što su korisnici slobodni čitati u knjižnicama. Popisi pročitanih knjiga koje su korisnici čitali ne moraju nužno otkrivati dobre ili loše namjere osobe, no kao dio FISA istrage ti popisi mogu biti sumnjivi agencijama. Sve navedeno moglo je dovesti do samocenzure knjižničara, smanjivanje onoga što knjižničari žele čitati u knjižnici i promatranje drugih knjižničara na isti način kao i korisnike. Sve to je imalo utjecaj na slobodu mišljenja i izražavanja u knjižnicama. Knjižnice prikupljaju podatke kao što su posudba

[79] Usp. Isto.
[80] Usp. Jaeger, Paul T... [et al]. Nav. dj. Str. 101.
[81] Usp. Carpenter, Zöe. Nav. dj.

knjiga, podatke o korištenju računala, broj osoba koje su pohađale edukacije i drugo, te ih knjižnice koriste za menadžerske svrhe i zbog budžeta. No, zbog zakona su svi ti podaci pod FISA nalogom, a neke su knjižnice zbog toga počele uništavati zapise, brisati informacije o korištenju računala kao i uništavati zapise o posudbi knjiga.[82]

Glaser opisuje slučaj iz 2005. godine kada su četiri knjižničara iz Connecticuta išli na sud zbog zahtjeva. Zahtjev je omogućavao FBI-u uvid u velike količine korisničkih podataka od pružatelja internetskih usluga bez sudskog naloga. Sudski postupak je na kraju odbačen, a knjižničari su jedini koji sada mogu otvoreno pričati o svojim iskustvima. Iste godine je ALA podnijela zahtjev Vrhovnom sudu s namjerom odbacivanja Domovinskog zakona. Knjižničari se nisu borili samo na sudu, postavljali su znakove koji su obavještavali korisnike da ne mogu jamčiti da će njihovi podaci o čitanju biti povjerljivi, na znakovima je pisalo „FBI nije bio ovdje (pratite jako pažljivo na uklanjanje ovog znaka)“.[83] Primjer takvih aktivnosti je i onaj iz 2003. godine kada su knjižničari u Paulding Countyju, Ohio postavili takve znakove na kojem su upozoravali korisnike da zbog brige o nacionalnoj sigurnosti njihove internetske navike, lozinke i e-mail sadržaji mogu biti pod nadzorom, dok su drugi knjižničari dijelili informativne letke ili organizirali sastanke o novim vladinim snagama za nadziranje. Knjižnice su počele uništavati podatke kao što su liste čekanja za korištenje računala, cache tvrdih diskova te druge podatke. Barbara Gail Snider navodi kako su knjižničari prije bili predstavljeni s knjigom, sada su predstavljeni s uništavačem papira.[84] Jedan od zanimljivih primjera koje navodi The Guardian je i onaj kada su se knjižničari borili kako bi zaštitili identitet korisnika koji je pisao bilješke na marginama biografije Osame bin Ladena. Tim postupkom knjižničari su željeli ukazati na povjerljivost podataka o korisnicima jer smatraju kako postoji direktna povezanost s demokracijom. Postavlja se pitanje, ako osobe nisu slobodne istraživati i čitati ili pretraživati internet, kako onda mogu sudjelovati u građanskim aktivnostima.[85] Jeager ukazuje da pod FISA istragom, podaci uključuju knjige, podatke, papire, dokumente i druge materijale, a Domovinski zakon uključuje i e-mailove (adresu i sadržaj), posjećene web stranice, korištenje baza podataka, pohađanje tečajeva u knjižnici, računalne datoteke i druge informacije koje se nalaze na tvrdom disku. Isti elementi zakona nisu ograničeni samo na korisnike, već omogućuju i pristup informacijama o privatnim

[82] Usp. Jaeger, Paul T... [et al]. Nav. dj. Str. 105.
[83] Usp. Glaser, April. Nav.dj.
[84] Usp. Carpenter, Zöe. Nav. dj.
[85] Usp. NSA surveillance: how libraries have been on the front line to protect privacy. URL: http://www.theguardian.com/world/2015/jun/05/nsa-surveillance-librarians-privacy (2016-01-10)

komunikacijama djelatnika. Sekcije Domovinskog zakona koji to omogućuju su sekcija 215, koja se najviše odnosi na knjižnice, kao i sekcije 203, 206-7, 209-10, 214, 216 i 218.[86]

Nakon što je Snowden objavio dokumente u kojima je otkriveno kako je NSA nadziranjem prikupljala metapodatke, knjižničari su među prvima shvatili ozbiljnost problema. Metapodaci su dijelovi informacija koje opisuju ili pomažu pri pronalaženju drugih informacija. U knjižnici metapodaci su na primjer autorovo ime ili naslov djela kao i individualne riječi iz naslova. Metapodaci su također deskriptori kojima se opisuje sadržaj članka ili knjige. Metapodaci koje NSA prikuplja su informacije o telefonskim pozivima, ali ne i sam sadržaj razgovora, već trajanje poziva, koga je osoba zvala i slično. No, metapodaci koji se prikupljaju u knjižnicama o korisnicima su primjerice koliko studenata je posudilo određene knjige, koliko puta je neka knjiga ili DVD posuđen. Većina knjižnica ne zadržava podatke o tome tko je posudio određeni naslov. Knjižničari smatraju da ono što osoba čita, gleda ili sluša je privatna stvar koja se tiče samo te osobe, a etika knjižničara se bazira na korisničkoj povjerljivosti još od 1936. godine. Metapodaci u knjižnici mogu biti jako korisni, jer knjižničare ne zanima tko je čitao određeni naslov, njih samo zanima je li taj naslov posuđen pet ili pedeset puta u zadnjih deset godina.[87]

Nakon što je Domovinski zakon ponovno došao u interes javnost nakon Snowdena, političari, knjižničari, ali i ostali pojedinci zabrinuti oko pojma privatnosti i nadziranja, tražili su ukidanje zloglasnog Domovinskog zakona, a posebno sekciju 215. U lipnju 2015. godine, nakon dugotrajne debate američki Kongres je odobrio Zakon o slobodi (eng. USA FREEDOM Act).[88] Taj zakon poništava sekciju 215 Domovinskog zakona kako bi se zabranilo masovno prikupljanje podataka, kao što su podaci o telefonskim razgovorima i internetskim metapodacima.[89] ALA je podržala činjenicu da je prihvaćen Zakon o slobodi te navodi kako je prihvaćanje ovog zakona presudno jer je ovo prva značajna reforma zakona o nadziranju u skoro 15 godina što znači da knjižnice, tehnološke kompanije, zagovarači građanske slobode te obični građani i drugi žele nazad privatnost koja im je obećana.[90] Ovaj zakon dopušta vladi da zahtjeva samo one zapise koji se odnose na aktivnosti osoba koje su

[86] Usp. Jaeger, Paul T... [et al]. Nav. dj. Str. 108-117.
[87] Usp. The library, the surveillance state, and you. URL: https://librarysmcm.wordpress.com/2013/07/29/the-library-the-surveillance-state-and-you/ (2016-01-17)
[88] USA Freedom Act. URL: https://judiciary.house.gov/issue/usa-freedom-act/ (2016-07-25)
[89] Usp. Domestic surveillance reform: private data collection and the USA FREEDOM Act. // Congressional Digest, 2015.
[90] Usp. ALA news. ALA calls passage of USA FREEDOM Act a milestone. URL: http://www.ala.org/news/press-releases/2015/06/ala-calls-passage-usa-freedom-act-milestone (2016-04-26)

pod istragom i zapise pojedinaca koji su u kontaktu s tom osobom. Zakon donosi reformu kojom se zabranjuje slanje zahtjeva bez sudskog naloga.[91]

Novi zakon nije savršen, no ide u pravom smjeru te sadrži glavne principe koje je podržala ALA:

- Zabranjuje masovno prikupljanje podataka, ne samo telefonskih razgovora već i drugih materijalnih stvari (izraz koji se koristio u sekciji 215), koji uključuju knjižnične zapise. Što znači da bilo koji zahtjev za podacima mora biti povezan s određenom istragom i biti povezan s usko određenim pojmom koji je određen u zakonu. NSA i FBI više neće biti u mogućnosti reći da su povijesti pretraživanja na javnim računalima materijalne stvari.

- Otvara mogućnost provjere zabrane o otkrivanju istrage.

- Omogućava tvrtkama, knjižnicama i drugima javnu objavu činjenice da su bili podvrgnuti sekciji 215 ili drugim zahtjevima vlade ili agencija.

- Zahtijeva od FISA suda stvaranje komisije koji su objektivni u donošenju odluka.[92]

ALA smatra kako je donošenje Zakona o slobodi ključan korak u napredovanju prema boljim uvjetima i trajnom cilju kojem idu knjižnice i knjižničari, kao i drugi pojedinci usmjereni prema zaštiti privatnosti.[93]

5.2. Kako zaštiti privatnost knjižničnih korisnika na internetu

Knjižnica je jedna od ustanova koja može pomoći u zaštiti korisnika i njihove privatnosti na internetu, jer su pojam privatnosti i knjižnica usko povezani. Knjižnice i knjižničari smatraju da je pravo na privatnost primarno pravo svakog pojedinca, što se odnosi i na korisnike koji se služe knjižnicom i računalima u knjižnici. Zbog prije navedenih razloga u kojima je pravo na privatnost korisnika bila ugrožena, knjižnice i knjižničari su odlučili poduzeti mjere kako

[91] Usp. Cox, Krista. The day we fight back: NSA reform bills to end mass surveillance and provide greater transparency, 2014. URL: http://www.arl.org/news/arl-news/3123-the-day-we-fight-back-nsa-reform-bills-to-end-mass-surveillance-and-provide-greater-transparency#.Vulz79LhDDd (2016-02-20)
[92] Usp. Eisgrau, Adam. Supporting the USA FREEDOM Act of 2015: ALA's perspective. URL: http://www.districtdispatch.org/2015/05/supporting-the-usa-freedom-act-of-2015-alas-perspective/ (2016-04-26)
[93] Usp. Isto.

bi spriječili daljnja kršenja privatnosti korisnika. Knjižničari su bili primorani promijeniti navike i steći vještine u korištenju novih tehnologija kako bi se zaobišlo špijuniranje od strane vladinih agencija i korporacija. Knjižnice su počele nuditi edukacije i tečajeve za korisnike u kojima objašnjavaju na koji način korisnici mogu zaštititi svoju online privatnosti, koje programe i alate koristiti koji će im omogućiti anonimnost dok pretražuju internetske stranice ili kada koriste društvene mreže. Osim što knjižničari educiraju korisnike i osvještavaju ih o opasnostima na internetu koje ugrožavaju njihovu privatnost, oni također educiraju druge knjižničare i uvode alate za zaštitu u knjižnice koje instaliraju na računala. Osim što obavještajne agencije mogu nadzirati internetske aktivnosti korisnika, knjižnice na taj način žele osigurati da ako agencije zatraže korisničke zapise, mogu znati da će privatnost korisnika ostati privatna. IFLA je navela kako knjižnice i informacijske ustanove imaju dužnost osiguravanja privatnosti njihovih korisnika te da će sredstva i usluge koje koriste ostati povjerljive.[94] U post-Snowdenovskom svijetu gdje se vladino i korporativno nadziranje spojilo kako se internet širio, principi zaštite privatnosti i osiguravanje intelektualne slobode su važniji nego ikada. Alati koje knjižničari uvode u knjižnice su program Tor, web tražilicu DuckDuckGo koja ne sprema korisničko pretraživanje, HTTPS Everywhere koji omogućava enkripciju stranica što onemogućava nadziranje.

Jedna od osoba koje su se zauzele za online privatnost knjižničnih korisnika je knjižničarka Alison Macrina, koja radi u knjižnici u Bostonu. Macrina je osnovala knjižnični projekt pod nazivom Library Freedom Project[95] koji podučava građane i korisnike knjižnice kako se zaštititi od nadziranja (vladinog i korporativnog), što je jedna od glavnih uloga knjižničara u digitalnom informacijskom društvu.

Osim što je instalirala nekoliko alata za čuvanje privatnosti na računala narodne knjižnice u Watertownu, Macrina je također poučavala korisnike o korištenju računala i privatnosti na internetu te je organizirala nekoliko radionica za knjižničare iz Massachussettsa o digitalnom nadziranju. Iako su nekim knjižničarima pojmovi poput nadziranja na internetu novi, informacijskim stručnjacima borba za intelektualnu slobodu i slobodu čitanja i izražavanja nije nova, kao ni prava marginaliziranih ljudi koji su pod najvišim stupnjem nadziranja.[96] Pokazalo se kako osobe koje nisu bijele, prolaze kroz veći stupanj nadziranja i meta su

[94] Usp. IFLA Statement on privacy in the library environment. URL: http://www.ifla.org/publications/node/10056 (2016-05-23)
[95] Library Freedom Project. URL: https://libraryfreedomproject.org/ (2016-05-23)
[96] Usp. Radical librarianship: how ninja librarians are ensuring patrons' privacy. URL: http://boingboing.net/2014/09/13/radical-librarianship-how-nin.html (2016-01-10)

učestalog ispitivanja i praćenja. Macrina navodi kako je o privatnosti počela razmišljati više nakon Snowdenovih otkrića, nije znala koliko je slučajeva kršenja privatnosti i zašto se to ne spominje. Također smatra kako u današnjem vremenu prikupljanja podataka od strane raznih agencija i korporacija, knjižničari ne poduzimaju dovoljno mjera kako bi zaštitili svoje korisnike, a u mnogo slučajeva je to zbog toga što nemaju dovoljno tehničkih vještina. Narodna knjižnica u San Joseu je pokrenula pilot projekt koji bi podučavao pismenost o privatnosti korisnicima knjižnice svih uzrasta. Macrina napominje kako se stvara pokret knjižničara koji su borci za privatnost, imaju sve više samopouzdanja u ono što znaju i što mogu pridonijeti u razgovoru o privatnosti jer su povezani s lokalnom zajednicom.[97] Kako bi mogli podučavati korisnike i uvesti potrebnu zaštitu u knjižnice s ciljem očuvanja privatnosti korisnika na internetu, knjižničari također trebaju steći nove vještine i znanja koja će im omogućiti instaliranje programa i alata za zaštitu privatnosti; knjižničari trebaju biti informacijski pismeni i znati na koje načine funkcionira određeni alat i za što služi, kako bi ih sami mogli koristiti te objasniti korisnicima što to znači za njihovu privatnost i kako se sami mogu zaštititi na vlastitim računalima.

Knjižničari koji imaju dodatna znanja o tehnologiji mogu održavati radionice u knjižnici na temu o zaštiti privatnosti na internetu i ukazati na probleme koji se javljaju. Korisnicima treba objasniti osnovne principe te najvažnije, objasniti kako se ove teme uklapaju u njihov život i zašto su važne. Knjižničari trebaju misliti i kako proširiti paradigmu privatnosti da uključuje, ne samo korisničke podatke o posuđivanju građe, nego i komunikaciju koju obavljaju online. U narodnoj knjižnici u Brooklynu, knjižničari su u suradnji s Seetom Peña Gangadharanom radili na studiji digitalne uključenosti, koja je uključivala razgovore između knjižničara o tome što oni vide da korisnici rade ili znaju i što ne rade i ne znaju, kada je riječ o zaštiti i sigurnosti na internetu.[98] Razgovaralo se o knjižničarskom neznanju i kako se na tome može dalje raditi, a u knjižnicama se također održavaju radionice o programiranju, enkripciji i sigurnom web pretraživanju. Alison Macrina preporuča dodatke za web preglednike i savjetuje ljudima da razmisle o pokrivanju ugrađene kamere koje se nalaze na laptopima. Instalirala je HTTPS Everywhere (dodatak za web preglednike koji enkriptira komunikaciju korisnika s web stranicama te zaštićuje pretraživanje) kako bi korisnici koji se služe računalima u knjižnici mogli pretraživati internet sa sigurnim poveznicama. Savjeti o zaštiti

[97] Usp. Carpenter, Zöe. Nav. dj.
[98] Usp. Morrone, Melissa. How your local library can help you resist surveillance state, 2014. URL: http://wagingnonviolence.org/feature/local-library-can-help-resist-surveillance-state/ (2016-01-18)

privatnosti se lako nađu na internetu, no pouzdana i iskusna osoba koja će pomoći korisnicima pri određivanju što će instalirati na laptop ili kako zaštiti pametne telefone, je puno bolja opcija. Knjižnice mogu pomoći pri stvaranju društva sa znanjima i izvorima kako bi se zaštitila privatnost i digitalna prava. Knjižnice mogu smanjiti štetu koja nastane ako se uzme u obzir da osobe komuniciraju s bližnjima preko Facebooka, logiraju se na primarne e-mail adrese preko knjižničnih WI-FI mreža i upisivaju osobne podatke poput OIB-a na računalima koji možda nisu njihovi. Gangadharan napominje kako bi poučavanju informacijske pismenosti najbolje bile škole, knjižnice i druge ustanove u zajednicama te kako bi poučavale o novim materijalima, kao što su privatnost na internetu.[99]

5.2.1. Alati za zaštitu privatnosti na internetu

Kao jedan od glavnih alata koji se preporučuje u zaštiti privatnosti na internetu je enkripcija. Njezina dostupnost omogućuje onima koji imaju vještine i znanja, zaštitu privatnosti naspram vlade koja ne podržava takav oblik komunikacije. Onima koji nemaju te vještine i znanja, prijeti se njihovoj privatnosti, podvrgavajući ih rizicima masovnog nadziranja i ograničavajući njihovu mogućnost uključenja u demokratski proces. Specijalno izvješće Ujedinjenih naroda[100] iz 2015. navodi kako enkripcija i anonimnost omogućuju individualcima slobodu mišljenja i izražavanja u digitalnom dobu. Online alati koji omogućuju end-to-end (E2E) enkripciju su važni u osiguravanju slobode govora i zaštiti privatnosti. Iako enkripcija ne štiti metapodatke (e-mail adresu, podatke o lokaciji mobitela), štiti sadržaj onoga što je enkriptirano. Nakon Snowdena, povećalo se zanimanje za korištenje takvim alatima i povećao se broj alata koji žele iskoristiti zabrinutost oko nadziranja. Tako se povećao broj aplikacija za instant poruke koje nude enkripcijsku komunikaciju, kao što su Telegram, Whatsapp i Signal. No unatoč tome, Snowdenova otkrića nisu imala veliki utjecaj na druge enkripcijske alate, kao što su tehnologije za enkripciju e-maila. Bilo je za očekivati da vlade neće podržati razvoj i uporabu enkripcije, posebno američka i britanska čiji se premijer žestoko bori protiv enkripcije, navodeći da vlasti ne bi smjele dopustiti komunikaciju između osoba koju ne mogu pročitati, jer su upravo oni ti koji nadziru pojedince te s povećanjem korištenja enkripcije, dolazi do ometanja nadziranja, što agencijama nije po volji. Takvi stavovi mogu dovesti do toga da vlade i obavještajne agencije postave tzv. stražnja

[99] Usp. Isto.
[100] Cannataci, J. A. Report of the special Rapporteur on the right to privacy, 2015.

vrata u enkripcijske programe kako bi i dalje mogli nadzirati internetske aktivnosti i špijunirati korisnike.[101]

Jedan od najpoznatijih alata za zaštitu internetskih aktivnosti je Tor (eng. The Onion Router) koji je nastao kao projekt američke mornarice s ciljem zaštite vojne komunikacije, no 2002. je postao samostalan projekt, a stvorili su go Roger Dingledine i Nick Mathewson.[102] Tor usmjerava internetski promet kroz serije čvorova s ciljem pomutnje izvora pretrage, a Tor se smatra učinkovitim alatom u osiguravanju anonimnosti pri korištenju interneta. Zbog načina na koji funkcionira, nije moguće točno odrediti koliko osoba koristi Tor mreže, no od prosinca 2015. smatra se da Tor ima oko dva milijuna korisnika. Tor je učinkovit u zaustavljanju „trećih strana" u nadgledanju i prikupljanju podataka o korisničkoj web aktivnosti, no svejedno je osjetljiv na prijetnje koje uključuju subverziju preko kontrole malicioznih čvorova i tempiranih napada te pokušaja deanonimizacije korisnika. Tor mreža ima svojih nedostataka no treba uvidjeti da pruža visoku razinu zaštite za razliku od ostalih alata koji trenutno postoje. Što je veći broj korisnika koji koriste Tor, softver postaje učinkovitiji, tako povećavajući anonimnost korisnika.[103] Tor web pretražitelj osigurava privatnost korisnika tako što preusmjerava korištenje interneta preko raširene globalne mreže releja u spriječavanju web stranice u dohvaćanju korisnikove lokacije i kako bi se zaštitile korisnikove aktivnosti na internetu i pretraživane stvari od nadziranja drugih. Promet koji prolazi preko releja i servera mogu biti e-mail poruke, informacije s web stranica, osobni podaci i drugo. Tor je zapravo modificirana verzija pretražitelja Mozilla Firefox na čije se verzije nadograđuje Tor softver s dodacima i omogućava anonimnost te promijeni IP adresu korisnika. Tor također blokira Flash dodatke u pretražitelju koji mogu narušiti privatnost i izvući osobne i ostale podatke.[104] Mnoge vlade, posebno američka vlada, se protive uporabi Tora jer smatraju da je idealan alat za teroriste i ostale koji žele obavljati ilegalne poslove, a Tor im nudi anonimnost kojom to mogu ostvariti. Tor se ironično razvio od vojnog projekta s ciljem čuvanja tajni i komunikacija do alata koji sada koriste osobe koje žele zaštititi svoje tajne, što se osobama na visokim pozicijama ne sviđa.

Za zaštitu se također preporuča web tražilica DuckDuckGo, koja za razliku od drugih web tražilica kao što su Google, Bing ili Yahoo, ne sprema povijest pretraživanja korisnika.

[101] Usp. Clark, IJ. Nav. dj. Str. 11-12.
[102] Usp. Tor Overview. URL: https://www.torproject.org/about/overview (2016-05-23)
[103] Usp. Isto.
[104] Usp. Tor Overview. Nav. dj.

DuckDuckGo na svojoj stranici[105] navodi kako tražilica ne prikuplja i ne dijeli osobne podatke, tako što preusmjeri korisnički upit da ne šalje te upite drugim stranicama. Stranice će znati da je korisnik bio na njima, ali neće znati pomoću kojih upita je korisnik došao do njih. Kada korisnik posjeti stranicu, web preglednik šalje podatke o računalu, kao što je IP adresa, DuckDuckGo s druge strane ne sprema takve podatke, čime se može osigurati privatnost korisnika. Alison Macrina je pobornik još jednog korisnog alata u zaštiti privatnosti, HTTPS Everywhere[106] dodatak koji se instalira na web preglednike kao što su Firefox, Chrome i Opera, što omogućava sigurnije pretraživanje jer je razina enkripcije povećana. HTTPS Everywhere je nastao u suradnji s The Tor Project i Electronic Frontier Foundation. Većina web stranica koristi HTTP koji za razliku od HTTPS-a nije enkriptiran te korištenjem tog protokola treće strane mogu saznati osobne podatke i sve što osoba pretražuje na internetu, a ovaj alat pretvara HTTP u HTTPS protokol.[107] Knjižnične web stranice, posebno online katalog, bi trebale koristiti HTTPS protokol kao zadani protokol zbog enkripcije i zaštite prometa između pretraživača i servera, čime se štiti privatnost pri pretraživanju kataloga i osigurava povjerljivost. Korištenje open source alternativa umjesto komercijalnih softvera može biti dobro, posebno zbog razloga što je open source softver bolji u pružanju zaštite privatnosti. Prebacivanje na open source pretraživače kao što je Firefox i korištenje ad-block dodataka koji blokiraju oglase, uklonile bi se osjetljivosti koje mogu ugroziti korisničku privatnost. Takve mjere bi se mogle i trebale poduzeti u knjižnicama i bili bi prvi koraci prema osiguravanju privatnosti knjižničnih korisnika.

5.2.2. Projekti zaštite privatnosti knjižničnih korisnika na internetu

Jedan od najpoznatijih projekata zaštite online privatnosti korisnika knjižnica u novije vrijeme je svakako projekt pod nazivom Library Freedom Project. Library Freedom Project[108] je projekt nastao suradnjom knjižničara, tehnoloških stručnjaka, odvjetnika i onih koji se zalažu za privatnost, a cilj projekta je ukazati na probleme nadziranja kroz provedbu intelektualnih sloboda u knjižnicama. Projekt podučava knjižničare o opasnostima nadziranja, o pravima na privatnost i odgovornostima, kao i o digitalnim alatima koji pomažu u zaustavljanju

[105] Usp. DuckDuckGo privacy policy. URL: https://duckduckgo.com/privacy (2016-05-23)
[106] HTTPS Everywhere. URL: https://www.eff.org/https-everywhere/ (2016-05-23)
[107] Usp. Isto.
[108] Library Freedom Project. URL: https://libraryfreedomproject.org/ (2016-05-23)

nadziranja. Projekt želi stvoriti promjene u knjižnicama i u zajednicama u kojima se nalaze, tako što će se privatnost staviti u centar rasprave. Nakon Snowdenovih otkrića 2013., Alison Macrina je osnovala Library Freedom Project i počela posjećivati narodne knjižnice diljem zemlje nudeći edukaciju o pravima na privatnosti, s posebnim naglaskom na tehnologije enkripcije. 2015. godine, Library Freedom Project je uspostavila Tor relejni čvor u knjižnici Kilton, New Hampshire, prvi takav relej u narodnoj knjižnici bilo gdje u svijetu. Tor releji se ponašaju kao čvorovi koji puštaju promet međusobno kako bi se omogućila troslojna anonimna enkripcija, te su važni u učinkovitosti usluge.[109] Ministarstvo domovinske sigurnosti (eng. Department for Homeland Security) je kontaktiralo policijsku upravu u gradu Lebanon, New Hampshire zbog narodne knjižnice Kilton te je policija, koristeći krilaticu da izbjegavanje nadziranja dovodi ljude u opasnost, pokušala spriječiti knjižnicu da provede taj projekt.[110] Unatoč pokušajima koji su doveli do kratkog zaustavljanja programa, relej je naposlijetku vraćen. Nadalje, predložena je legislacija koja bi dopustila knjižnicama instaliranje i korištenje kriptografskih softvera za privatnost, uključujući Tor. Uspostavljanje Tor releja u narodne knjižnice u SAD-u pokazuje da je moguće osigurati privatnost korisnika u vremenu masovnog nadziranja, osiguravajući veću autonomiju u korištenju interneta.[111]

Library Freedom Project na svojoj web stranici nudi korisne savjete i popis alata koji se mogu instalirati ili u knjižnici ili korisnici mogu sami na svojim računalima staviti potrebne programe koji će zaštititi njihovu privatnost na internetu. LFP i njihovi suradnici posjećuju knjižnice diljem SAD-a i nude resurse koji su im potrebni kako bi zaštitili privatnost na internetu u svojim knjižnicama i kako bi zaštitili zajednicu u kojoj se nalaze. Nude edukacije za knjižničare koje podučavaju o raznim stvarima, kao što su prijetnje koje nastaju iz vladinog nadziranja, pravima na privatnost, objašnjavaju kako koristiti alate potrebne za zaštitu privatnosti. Također nude kurikulum o predavanjima o privatnosti, pomoć pri postavljanju infrastrukture za zaštitu privatnosti i druge oblike zaštite. Poseban dio web stranice je postavljen za knjižničare na kojem se nalaze resursi i alati koji su potrebni za zaštitu privatnosti knjižničnih korisnika na internetu.

Drugi projekt koji se bavi zaštitom privatnosti knjižničnih korisnika na internetu je projekt pod nazivom Choose Privacy Week. Choose Privacy Week je događanje pod

[109] Usp. Clark, IJ. Nav. dj. Str. 18-19.
[110] Usp. Clark, IJ. Surveillance, freedom, Tor and libraries. URL: http://infoism.co.uk/2015/09/surveillance/ (2016-01-14)
[111] Usp. Clark, IJ. The digital divide in the post-Snowden era. Str. 18-19.

pokroviteljstvom Ureda za intelektualnu slobodu. Projekt nudi besplatne video materijale, obrazovne brošure, planove predavanja i ostale ideje za knjižnice i knjižničare za obrazovanje korisnika o pitanjima koje se tiču privatnosti. Projekt također pomaže knjižnicama da postanu organizacijski modeli kada je riječ o zaštiti podataka i privatnosti knjižničnih korisnika.[112] Ovaj projekt je osnovan od strane ALA-e te je inicijativa koja poziva na osvještavanje korisnika knjižnica o pravima na privatnost u digitalnom dobu te se odvija u jednom tjednu svake godine. Knjižnicama su na raspolaganju alati potrebni u edukaciji i uključivanju korisnika te resursi pomoću kojih se misli kritično i korisnici se informiraju o svojoj privatnosti. Knjižnice diljem SAD-a će sudjelovati u CPW tako što će organizirati događanja i aktivnosti kojima se žele uključiti i osvijestiti knjižnični korisnici o problemima privatnosti. Web stranica[113] ima niz alata i savjeta kako informirati ne samo knjižničare već i knjižnične korisnike o problemima privatnosti na internetu. Savjetuju knjižničarima da na predavanjima prikazuju video materijale i dokumentarce, u kojima o privatnosti raspravljaju mladi, roditelji, knjižničari, autori poput Neila Gaimana i drugih. Oni upozoravaju na masovno nadziranje u digitalnom dobu i na koji način to vlade zloupotrebljavaju te kako prikupljaju, čuvaju i koriste podatke koje su prikupili o pojedinicima i njihovim životima. Također, održavaju razne radionice gdje se educiraju knjižnični korisnici o temama poput privatnosti na internetu, zašto je privatnost važna u digitalnom dobu, kako zaštititi svoju online privatnost, kako zaštititi privatnost mladih na internetu i ostalo. Edukacije se održavaju u svim vrstama knjižnica, od školskih, sveučilišnih do narodnih.

Velika većina projekata koji se bave zaštitom privatnosti na internetu korisnika knjižnica se odvijaju u SAD-u, jako je malo edukacija koje se provode u Europi, a koje se mogu usporediti s navedena dva projekta koja se provode diljem SAD-a i čije knjižnice educiraju ne samo korisnike, već i knjižničare. Oni svoja znanja prenose na korisnike te ih savjetuju kako i na koji način zaštititi privatnost na internetu koja je svakim danom u sve većoj opasnosti. Radionice i edukacije koje se bave zaštitom privatnosti knjižničnih korisnika na internetu i koje upozoravaju na opasnosti masovnog nadziranja u Hrvatskoj skoro pa nema. Tek nekoliko predavanja koja su održana u nekoliko većih knjižnica u Hrvatskoj, no ne pravih edukacija, koje će educirati i knjižničare i korisnike. Knjižničari trebaju imati znanja i vještine informatičke pismenosti kako bi znali koristiti alate i programe potrebne u zaštiti privatnosti

[112] Usp. Jones, Barbara M. Intelektualna sloboda u teškim vremenima. // Slobodan pristup informacijama: 10. okrugli stol / uredile Alemka Belan-Simić i Aleksandra Horvat. Zagreg: Hrvatsko knjižničarsko društvo, 2011. Str. 13.
[113] Usp. Choose Privacy Week. URL: https://chooseprivacyweek.org/ (2016-05-23)

te kako bi mogli podučiti korisnike o tome i dati im informacije koje se tiču njihove privatnosti na internetu. Manjak edukacijskih radionica i tečajeva se može pripisati i činjenici da još uvijek većina građana, kao i knjižničara, nisu svjesni opasnosti koje mogu ugroziti privatnost kada se koristi internet i druge tehnologije. Istraživanjem koje se provelo, htio se saznati stav i mišljenje studenata Informacijskih znanosti, koji će biti budući informacijski stručnjaci i knjižničari, o privatnosti na internetu i ulozi knjižnica u zaštiti privatnosti knjižničnih korisnika.

6. Istraživanje o zaštiti privatnosti na internetu među studentima Informacijskih znanosti u Zadru

6.1. Svrha i cilj istraživanja

Svrha ovog istraživanja je ukazati na važnost zaštite privatnosti na internetu te uloge knjižnica u zaštiti korisnika i njihove privatnosti na internetu od nadziranja koje provode vlade i korporacije. Mnogi nisu ni svjesni u kolikoj mjeri se podaci pojedinaca koje oni slobodnom voljom stavljaju na internet koriste u razne svrhe. Istraživanjem se želi osvijestiti buduće knjižničare o opasnostima kršenja privatnosti na internetu i masovnog nadziranja kojima se ugrožava njihova privatnosti i privatnost knjižničnih korisnika.

Glavni ciljevi ovog istraživanja bili su saznati kako i na koji način studenti Odjela informacijskih znanosti u Zadru štite privatnost na internetu te koje je njihovo mišljenje o ulozi knjižnica u zaštiti privatnosti na internetu i borbi protiv masovnog nadziranja. Istraživačka pitanja su:

1) Koje društvene mreže koriste i koje mišljenje imaju o prikupljanju podataka od strane oglašivača?
2) Koji osobni podaci su o njima dostupni na internetu?
3) Koliko je važna privatnost na internetu i što ispitanici čine kako bi se zaštitili?
4) Smatraju li ispitanici da su knjižnice važne za zaštitu privatnosti korisnika na internetu te jesu li upoznati s činjenicom da knjižnice aktivno sudjeluju u aktivnostima protiv masovnog nadziranja?

Hipoteza istraživanja je da

1) Ispitanici koji koriste društvene mreže i koji imaju ekspertna znanja iz korištenja računala imaju jače razvijenu svijest o problemima zaštite privatnosti na internetu i načinima zaštite privatnosti
2) Ispitanici ne prepoznaju knjižnice kao institucije koje sudjeluju u aktivnostima povezanim sa zaštitom privatnosti i u borbi protiv masovnog nadziranja

6.2. Metodologija istraživanja

Istraživanje je provedeno na Odjelu informacijskih znanosti Sveučilišta u Zadru, a ispitanici su bili studenti informacijskih znanosti.

6.2.1. Metoda i instrument istraživanja

Metoda korištena u istraživanju za prikupljanje podataka je kvantitativna metoda, a istraživački instrument je anketa. Anketa se definira kao vrsta statističkog istraživanja koje proučava agregate jedinica, najčešće ljudi, ekonomskih ili društvenih cjelina ili institucija. Drugim riječima, anketa je naziv za skup postupaka pomoću kojih se prikupljaju i analiziraju podaci prikupljeni od ljudi kako bi se saznali detalji o njihovu ponašanju ili o stavovima, mišljenjima, namjerama, interesima i slično, zbog potreba službene statistike, poslovnih istraživanja, ispitivanja javnoga mnijenja, istraživanja tržišta ili istraživanja u neke druge svrhe. Ankete se razlikuju prema načinu prikupljanja podataka, uz pomoć ili bez pomoći anketara i prema vrsti anketnog upitnika, papirnatog ili u elektroničkoj formi.[114]

Ispitanici, odnosno studenti informacijskih znanosti u Zadru su odabrani namjernim uzorkom, što znači da je sam istraživač odabrao tu skupinu za svoje istraživanje. Studenti su odabrani kao istraživački uzorak jer su skupina osoba koje su odrasle s tehnologijom, koriste internet i društvene mreže te su studenti knjižničarstva, koji se svakodnevno susreću s pojmovima zaštite privatnosti, intelektualne slobode, raznim informacijama iz područja koji su usko vezani s temom istraživanja. Broj ispitanika koji su ispunili anketu je 55. Ispitanicima je poslan anketni upitnik u elektroničkom obliku, preko online alata za izradu anketa SurveyMonkey. Anketa se sastojala od 26 pitanja, anketa (za opširniju verziju vidi prilog broj 1) je podijeljena u četiri cjeline: prva cjelina se odnosila na aktivnosti, društvene mreže, podatke koji su dostupni o ispitanicima na internetu i oglašivačima koji prikupljaju podatke, druga se odnosila na važnost privatnosti, zaštiti privatnosti i na koje načine ispitanici štite svoju privatnost na internetu, treća se odnosila na pojam masovnog nadziranja, alate koji štite privatnost na internetu i o ulozi knjižnica u zaštiti privatnosti korisnika i borbi protiv masovnog nadziranja, četvrta cjelina se odnosila na aktivnosti koje ispitanici obavljaju na računalu, koliko su vješti i sigurni u obavljanje tih aktivnosti te pitanja o spolu, godini i godini

[114] Usp. Dumičić, Ksenija; Žmuk, Berislav. Karakteristike korisnika interneta u Hrvatskoj i reprezentativnost internetskih anketa. // Zbornik Ekonomskog fakulteta u Zagrebu 7, 2(2009). Str. 117.

studija. Distribucija ankete provedena je preko sustava Merlin što znači da su svi studenti Odjela za informacijske znanosti bili u mogućnosti ispuniti anketu. Ukupan broj studenata na Odjelu je 180 studenata (150 redovnih i 30 izvanrednih).

6.2.2. Tijek istraživanja

Istraživanje je provedeno tijekom lipnja i srpnja 2016. godine. Tijek istraživanja se odvio u dva dijela: prvi dio istraživanja je proveden među ispitanicima od 24. 06. 2016. do 27. 06. 2016. kada je anketu ispunio samo 21 ispitanik. Zbog toga je ponovljen poziv studentima na ispunjavanje ankete, od 06. 07. 2016. do 12. 07. 2016. Tada je anketu ispunilo još 34 ispitanika, što je dovelo do konačnog broja od 55 ispitanika. Kao i svako istraživanje i ovo je imalo svoje probleme tijekom provedbe istraživanja. Planirani namjerni uzorak studenata su bili svi studenti koji trenutno studiraju informacijske znanosti, s ciljem prikupljanja što značajnijih odgovora i mišljenja ispitanika kako bi rezultati istraživanja bili što opširniji i kako bi se dobilo saznanje budućih knjižničara i informacijskih stručnjaka o problemima koji zahvaćaju ne samo knjižnične korisnike, već milijune drugih širom svijeta, pa tako i same ispitanike. Zbog činjenice da je isprva bio mali broj odazvanih ispitanika (21), poziv na ispunjavanje ankete se morao ponoviti te je tada veći broj ispitanika (34) ispunio anketu.

Nakon što se prikupio dovoljan broj ispitanika napravljena je analiza s ciljem donošenja zaključaka na temelju rezultata.

6.3. Rezultati istraživanja

6.3.1. Rezultati ankete

Svi ispitanici iz istraživanja su studenti informacijskih znanosti Sveučilišta u Zadru. Anketa se sastojala od 26 pitanja u kojima su ispitanici izrazili stavove i mišljenja o zaštiti privatnosti na internetu, ulozi knjižnica u zaštiti privatnosti te borbi protiv masovnog nadziranja. Pitanjima se ispitivalo slaganje i mišljenje ispitanika o određenim pitanjima vezanima uz provedeno istraživanje.

Raspodjela prema spolu je prikazana u tablici 1., a raspodjela prema godini studija u tablici 2.

Tablica 1. Spol ispitanika

Spol	Broj ispitanika	Postotak
Muški	4	7,2%
Ženski	44	80%

Iz tablice 1 se vidi da je razlika između spolova velika, anketu je ispunilo više pripadnica ženskog spola, njih 44 (80%), dok je pripadnika muškog spola 4 (7,2%). Ostalih 7 ispitanika (12,8%) se nisu izjasnili u vezi spola. Ovako velika razlika među spolovima se može pripisati i činjenici da na studiju informacijskih znanosti ima više studentica nego studenata.

Tablica 2. Godina studija ispitanika

Godina studija	Broj ispitanika	Postotak
1. godina preddiplomskog studija	3	5,4%
2. godina preddiplomskog studija	5	9%
3. godina preddiplomskog studija	8	14,5%
1. godina diplomskog studija	10	18,1%
2. godina diplomskog studija	22	40%

Iz tablice 2 se vidi da je najveći broj ispitanika s 2. godine diplomskog studija, dok je najmanji broj ispitanika s 1. godine preddiplomskog studija. Da je broj ispitanika s 1. godine preddiplomskog studija bio veći, mogla se napraviti analiza između odgovora studenata 1. god. preddiplomskog studija i studenata s 2. god. diplomskog studija, jer bi se napravila analiza razmišljanja i stavova studenata koji su tek krenuli u svijet knjižnica i knjižnične profesije i izlaganju o informacijama o zaštiti privatnosti, ne samo u knjižnicama već i na internetu i studenata koji već nekoliko godina uče o pojmovima relevantnim za ovo istraživanje. Vjerojatno bi se uočile razlike u mišljenjima i stavovima i pogledu na zaštitu privatnosti na internetu. Nakon 2. god. diplomskog studija, najviše ispitanika je bilo s 1. god. diplomskog studija.

Prosječna dob ispitanika je 26 godina. Najveći broj ispitanika je imao između 20 i 26 godina, njih 35 (64%), a ispitanika između 27 i 51 godine je bilo 13 (24%). 7 ispitanika (12%) nije željelo otkriti koliko imaju godina.

Pitanje koje se odnosilo na aktivnosti koje ispitanici obavljaju na internetu pokazuju da ispitanici najviše koriste internet za aktivnosti vezane uz komunikaciju s drugima (91%), obrazovanje (91%) i pregledavanje društvenih mreža (91%), dok aktivnosti koje najmanje obavljaju dok koriste internet su online kupovina (24%), bankovne transakcije (29%) i igranje igrica (33%). Rezultati nisu iznenađujući jer većina korisnika interneta obavlja upravo ovakve aktivnosti dok su na internetu, studenti nisu drugačiji, u Hrvatskoj se još nedovoljno kupuje preko interneta ili se obavljaju bankovne transakcije kao što je slučaj drugdje u svijetu, što je pokazalo i istraživanje provedeno na Državnom zavodu za statistiku Republike Hrvatske.[115] Kako je prije navedeno u teorijskom dijelu, ovakve aktivnosti su podložne krađi identiteta i zloupotrebi osobnih podataka, kada se pojedinac nađe na meti hakera ili prevaranata.

Kako je bilo i za očekivati, najčešće korištena društvena mreža među ispitanicima je Facebook (87,2%), nakon čega slijedi Instagram (33%), dok su kod opcije rijetko ispitanici odabirali najmanje korištene društvene mreže LinkedIn (65,4%) i Twitter (71%). Nije neobično da je Facebook najčešće korištena mreža među studentima, jer je i u svijetu najviše korištena društvena mreža.

Korelacija između korištenja društvenih mreža i poznavanja postavki privatnosti društvenih mreža iznosi r=0,74 što znači da je to snažna pozitivna korelacija. Drugim riječima, ispitanici poznaju postavke privatnosti onih društvenih mreža koje najviše koriste, dok s druge strane najmanje poznaju postavke onih koje ne koriste toliko često. Najveći postotak poznavanja postavki privatnosti je za Facebook (56%), dok je najmanji postotak poznavanja za Tumblr (36%).

Tablica 3. Dostupnost podataka ispitanika na internetu prema njihovom saznanju

Podaci	Postotak
Puno ime i prezime	85,4%
Fotografije	73%
Datum rođenja	62%
Mjesto stanovanja	60%
E mail adresa	51%

[115] Usp. Primjena informacijskih i komunikacijskih tehnologija (IKT) u kućanstvima i kod pojedinaca u 2014. // Državni zavod za statistiku Republike Hrvatske, 2014. URL: http://www.dzs.hr/Hrv_Eng/publication/2014/02-03-02_01_2014.htm (2016-09-02)

Adresa	11%
Broj telefona	5,4%
Ništa od navedenog	5,4%

Iz tablice 3 se vidi kako su podaci najviše dostupni o ispitanicima na internetu po njihovom saznanju, ime i prezime, fotografije (73%) i datum rođenja (62%), dok su najmanje dostupni adresa (11%), broj telefona (5,4%) te ništa od navedenog (5,4%). Dvoje ispitanika u rubrici ostalo su naveli 'Ne znam' i 'Sve ono što sam objavio'. Navedeni podaci se najviše koriste kao dio profila na društvenim mrežama, posebno Facebooku gdje su pravo ime i prezime nužni, a sve ostalo je na izbor korisniku. Podaci koji su dostupni o ispitanicima na internetu su po njihovom saznanju, dakle što su oni sami svjesno stavili na internet i podijelili s drugima.

Tablica 4. Korelacije između stavova prema povezanosti važnosti privatnosti i odnosa web stranica prema podacima

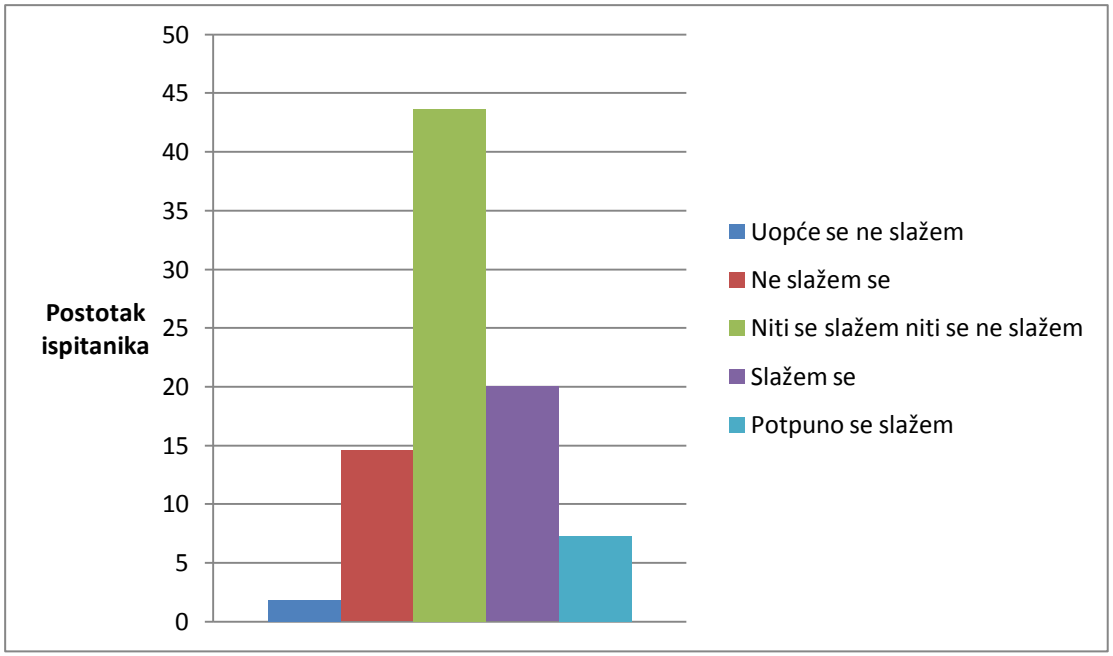
	Je li Vam važna privatnost na internetu
Web stranice prodaju/dijele vaše osobne podatke s drugima?	0,50
Web stranice prate vaše kretanje po njihovoj stranici?	0,43
Web stranice prate vaše kretanje po internetu?	0,49
Web stranice prate vaše online kupovine?	0,07
Web stranice stvaraju vaš profil na temelju pretraživanja?	0,38
Web stranice prilagođavaju oglase na temelju vaših pretraživanja?	0,39

Korelacija stavova iz tablice 4 o tome je li privatnost važna ispitanicima i o odnosu web stranica prema njihovim podacima otkriva da su korelacije u većini slučajeva umjereno pozitivne korelacije. Takva korelacije se odnosi posebno na pitanja o važnosti privatnosti kada web stranice prodaju ili dijele osobne podatke s drugima (r=0,50), kada web stranice prate kretanje po internetu (r=0,49) i kada web stranice prate kretanje po njihovim stranicama (r=0,43). Što znači da je ispitanicima privatnost važna kada web stranice prikupljaju njihove podatke i prate kretanje po njihovim stranicama ili po internetu. Ispitanicima je najmanje

važna privatnost kada je riječ o praćenju web stranica online kupovine, gdje je slaba korelacija (r=0,07). Studenti su odgovorili kako im je privatnost na internetu jako važna (56,3%), dok nitko ne smatra da privatnost na internetu nije važna, upućujući na to da su svjesni koliko je važno imati svaku vrstu privatnosti, uključujući onu na internetu.

Tijekom korištenja interneta ispitanici su odgovorili da su u najvećem postotku odbili koristiti web stranicu koja je tražila njihove osobne podatke (93%), očistili kolačiće (cookies) i povijest pretraživanja na web pregledniku (87,2%), koristili javno računalo u npr. knjižnici za pretraživanje interneta (85,4%) te dali lažne ili nepotpune podatke o sebi (76,3%). S druge strane najmanji postotak ih je koristio web tražilicu koja ne prati povijest pretraživanja, poput DuckDuckGo (71%), usluge za anonimno pregledavanje interneta, poput proxyja, Tora, ili virtualne privatne mreže (62%) i enkripciju za tekstualne poruke, telefonske razgovore ili e-mailove (60%). Rezultati koji upućuju na manji postotak korištenja tražilica i usluga koje štite privatnost korisnika na internetu može ukazivati da studenti ne štite svoju privatnost na internetu na taj način ili nisu upoznati s tim uslugama koje žele zaštititi privatnost na internetu i spriječiti masovno nadziranje. Kako je navedeno u teorijskom dijelu, edukacije i radionice koje obučavaju knjižničare i knjižnične korisnike o problemima zaštite privatnosti na internetu i borbi protiv masovnog nadziranja koriste upravo tražilice poput DuckDuckGo i alate poput Tora kako bi korisnici u knjižnici na siguran način pretraživali internet i zaštitili svoju privatnost u online okruženju.

Što se tiče alata za zaštitu privatnosti na internetu, ispitanici su odgovorima pokazali da ne koriste alate poput Tora, HTTPS Everywhere i DuckDuckGo. Tor koristi samo 1,8% dok ga ne koristi 71% ispitanika; DuckDuckGo također koristi samo 1,8%, a ne koristi ga 64%; najmanje korišteni alat je HTTPS Everywhere kojeg koristi 0% ispitanika, s njim je upoznato njih 13%, dok ga ne koristi 75% ispitanika.



Slika 1. Smatraju li ispitanici da knjižnice imaju veliku ulogu u korisničkoj zaštiti privatnosti na internetu

Iz priloženog grafikona vidi se da su ispitanici neodlučni kada je riječ o ulozi knjižnice u zaštiti privatnosti na internetu. Njih 44% niti se slaže niti se ne slaže s tom tvrdnjom, dok se s tvrdnjom slaže 20% ispitanika, dodatno, njih 15% se ne slaže da knjižnice imaju veliku ulogu u korisničkoj zaštiti. Na pitanje o upoznatosti s činjenicom da su knjižnice bile među prvima u borbi protiv masovnog nadziranja, 38% je odgovorilo da su vrlo malo upoznati s tom činjenicom, dok je da odgovorilo 29% ispitanika. To potvrđuje i korelacija između ova dva pitanja (r=-0,36) što označava umjerenu negativnu korelaciju te pokazuje da ispitanici nemaju mišljenje o ulozi knjižnica u zaštiti privatnosti na internetu i nisu znali da su knjižnice među prvima stale u obranu intelektualne slobode i protiv masovnog nadziranja.

Pitanje o načinu na koji knjižnice mogu zaštititi privatnosti korisnika na internetu bilo je otvorenog tipa, što znači da su ispitanici sami upisivali odgovor na pitanje. Bilo je raznolikih odgovora, većina korisnika je odgovorila da bi knjižnice trebale educirati korisnike, pomoću radionica, letaka, predavanja, programima obrazivanja o zaštiti privatnosti, instaliranjem alata za zaštitu privatnosti, regulacijom zakona i zaštitom korisničkih podataka u knjižnici na njihovim računalima i bazama podataka. No, neki od ispitanika smatraju da u današnje vrijeme nema privatnosti i kako nema načina zaštite privatnosti na internetu dok neki ne znaju dati odgovor na to pitanje.

Tablica 5. Deskriptivna statistika ispitanika

	M	SD
Smatrate li da bi pojedinci trebali biti u mogućnosti koristiti internet u potpunoj anonimnosti?	3,75	0,93
Smatrate li da je Vaša privatnost na internetu dobro zaštićena?	2,34	0,86
Jeste li spremni dati osobne podatke web stranicama koje koristite tako da oglasi budu prilagođeni Vama i Vašim interesima?	2,03	0,81
Je li u redu da oglašivači prikupljaju podatke o Vama?	1,94	1,00

M – aritmetička sredina; SD – standardna devijacija

Deskriptivna statistika iz tablice 5 otkriva da se ispitanici najviše slažu s tvrdnjom da bi pojedinci trebali biti u mogućnosti koristiti internet u potpunoj anonimnosti (M=3,75) odnosno najviše ih je odabralo opciju 'slažem se' (40%). S druge strane iz tablice je vidljivo kako se ne slažu s tvrdnjom da je u redu da oglašivači prikupljaju podatke o njima (M=1,94) odnosno najviše ih je odabralo opciju 'uopće se ne slažem' (40%). No, u tom pitanju je također visok varijabilitet što označava da su ispitanici odgovarali raznoliko i nisu svi imali isto mišljenje te se 1,8% su potpunosti slaže s tvrdnjom da oglašivači mogu prikupljati podatke o njima. Može se zaključiti da iako se većina ne slaže s tim da oglašivači mogu slobodno prikupljati podatke o njima, neki od njih se ne brinu za činjenicu da su njihovi podaci u rukama kompanija koje te podatke mogu koristiti u bilo koje svrhe. Korelacija između spremnosti davanja osobnih podataka web stranicama kako bi oglasi bili prilagođeni ispitanicima i prikupljanju podataka od strane oglašivača je umjereno pozitivna (r=0,52) što

znači da se većina ispitanika ne slaže s tvdnjama i žele svoje podatke zadržati za sebe, a ne dopustiti web stranicama i oglašivačima korištenje istih kako bi prilagodili oglase namjenjene ispitanicima.

Ispitanici su podijeljeni oko pitanja koje se odnosi na pojam masovnog nadziranja, koje provode vlade i agencije poput NSA, a čije dokumente je otkrio Edward Snowden, gdje je 42% ispitanika odgovorilo kako su upoznati s tim pojmom, dok je njih 36,3% odgovorilo kako su vrlo malo upoznati s tim pojmom. Ispitanici se ne slažu s tvrdnjom o masovnom prikupljanju podataka i metapodataka o pojedincima na internetu, njih 36,3%. Korelacija između ove dvije tvrdnje je slaba (r=-0,02), što znači da ispitanici ne vide povezanost između poznavanja pojma masovnog nadziranja i masovnog prikupljanja podataka o pojedincima na internetu, iako su te dvije stvari povezane te zbog masovnog nadziranja koje provode svjetske vlade i obavještajne agencije masovno se prikupljaju osobni podaci na internetu. Zbog toga je potrebna veća zaštita privatnosti na internetu.

Ispitanici su odgovorili da posjeduju stolno i prijenosno računalo (38%) i samo prijenosno računalo (35%), što znači da velika većina ispitanika posjeduje ili samo prijenosno računalo ili obje vrste računala. Aktivnosti koje ispitanici najčešće obavljaju na računalima su korištenje web preglednika i web tražilice, koji svaki dan ili skoro svaki dan koristi 85,4% ispitanika, komuniciranje s drugim osobama preko e-maila, chata, društvenih mreža svakodnevno koristi 82% ispitanika, dok njih 64% čita tekstualne materijale koji nisu dio studentskih obveza, kao što su knjige ili novine. Barem jednom tjedno 42% ispitanika koriste Word ili drugi program za obradu teksta, dok najmanje koriste računalo kako bi napravili HTML ili XML dokument, njih 53% je odgovorilo da nikada ili skoro nikada ne obavljaju tu aktivnost na računalu.

Tablica 6. Procjena razine znanja korištenja računala i interneta

Skala	Postotak
1	0%
2	7,2%
3	31%
4	42%
5	7,2%

Iz tablice 6 vidljivo je da su ispitanici na pitanje o razini znanja korištenja računala i interneta na skali od 1 koja označava početnika do 5 koja označava eksperta, najviše birali razinu 4 (42%), dok nitko od ispitanika nije odabrao razinu 1, što znači da nitko ne smatra da je početnik u korištenju računala i interneta. Nakon razine 4, najviše se birala razina 3 (31%), što označava da su ispitanici relativno sigurni u svoje znanje kada je riječ o korištenju ovih tehnologija. Isti postotak ih je odabrao najvišu razinu 5, odnosno ekspert (7,2%) kao i razinu 2 (7,2%) što znači da su ipak postoje neki koji nisu sigurni u svoja znanja kako su iskazali u ovoj samoprocjeni. Studenti su najsigurniji u vještine obavljanja zadataka kao što su slanje e-maila s privitkom (73%), preuzimanje i spremanje materijala s interneta kao što su PDF dokumenti ili slike (71%), stvaranje tekstualnog dokumenta koristeći Word (67%) kao i pretraživanje potrebnih informacija (56%). Relativno su sigurni u vještine stvaranja HTML ili XML dokumenta i korištenja interneta na siguran način kako bi zaštitili privatnost s istim postotkom (44%). Najnesigurniji su pri korištenju programskih jezika poput Pythona ili Javascripta (36%). Zadnji podatak ne bi trebao biti iznenađujući jer studenti se nisu imali priliku tijekom studija previše susresti s programskim jezicima jer nisu bili dio nastave, osim ako nisu sami bili zainteresirani i učili programske jezike u slobodno vrijeme.

6.4. Rasprava i zaključak istraživanja

Cilj ovog istraživanja bio je istražiti kako i na koji način studenti Informacijskih znanosti u Zadru štite svoju privatnost na internetu te koje je njihovo mišljenje o ulozi knjižnica u zaštiti privatnosti na internetu te borbi protiv masovnog nadziranja.

Prvo istraživačko pitanje odnosilo se na društvene mreže koje ispitanici koriste. Facebook je očekivano prva društvena mreža koju ispitanici koriste i nema ništa iznenađujuće u tome, iznenađujuće može biti činjenica da ispitanici najmanje koriste Twitter, jednu od najpopularnijih društvenih mreža na svijetu s preko 320 milijuna korisnika u 2016. Studentima očito Twitter nije zanimljiv kao društvena mreža jer nudi ograničene mogućnosti kojih Facebook ima u izobilju. Kada se koristi Twitter komunikacija s drugima nije ista kao na Facebooku, a ulogu može igrati i ograničeni broj znakova koji se koriste na Twitteru. No, kada je riječ o zaštiti privatnosti korisnika, upravo je Twitter jedna od društvenih mreža koja štiti privatnosti korisnika i za razliku od Facebooka, nije surađivala s američkom vladom kao dio masovnog nadziranja građana. Facebook je jedna od društvenih mreža s puno propusta u

svojim postavkama privatnosti te zbog toga, kako je navedeno i u teorijskom dijelu, Facebook je jedna od tvrtki koje su dopustile da američka vlada i njene obavještajne agencije koriste osobne podatke i sadržaje koje su korisnici objavili kako bi nadzirali i špijunirali građane ne samo SAD-a već i svijeta. Pomoću programa PRISM ili XKeyscore sve ono što su korisnici objavili na svojim Facebook profilima, javno ili ne, bilo je podložno nadzoru upravo zato što su u Facebooku dali dopuštenje agencijama. Osim što su surađivali s vladom i agencijama, Facebook se našao i pod kritikama jer prodaje osobne podatke i podatke povezane s Facebook računom oglašivačima, koji onda za uzvrat analiziraju korisničke navike i šalju personalizirane oglase svakom pojedinom korisniku.

Upravo je jedno od istraživačkih pitanja bilo o mišljenju ispitanika o prikupljanju podataka od strane oglašivača, gdje su izrazili stav da nije u redu da oglašivači prikupljaju podatke o njima (40%) te se ne slažu s tvrdnjom o prilagođenim oglasima (45%). Time se jasno vidi da ispitanici ne žele da njihovi osobni podaci završe u rukama korporacija koje s tim podacima rade što žele, što je uostalom prikazano i u deskriptivnoj statistici (Tablica 5) gdje su se studenti najmanje složili s tvrdnjom o prikupljanju podataka od strane oglašivača i drugih korporacija. Jedna od tih korporacija je i Facebook, koja od korisnika očekuje da unesu određeni broj osobnih podataka kako bi mogli koristiti tu mrežu. Istraživačko pitanje povezano s tim se odnosi na osobne podatke koji su dostupni o njima na internetu, po njihovom saznanju. Iz analize rezultata (Tablica 3) vidi se da su o ispitanicima najviše dostupni podaci poput imena i prezimena, fotografija, datuma rođenja i mjesta stanovanja. Iako ispitanici misle da njihovo puno ime i prezime na internetu može stajati bezopasno i da nitko neće koristiti u loše svrhe, stvarnost je drugačija. Osim što podatke o pojedincima koji se nalaze na društvenim mrežama ili bilo kojem drugom mjestu na internetu mogu iskoristiti prevaranti, također ih mogu koristiti vlade, korporacije i slične ogranizacije. Preko imena i prezimena može se saznati datum rođenja, broj telefona, mjesto stanovanja i drugi osobni podaci koji se mogu iskoristiti u svrhe na koje pojedinac nije pristao. S fotografija se može saznati gdje je pojedinac bio u određenom trenutku, s kim je bio, koju vrstu pića ili hrane jede ako je na slici takvo što, koju vrstu odjeće nosi i slično. Takozvane treće strane to mogu uzeti i napraviti profil pojedinca, a da on nije niti svjestan toga, slati mu određene oglase koji su povezani s temama sa slika ili vlade u slučaju sumnje na terorizam, gdje preko nekoliko podataka objavljenim na internetu mogu saznati sve o pojedincu kojeg nadziru. Kako bi se zaštitila privatnost na internetu, trebalo bi objaviti što manje osobnih podataka na društvenim mrežama i na internetu, pa čak i one za koje se smatra da su bezazleni. Treba uzeti u obzir da

su navedeni podaci oni kojih su ispitanici svjesni da su na internetu, koje su vjerojatno i sami stavili tamo, no može se postaviti pitanje koliko je osobnih podataka na internetu o ispitanicima, a koji su se tamo našli bez njihovog saznanja.

Jedno od važnih istraživačkih pitanja vezanih uz ovo istraživanje je o važnosti privatnosti na internetu i što ispitanici čine kako bi se zaštitili od narušavanja privatnosti. Ispitanici su pokazali da im je privatnost na internetu važna, njih više od 56% su se izjasnili da im je privatnost na internetu jako važna, dok ih se 35% izjasnilo da im je privatnost važna. Rezultati pokazuju kako su studenti svjesni opasnosti koje prijete privatnosti na internetu te da je ta vrsta privatnosti isto važna kao i svaka druga. Međutim, ispitanici ne koriste ili koriste, ali jako malo, alate koji štite privatnost na internetu, kao što su Tor, DuckDuckGo i HTTPS Everywhere. Tor i DuckDuckGo koristi samo 1,8%, dok HTTPS Everywhere ne koristi nitko. Tor ne koristi 71% ispitanika, DuckDuckGo 64%, a HTTPS Everywhere 75%. Evidentno je iz rezultata da studenti nisu korisnici navedenih alata za zaštitu privatnosti, iako su upoznati s njima. Navedeni alati su izabrani kao dio istraživanja jer se oni najčešće koriste u knjižnicama i kao dio edukacije knjižničara i korisnika, kako je opisano u teorijskom dijelu, gdje projekt za zaštitu korisničke privatnosti na internetu, Library Freedom Project, diljem SAD-a uvodi upravo ove alate u knjižnice kako bi korisnici znali da je njihova privatnost zaštićena kada pretražuju internet u knjižnici. Alati su izabrani jer su najučinkovitiji u zaštiti privatnosti te su njihove postavke privatnosti napravljene tako da se osigurava anonimno pretraživanje i ne spremaju se podaci o pretraživanju koje korisnici obavljaju. Razlog zašto ispitanici ne koriste ove alate nije poznat, no možda smatraju da im je sa i bez njih privatnost ugrožena ili nemaju naviku koristiti druge alate koji nisu standardni, iako bi korištenjem ovakvih i sličnih alata barem malo zaštitili privatnost koja na internetu nestaje svakim danom sve više.

Drugo istraživačko pitanje važno za istraživanje se odnosilo na to je li ispitanici smatraju da su knjižnice važne za zaštitu privatnosti korisnika na internetu te jesu li upoznati s činjenicom da se knjižnice bore protiv masovnog nadziranja. Ispitanici o važnosti knjižnica u zaštiti privatnosti (Slika 1) nisu imali mišljenje, njih 44% je odgovorilo kako se niti slažu niti ne slažu s tim te su zapravo bili podijeljeni oko slaganja, njih 20% smatraju da su knjižnice važne u ulozi zaštite korisničke privatnosti na internetu, a 15% is smatra da knjižnice nemaju veliku ulogu u tome. Rezultati su iznenađujući jer za očekivati bi bilo da su studenti u najvećem postotku odgovorili kako su knjižnice važne i imaju veliku ulogu u zaštiti

korisničke privatnosti, ne samo na internetu i općenito, no to nije bio slučaj. Ispitanici su neodlučni i nemaju zapravo mišljenje o ulozi knjižnice, iako bi knjižnice kao ustanove koje sakupljaju i distribuiraju razna znanja i ustanove koje štite intelektualnu slobodu i pristupu informacijama, kao i zaštitu privatnosti svojih korisnika. Prave razloge zašto studenti smatraju da knjižnice nemaju toliko veliku ulogu u zaštiti privatnosti na internetu bi trebalo dodatno istražiti. Ispitanici su u otvorenom tipu pitanja koji se odnosio na to kako knjižnice mogu zaštititi privatnost na internetu najviše navodili edukacije, radionice i programe kojima bi korisnici stekli nova znanja i vještine potrebne za to. Što se tiče upoznatosti da se knjižnice bore protiv masovnog nadziranja, 38% ih je odgovorilo da su vrlo malo upoznati s tom činjenicom, dok je 29% odgovorilo kako su upoznati, a 11% nisu nikako upoznati s tom činjenicom. To se može povezati sa saznanjem da su ispitanici vrlo malo upoznati s pojmom masovnog nadziranja (36,3%), razlog za to može biti što, iako je masovno nadziranje još uvijek aktualno i velike rasprave se i dalje vode oko toga, nije toliko prisutno u medijima kao što je to bilo 2013. kada je Edward Snowden prvi put novinarima dao dokumente koji su otkrivali u kojoj mjeri su američke agencije nadzirale građane svijeta. Drugi razlog može biti da ih takve teme ne zanimaju previše i ne povezuju masovno nadziranje s knjižnicama.

Hipoteze istraživanja su se pokazale točne te ukazuju da su studenti koji više koriste društvene mreže, koji znaju za pojam masovnog nadziranja, koji su sigurniji u svoje vještine obavljanja pojedinih akivnosti te koji koriste alate za zaštitu privatnosti, više upoznati s problemima zaštite privatnosti na internetu i načinima zaštite privatnosti od onih koji slabije poznaju alate poput Tora i koji ne poznaju u tolikoj mjeri postavke privatnosti na društvenim mrežama. Također, ispitanici nisu prepoznali knjižnice kao institucije koje sudjeluju u zaštiti privatnosti i borbi protiv masovnog nadziranja. To upućuje da bi knjižnice, kao ustanove namjenjene širenju znanja, intelektualne slobode i zaštiti privatnosti, trebale početi s provedbom edukacija i radionica koje bi educirale ne samo korisnike, već i same knjižničare koji bi onda svoja znanja širili dalje te osigurali korisnicima sigurno mjesto u knjižnici gdje mogu biti sigurni da je njihova privatnost na internetu dobro zaštićena i neće biti zloupotrebljena. Isto tako, korisnici mogu iskoristiti novostečeno znanje kako bi se zaštitili i u svom domu, gdje ipak provode više vremena i koriste internet u razne svrhe.

Kao zaključak ovog istraživanja, može se uvidjeti kako su ispitanici svjesni koliko je važna privatnost na internetu te se protive oglašivačima i web stranicama u prikupljanjju njihovih osobnih podataka koje mogu iskoristiti za svrhe koje narušavaju privatnost korisnika, posebno

korisnika društvenih mreža poput Facebooka, kojeg ispitanici i najviše koriste. Mnogi podaci o ispitanicima se nalaze na internetu, kojih su oni svjesni no korištenjem dostupnih podataka koje sami ispitanici objave na internetu, može se doći do ostalih podataka koji su prikupljeni bez dopuštenja i kojih pojedinci nisu ni svjesni da se nalaze na internetu. Međutim, iako su ispitanici svjesni važnosti privatnosti na internetu, iznenađujući rezultati su dobiveni kada je riječ o ulozi knjižnica u zaštiti privatnosti na internetu, gdje je većina bila neodlučna i nisu smatrali da knjižnice imaju veliku ulogu u tome, a određeni dio ispitanika smatra da knjižnice uopće nemaju veliku ulogu u tome. Također, veći postotak ih je vrlo malo upoznato s masovnim nadziranjem, što je uz ulogu knjižnica u zaštiti privatnosti na internetu glavni dio ovoga rada i istraživanja. Rezultate ovog istraživanja bi trebalo dodatno potvrditi ili opovrgnuti ponovnim istraživanjem koje bi sadržavalo više ispitanika i koje bi se provelo na više Odjela informacijskih znanosti diljem Hrvatske. Dakle, kako bi se potvrdili rezultati dobiveni ovim istraživanjem, trebali bi se dodatno istražiti stavovi ispitanika tako što bi se provelo novo istraživanje koje bi obuhvatilo veći broj sudionika i na ostalim Odjelima informacijskih znanosti na hrvatskim sveučilištima.

7. Zaključak

Privatnost je pravo svakog pojedinca, bez obzira na spol, dob, rasu ili socijalni status. Osoba ima pravo na kontrolu informacija koje dijeli s drugima. Ta privatnost uključuje i privatnost na internetu, čija zaštita se razvojem tehnologija sve više dovodi u pitanje. Zbog različitih kršenja privatnosti, bilo od strane tvrtki, oglašivača, vlada ili obavještajnih agencija i drugih, zaštita na internetu je postala jako važna stvar, no čiju potpunu važnost neki još nisu prepoznali kao takvu. Fizička privatnost osobe se još uvijek tretira kao važnija i na koju velika većina obraća pozornost, dok s druge strane o privatnosti na internetu još nije razvijena svijest da je i takva vrsta privatnosti jako važna te ako se krši, može dovesti do velikih posljedica ako su osobni podaci dostupni onima koji ih mogu zloupotrijebiti. Na društvenim mrežama dnevno se objave milijuni informacija o osobama koje ih koriste, od imena i prezimena do fotografija. Ovaj diplomski rad ukazuje na važnost zaštite privatnosti na internetu i uloge knjižnice u tome, kao ustanove koja se bori za javno dobro i intelektualnu slobodu.

Privatnosti na internetu prijeti mnogo opasnosti, od primjerice kolačića (eng. cookies) koji podatke prosljeđuje pregledniku koji ih sprema, a pomoću njih se mogu povezati informacije o korisniku i stvoriti profil koji se može zloupotrijebiti do društvenih mreža koje omogućuju korisniku da napravi profil u kojem se traže osobni podaci, koji mogu biti iskorišteni u razne svrhe, a zbog činjenice da su društvene mreže besplatne i zarađuju preko oglasa, ti podaci često završe u vlasništvu korporacija. Korporacije prikupljaju i prodaju podatke te zarađuju od njihove prodaje, a korisnicima nude besplatne društvene mreže i druge usluge, koje imaju svoju cijenu korištenja. Osim navedenih prijetnji privatnosti na internetu, postoji i ona masovnog nadziranja, koje provode svjetske vlade, posebno američka i britanska, kao i njihove obavještajne agencije. Rad donosi pregled provođenja masovnog nadziranja nad građanima svijeta, koje je u javnost dospjelo nakon što je Edward Snowden 2013. godine objavio dokumente u kojima raskrinkava američku vladu i obavještajnu agenciju NSA kao glavne krivce za masovno nadziranje osoba na internetu i prikupljanju njihovih podataka kao mjere protiv terorizma. Američka vlada uz britansku i njihove agencije, preko programa kao što su PRISM, XKeyscore i Tempora, su prikupljali podatke i metapodatke milijuna ljudi na internetu, preko njihovih društvenih mreža, računalnih sustava, mobilnih kompanija i drugih tehnoloških alata.

Rad se bavi i ulogom knjižnice u zaštiti privatnosti korisnika na internetu te borbi protiv masovnog nadziranja. Knjižnice se smatraju ustanovama koje štite privatnost svojih korisnika i koje promiču intelektualnu slobodu, slobodu govora i pristup informacijama, a sada i zaštitu privatnosti na internetu. No, čak su i knjižnice imale period u kojem se njihova uloga čuvara javnog dobra našla u opasnosti od uplitanja vlada i agencija te su neke knjižnice posustale u provedbi svojih etičkih načela. Takva vremena se odnose posebno na vrijeme ratova kao što su Prvi i Drugi svjetski rat, kada su knjižnice bile izložene cenzuri, razdoblje Hladnog rata, kada se prvi put počelo nadzirati korisnike za koje se sumnjalo da su ili američki ili sovjetski špijuni i kada su knjižnice bile prisiljene odavati osobne podatke korisnika, kada je pokrenut i FBI program za nadziranje. Međutim, većina knjižnica i knjižničara su stali u obranu svojih korisnika i u zaštitu njihove privatnosti, kao i nakon napada 11. rujna kada je u SAD-u donešen Domovinski zakon koji je izravno utjecao na knjižnice. Tada su FBI i druge agencije mogle tražiti od knjižnica osobne podatke korisnika, kao i njihovu internetsku povijest pretraživanja. Knjižničari su se pobunili i poveli borbu protiv masovnog nadziranja pojedinaca, kako u knjižnicama, tako i na internetu. Nakon Snowdenovih otkrića, knjižničari su ponovno bili među prvima koji su stali na stranu zaštite privatnosti i počeli provoditi edukacije koje uče knjižničare i korisnike kako se zaštititi na internetu i koje alate koristiti pri tome.

U radu je provedeno istraživanje čiji je cilj istražiti mišljenja i stavove studenata Informacijskih znanosti u Zadru o privatnosti i načinu zaštite privatnosti na internetu te njihovom mišljenju o ulozi knjižnice u zaštiti. Rezultati istraživanja koje je provedeno pomoću kvantitativne metode ankete pokazuju da su studenti svjesni da je privatnost na internetu važna i da je njima važna kada su u online okruženju te znaju za opasnosti koje prijete na internetu. Također, protive se oglašivačima i prikupljanju podataka koji se koriste u svrhe poput prilagođavanja oglasa. Istraživanje je također pokazalo da alate koji knjižničari koriste u knjižnicama u drugim zemljama kako bi zaštitili privatnost korisnika, kao što su Tor ili DuckDuckGo koristi jako mali broj studenata, dok je više onih koji ih uopće ne koriste. Što se tiče uloge knjižnica u zaštiti privatnosti na internetu, studenti su pokazali da su neodlučni o važnosti knjižnica te je čak veliki broj njih odgovorio kako se ne slažu da knjižnice imaju veliku ulogu u tome, što je možda iznenađujući podatak. Nadalje, vrlo malo su upoznati s činjenicom da se knjižnice bore protiv masovnog nadziranja.

Rezultate koji su dobiveni u ovom istraživanju trebalo bi dodatno potvrditi ili opovrgnuti novim istraživanjem, koje bi dakle uključivalo više ispitanika i više Odjela informacijskih znanosti, kako bi se dodatno istražili stavovi studenata o temi zaštite privatnosti na internetu i borbi protiv masovnog nadziranja. Ovaj rad može poslužiti kao polazišna točka daljnjeg istraživanja o ovoj temi i mogućih knjižničnih edukacija. Takvih edukacija u Hrvatskoj ima u neznatnom broju za razliku od Sjedinjenih Američkih Država gdje su takve edukacije jako česte. Edukacije koje bi se provodile obuhvaćale bi i knjižničare i korisnike, kako bi se ukazalo na probleme koji narušavaju privatnost na internetu te osvjestilo o važnosti zaštite privatnosti na internetu.

8. Literatura

1. ALA news. ALA calls passage of USA FREEDOM Act a milestone. URL: http://www.ala.org/news/press-releases/2015/06/ala-calls-passage-usa-freedom-act-milestone (2016-04-26)
2. Analysis of the USA Patriot Act related to libraries. URL: http://www.ala.org/offices/oif/ifissues/issuesrelatedlinks/usapatriotactanalysis (2016-07-25)
3. Boban, Marija. Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu. // Zbornik radova Pravnog fakulteta u Splitu 49, 3(2013).
4. Buitelaara, J. C. Privacy and Narrativity in the Internet Era. // The Information Society: An International Journal, 30:4.
5. Cannataci, J. A. Report of the special Rapporteur on the right to privacy, 2015.
6. Carpenter, Zöe. Librarians versus the NSA: your local library is on the front lines against government surveillance, 2015. URL: http://www.thenation.com/article/librarians-versus-nsa/ (2016-01-16)
7. Choose Privacy Week. URL: https://chooseprivacyweek.org/ (2016-05-23)
8. Clark, IJ. Surveillance, freedom, Tor and libraries. URL: http://infoism.co.uk/2015/09/surveillance/ (2016-01-14)
9. Clark, IJ. The digital divide in the post-Snowden era. // Journal of Radical Librarianship, 2(2016). URL: http://infoism.co.uk/digitial-divide-snowden.pdf (2016-03-20)
10. Cox, Krista. The day we fight back: NSA reform bills to end mass surveillance and provide greater transparency, 2014. URL: http://www.arl.org/news/arl-news/3123-the-day-we-fight-back-nsa-reform-bills-to-end-mass-surveillance-and-provide-greater-transparency#.Vulz79LhDDd (2016-02-20)
11. Domestic surveillance reform: private data collection and the USA FREEDOM Act. // Congressional Digest, 2015.
12. Dreyfuss, Benjamin; Dreyfuss, Emily. What is the NSA's PRISM program? (FAQ), 2013. URL: http://www.cnet.com/news/what-is-the-nsas-prism-program-faq/ (2016-05-23)
13. DuckDuckGo privacy policy. URL: https://duckduckgo.com/privacy (2016-05-23)

14. Dumičić, Ksenija; Žmuk, Berislav. Karakteristike korisnika interneta u Hrvatskoj i reprezentativnost internetskih anketa. // Zbornik Ekonomskog fakulteta u Zagrebu 7, 2(2009).
15. Eisgrau, Adam. Supporting the USA FREEDOM Act of 2015: ALA's perspective. URL: http://www.districtdispatch.org/2015/05/supporting-the-usa-freedom-act-of-2015-alas-perspective/ (2016-04-26)
16. Glaser, April. Long before Snowden, librarians were anti-surveillance heroes, 2015. URL: http://www.slate.com/blogs/future_tense/2015/06/03/usa_freedom_act_before_snowden_librarians_were_the_anti_surveillance_heroes.html (2016-01-15)
17. Gledec, Gordan; Mikuc, Miljenko; Kos, Mladen. Sigurnost u privatnim komunikacijskim mrežama. // MIPRO 2008 - HEP Informatička i komunikacijska tehnologija (ICT) u vođenju elektroenergetskog sustava / uredio Josip Kljajić. Rijeka: Denona Ltd., Zagreb, 2008. URL: https://www.fer.unizg.hr/_download/repository/Sigurnost_u_privatnim_komunikacijskim_mrezama.pdf (2016-04-08)
18. Greenwald, Glenn. XKeyscore: NSA tool collects nearly everything a user does on the internet, 2013. URL: http://www.tietotori.fi/Keskustelualueet/Muu%20maailma/Yhdysvallat/I00470F08.0/Sinisilm%C3%A4isille%20mietitt%C3%A4v%C3%A4%C3%A4.pdf (2016-05-23)
19. Hogan, Mel; Shepherd, Tamara. Information ownership and materiality in the age of big data surveillance. // Journal of Information Policy, 5(2015).
20. Horvat, Aleksandra. Javno i tajno u knjižničarskoj struci. URL: http://dzs.ffzg.unizg.hr/text/jit_u_%20knjiz.htm (2016-04-10)
21. Hrvatski Sabor. Ustav Republike Hrvatske. URL: http://www.sabor.hr/Default.aspx?art=1841 (2016-04-01)
22. HTTPS Everywhere. URL: https://www.eff.org/https-everywhere/ (2016-05-23)
23. IFLA-ina Izjava o privatnosti u knjižnici. URL: http://www.hkdrustvo.hr/clanovi/alib/datoteke/file/IFLA-ina%20Izjava%20o%20privatnosti.pdf (2016-04-03)
24. IFLA Statement on privacy in the library environment. URL: http://www.ifla.org/publications/node/10056 (2016-05-23)

25. Ingram, Philip. How many CCTV camers are there globally? URL: http://www.securitynewsdesk.com/how-many-cctv-cameras-are-there-globally/ (2016-04-03)
26. Jaeger, Paul T... [et al]. The USA Patriot Act, the Foreign Intelligence Surveillance Act, and Information Policy Research in Libraries: issues, impacts, and questions for libraries and researchers. // The Library Quarterly: information, community, policy 74, 2(2004).
27. Jones, Barbara M. Intelektualna sloboda u teškim vremenima. // Slobodan pristup informacijama: 10. okrugli stol / uredile Alemka Belan-Simić i Aleksandra Horvat. Zagreb: Hrvatsko knjižničarsko društvo, 2011.
28. Landau, Susan. Making sense from Snowden: what's significant in the NSA surveillance revelations. // IEEE, 2013. URL: http://www.cs.siue.edu/~wwhite/IS376/ReadingAssignments/0930_MakingSenseFromSnowden.pdf (2016-05-04)
29. Library Freedom Project. URL: https://libraryfreedomproject.org/ (2016-05-23)
30. Lyon, David. Surveillance, Snowden, and big data: capacities, consequences, critique. // Big Data & Society, 2014.
31. Morrone, Melissa. How your local library can help you resist surveillance state, 2014. URL: http://wagingnonviolence.org/feature/local-library-can-help-resist-surveillance-state/ (2016-01-18)
32. Newell, Bryce Clayton; Randall, David P. Video surveillance in public libraries: a case of unintended consequences? // IEEE, 2012. URL: http://www.computer.org/csdl/proceedings/hicss/2013/4892/00/4892b932.pdf (2016-01-16)
33. NSA slides explain the PRISM data-collection program, 2013. URL: http://cyber-peace.org/wp-content/uploads/2013/06/NSA-slides-explain-the-PRISM-data-collection-program-The-Washington-Post.pdf (2016-05-23)
34. NSA surveillance: how libraries have been on the front line to protect privacy. URL: http://www.theguardian.com/world/2015/jun/05/nsa-surveillance-librarians-privacy (2016-01-10)
35. Primjena informacijskih i komunikacijskih tehnologija (IKT) u kućanstvima i kod pojedinaca u 2014. // Državni zavod za statistiku Republike Hrvatske, 2014. URL: http://www.dzs.hr/Hrv_Eng/publication/2014/02-03-02_01_2014.htm (2016-09-02)

36. Privacy Online: perspectives on privacy and self-disclosure in the social web. Berlin: Springer, 2011.
37. Radical librarianship: how ninja librarians are ensuring patrons' privacy. URL: http://boingboing.net/2014/09/13/radical-librarianship-how-nin.html (2016-01-10)
38. Randall, David P.; Newell, Bryce Clayton. The panoptic librarian: the role of video surveillance in the modern public library. URL: https://www.ideals.illinois.edu/bitstream/handle/2142/47307/132_ready.pdf?sequence=2 (2016-01-13)
39. Reeve, Tom. BSIA attempts to clarify question of how many CCTV cameras are there in the UK, 2013. URL: http://www.securitynewsdesk.com/bsia-attempts-to-clarify-question-of-how-many-cctv-cameras-in-the-uk/ (2016-04-03)
40. Richards, Pamela Spence. Cold war librarianship: Soviet and American library activities in support of National Foreign Policy. // Libraries and Culture 36, 1(2001).
41. Rogers, Robert A. Censorship and libraries in the Soviet Union. // Journal of library history, philosophy, and comparative librarianship 8, 1(1973).
42. Starr, Joan. Libraries and national security: an historical review. // First Monday 9, 12(2004). URL: http://firstmonday.org/ojs/index.php/fm/article/view/1198/1118 (2016-03-17)
43. Strauß, Stefan; Nentwich, Michael. Social networking sites, privacy and the blurring boundary between public and private spaces. // Science and Public Policy 4(2013).
44. Tempora: the world's largest XKeyscore is now available to qualified NSA users, 2012. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHc5f6.dir/doc.pdf (2016-05-23)
45. The Guardian. Edward Snowden and the NSA files – timeline. URL: http://www.immagic.com/eLibrary/ARCHIVES/GENERAL/GMGP_UK/G130623S.pdf (2016-05-03)
46. The library, the surveillance state, and you. URL: https://librarysmcm.wordpress.com/2013/07/29/the-library-the-surveillance-state-and-you/ (2016-01-17)
47. The USA Patriot Act: preserving life and liberty. URL: https://www.justice.gov/archive/ll/highlights.htm (2016-07-25)
48. Tor Overview. URL: https://www.torproject.org/about/overview (2016-05-23)

49. USA Freedom Act. URL: https://judiciary.house.gov/issue/usa-freedom-act/ (2016-07-25)
50. Velika promjena: SOA dobiva pristup gradskim nadzornim kamerama. URL: http://www.telegram.hr/politika-kriminal/velika-promjena-soa-dobiva-pristup-gradskim-nadzornim-kamerama/ (2014-04-03)
51. Zagreb pokriven s četiri tisuće nadzornih kamera. URL: http://www.poslovni.hr/hrvatska/zagreb-pokriven-s-cetiri-tisuce-nadzornih-kamera-299781 (2016-04-03)

9. Abstract

The role of libraries in the protection of privacy on the Internet and the fight against mass surveillance

This thesis deals with the theme of protection of the privacy on the Internet and the role of libraries in it as well as fight against mass surveillance. The work is divided into two parts, the theoritical part which is based on the literature, and the research part. The theoretical part contains the concepts and definitions of privacy and protecting the privacy on the Internet, along with the role of libraries in that protection and the concept of mass surveillance by the governments and intelligence agencies, such as the US National Security Agency (NSA) and its programs for surveilling of millions of people around the world. Also, the theoretical part deals with the library fight against mass surveillance and services that librarians use and educations carried out in order to protect users' privacy on the Internet. The research part of the work deals with the investigation conducted by the survey among students of Information Sciences at the University of Zadar, whose goal was to find out how students protect privacy on the Internet and find out their opinions on the role of libraries in the protection of privacy on the Internet and the fight against mass surveillance. The research wants to alert future librarians about the dangers of violation of privacy on the Internet and mass surveillance that threatens their privacy and privacy of library users. This work is intended as a basis for further research on the topic and the possible implementation of education in libraries as well as pointing out the problems that threaten privacy on the Internet.

Keywords: privacy, Internet, libraries, mass surveillance

10. Prilozi

Prilog br. 1

Anketni upitnik

Ovaj anketni upitnik je dio diplomskog rada i istraživanja o zaštiti privatnosti na internetu, ulozi knjižnica u zaštiti privatnosti te masovnom nadziranju. Anketni upitnik je anoniman, a rezultati će se koristiti isključivo za svrhe rada.

Molimo Vas da iskreno odgovorite na postavljena pitanja.

Ispunjavanje anketnog upitnika traje otprilike 10ak minuta.

Hvala na suradnji!

1. Za koje aktivnosti Vam služi internet? Odaberite sve aktivnosti koje obavljate na internetu.

Skala:
Često | Rijetko | Nikada

Obrazovanje
Čitanje vijesti
Pregledavanje društvenih mreža
Slušanje glazbe
Pregledavanje video materijala
Online kupovina
Bankovne transakcije
Planiranje putovanja
Igranje igrica
Komunikacija s drugima

2. Koje od navedenih društvenih mreža koristite?

Skala:
Često | Rijetko | Nikada

Facebook
Twitter
Tumblr
Instagram
Pinterest
LinkedIn

3. Jeste li upoznati s postavkama privatnosti društvenih mreža koje koristite?

Skala:
Da | Djelomično | Ne | Ne znam

Facebook
Twitter
Tumblr
Instagram
Pinterest
LinkedIn

4. Koji osobni podaci su dostupni o Vama na internetu po Vašem saznanju?

Puno ime i prezime
Datum rođenja
E-mail adresa
Mjesto stanovanja
Fotografije
Adresa
Broj telefona
Ništa od navedenog
Ostalo:

5. Jeste li spremni dati osobne podatke web stranicama koje koristite tako da oglasi budu prilagođeni Vama i Vašim interesima?

Skala:
Uopće se ne slažem | Ne slažem se | Niti se slažem niti se ne slažem | Slažem se | Potpuno se slažem

6. Je li u redu da oglašivači prikupljaju podatke o Vama?

Skala: Uopće se ne slažem | Ne slažem se | Niti se slažem niti se ne slažem | Slažem se | Potpuno se slažem

7. Koliko Vam je važna privatnost kada:

Skala: Jako važna | Važna | Ne znam | Nevažna | Uopće nije važna

Web stranice prodaju/dijele vaše osobne podatke s drugima?
Web stranice prate vaše kretanje po njihovoj stranici?
Web stranice prate vaše kretanje po internetu?
Web stranice prate vaše online kupovine?
Web stranice stvaraju vaš profil na temelju pretraživanja?
Web stranice prilagođavaju oglase na temelju vaših pretraživanja?

8. Je li Vam važna privatnost na internetu?

Skala: Jako važna | Važna | Niti važna niti nevažna | Nevažna | Uopće nije važna

9. Smatrate li da je Vaša privatnost na internetu dobro zaštićena?

Skala: Uopće se ne slažem | Ne slažem se | Niti se slažem niti se ne slažem | Slažem se | Potpuno se slažem

10. Tijekom korištenja interneta, jeste li učinili neku od navedenih stvari?

Skala: Da | Ne | Ne odnosi se na mene | Ne znam

Očistili kolačiće (cookies) i povijest pretraživanja na web pregledniku?

Postavili web preglednik tako da onemogući ili isključi kolačiće?
Koristili privremenu e-mail adresu ili korisničko ime?
U web preglednik stavili dodatak (add-on) za zaštitu privatnosti?
Dali lažne ili nepotpune podatke o sebi?
Koristili uslugu koja Vam omogućava anonimno pregledavanje interneta; poput proxyja, Tora, ili virtualne privatne mreže (VPN)?
Često mijenjali lozinku?
Koristili enkripciju za tekstualne poruke, telefonske razgovore ili e-mailove?
Odbili koristiti web stranicu koja je tražila Vaše osobne podatke?
Koristili javno računalo (npr. u knjižnici) kako bi pretraživali internet?
Koristili web tražilicu koja na prati vašu povijest pretraživanja, poput DuckDuckGo?

11. Smatrate li da bi pojedinci trebali biti u mogućnosti koristiti internet u potpunoj anonimnosti?

Skala: Uopće se ne slažem | Ne slažem se | Niti se slažem niti se ne slažem | Slažem se | Potpuno se slažem

12. Jeste li upoznati s pojmom masovnog nadziranja, koje provode vlade i obavještajne agencije poput Nacionalne sigurnosne agencije (NSA) čije je dokumente otkrio Edward Snowden?

Skala: Da | Vrlo malo | Nimalo | Ne znam

13. Slažete li se s postupkom masovnog prikupljanja podataka (metapodataka) o pojedincima na internetu?

Skala: Uopće se ne slažem | Ne slažem se | Niti se slažem niti se ne slažem | Slažem se | Potpuno se slažem

14. Jeste li upoznati s uslugom za zaštitu privatnosti pod nazivom Tor?

Skala: Upoznat/a | Koristim | Ne koristim

15. Jeste li upoznati s uslugom za zaštitu privatnosti pod nazivom HTTPS Everywhere?

Skala: Upoznat/a | Koristim | Ne koristim

16. Jeste li upoznati s uslugom za zaštitu privatnosti pod nazivom DuckDuckGo?

Skala: Upoznat/a | Koristim | Ne koristim

17. Smatrate li da knjižnice imaju veliku ulogu u korisničkoj zaštiti privatnosti na internetu?

Skala: Uopće se ne slažem | Ne slažem se | Niti se slažem niti se ne slažem | Slažem se | Potpuno se slažem

18. Na koji način bi knjižnice mogle zaštiti privatnost korisnika na internetu?

19. Jeste li upoznati s činjenicom da su knjižnice bile među prvima u borbi protiv masovnog nadziranja?

Skala: Da | Vrlo malo | Nimalo | Ne

20. Posjedujete li računalo kod kuće?

Da, posjedujem stolno računalo
Da, posjedujem prijenosno računalo
Da, posjedujem stolno i prijenosno računalo
Ne posjedujem računalo

21. Koliko često obavljate navedene aktivnosti na računalu?

Skala: Svaki dan ili skoro svaki dan | Barem jednom tjedno | Nekoliko puta mjesečno | Nikada ili skoro nikada

Korištenje Worda ili drugih programa za obradu teksta
Korištenje Excela ili drugih programa za obradu podataka
Korištenje PowerPointa ili drugih programa za izradu prezentacija

Instaliranje softverskih programa na računalo
Stvaranje HTML ili XML dokumenata
Uređivanje fotografija i drugih slikovnih dokumenata
Korištenje web preglednika i web tražilica
Slanje e-mail poruka online, pomoću Outlooka ili drugih e-mail usluga
Pretraživanje relevantnih informacija na pouzdanim izvorima na internetu
Gledanje video materijala koji se odnose na područje koje Vas zanima, a koje nije povezano sa studentskim obvezama (gledanje dokumentaraca, predavanja i dr)
Čitanje tekstualnih materijala koji se odnose na područje koje Vas zanima, a koje nije povezano sa studentskim obvezama (čitanje knjiga, članaka, novina)
Komunikacija s drugima (e-mail, chat, društvene mreže, Skype, forum i dr)
Preuzimanje i spremanje materijala s interneta (PDF, tekstualni dokument, slika i dr)

22. Koliko ste sigurni u Vaše vještine obavljanja sljedećih zadataka?

Skala: Vrlo siguran/na | Relativno siguran/na | Niti siguran/na niti nesiguran/na | Nesiguran/na

Stvaranje tekstualnog dokumenta koristeći Word ili drugi program za obradu teksta
Uređivanje fotografija i drugih slikovnih dokumenata
Stvaranje HTML ili XML dokumenta
Stvaranje baze podataka
Slanje e-maila s privitkom
Instaliranje softverskih programa na računalo
Korištenje programa poput Excela za stvaranje dokumenta koji sadržava tablice ili grafove
Stvaranje multimedijske prezentacije s tekstom, slikama i animacijama
Stvaranje vlastite web stranicu i održavanje web stranice
Korištenje programskih jezika poput Pythona, JavaScripta, C++ i drugih
Preuzimanje i spremanje materijala s interneta (PDF, tekstualni dokument, slika i dr)
Pretraživanje informacija koje su Vam potrebne
Procjenjivanje pouzdanosti informacija koje pronađete na internetu
Procjenjivanje pouzdanih izvora informacija na internetu
Korištenje raznih društvenih mreža i opcija koje se na njima nude
Korištenje interneta na siguran način kako bi zaštitili privatnost
Zaštita od neželjene pošte i prijevara na internetu

23. Na skali od 1 do 5 (gdje je 1 početnik, a 5 ekspert), kako biste procjenili Vašu razinu znanja korištenja računala i interneta?

1
2
3
4
5

24. Koliko imate godina? Molimo navedite samo broj.

25. Kojeg ste spola?

Muškog
Ženskog

26. Koja ste godina studija?

1. godina preddiplomskog studija
2. godina preddiplomskog studija
3. godina preddiplomskog studija
1. godina diplomskog studija
2. godina diplomskog studija