Digitalni otisci i digitalne tetovaže

Kanaet, Vanessa

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2018./ 2019.

Vanessa Kanaet

DIGITALNI OTISCI I DIGITALNE TETOVAŽE

Diplomski rad

Mentor: dr.sc. Kristina Kocijan, izv. prof.

Zagreb 2019.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____

Vanessa Kanaet

Sadržaj

Sažetak

1.

Uvod

Korištenje interneta u svrhu komunikacije uvelo je važne promjene kod većine internet korisnika. Brzo širenje informacijskih i komunikacijskih tehnologija nezaustavljiva je sila koja ulazi u gotovo svaku sferu suvremenog života. Pod najvećim utjecajem svakako su najmlađe generacije koje su sve više ovisne o korištenju interneta, a posebice društvenih mreža. Malo bi bilo reći da su društvene mreže postale sastavni dio života današnjeg društva. Web stranice kao što su Facebook, Twitter, Instagram, Youtube i sl. uvelike utječu na današnji oblik komunikacije među ljudima. Fotografije koje dijelimo, komentari koje pišemo, videozapisi koje *lajkamo*, drugim ljudima govore nešto o nama. Čak i ako ih izbrišemo, oni su i dalje dostupni, i drugi korisnici (ili čak web-lokacije ili aplikacije) ih mogu spremati i dijeliti.

Život mladeži svakodnevno se bilježi online. Bilježe ga oni sami, njihovi prijatelji, pa čak i njihove obitelji, ponekad čak i prije rođenja osobe o kojoj se podatci bilježe. Koje su prevencije i tko bi trebao sudjelovati u procesu zaštite podataka kod najmlađih generacija? Kako utjecati na ono što se objavi na internetu, koje su posljedice izlaganja svojih osobnih podataka i privatnih informacija? Ostaje li sve što objavimo negdje zabilježeno i može li se ono što javno objavimo trajno ukloniti?

Odgovori na ova pitanja vežu se uz pojmove kao što su 'digitalni otisci' i 'digitalne tetovaže'. Kako bi se čitatelja upoznalo s ovim terminima, rad prati sljedeću strukturu. U prvom poglavlju navodi se zaštita podataka na internetu i moguće opasnosti koje prijete prilikom napada na određene podatke. Nadalje se upoznajemo s pojmom društvenih mreža i njihovog utjecaj na digitalni identitet, kao i ostavljanja tragova na društvenim mrežama. Sljedeće poglavlje definira pojam digitalnog identiteta i čimbenike koji čine digitalni identitet. U narednom poglavlju obrađena je tema digitalnog otiska, kako su ti otisci vidljivi i kako se zaštititi prilikom ostavljanja tragova na internetu. Iduće poglavlje govori o „digitalnoj tetovaži“, njenoj trajnosti, posljedicama ostavljanja digitalne tetovaže, što ju sve čini i sl. Posljednje poglavlje ovog rada orijentirano je na djecu predškolske dobi kao najizloženije grupe korisnika interneta, moguće opasnosti izlaganja djece i njihovih podataka online te kako zaštititi djecu i njihove podatke i tko treba sudjelovati u tom procesu. Na kraju rada iznesen je zaključak o posljedicama ostavljanja digitalnih tragova i digitalnih tetovaža te koje sve mjere zaštite na internetu su se dokazale kao najuspješnije.

2.

Zaštita podataka na internetu

Zbog velike rasprostranjenosti i upotrebe interneta, zaštita podataka, odnosno privatnosti i sigurnosti na internetu, od presudne je važnosti za opstanak pojedinih stranica, ali i čitavih kategorija stranica koje se koriste. To se naročito odnosi na stranice ili aplikacije koje nude bankarske usluge, usluge transfera novaca, internetske trgovine, ali i portale koje sadrže osobne podatke kao što su online zdravstveni kartoni, podaci o zaposlenju itd. Također, zaštita podataka najmlađih korisnika interneta problem je o kojem se sve više raspravlja, a više o njemu govorit će se u posljednjem poglavlju.

Zaštita privatnosti jedan je od ključnih problema upotrebe interneta. „Naime, postojeće tehnologije omogućile su da se vrlo jednostavno i gotovo besplatno prikupljaju osobni podaci i nadziru online aktivnosti korisnika, što je plodno tlo za njihovu zloupotrebu“ (Brautović, 2007: 28). Zaštita podataka grana je informacijske sigurnosti koja se odnosi na pravilno rukovanje podacima koji se odnose na pristanak, obavijest, osjetljivost i regulatorne probleme (Buckbee, 2018). Zaštita podataka može se odnositi na privatne i pravne osobe. Sigurnost i privatnost podataka često se koriste kao sinonimi, ali postoje određene razlike.

Sigurnost podataka općenito se može smatrati zaštitom podataka na vašoj mreži od vanjskih napadača i određuje način na koji se podaci prikupljaju, dijele i koriste. Uloga **privatnosti podataka** je osiguravanje ispravnog načina korištenja tih podataka (Buckbee, 2018). Prema Kovačeviću (2010), podaci u okviru informacijskih sustava mogu se javiti u sljedećim oblicima:

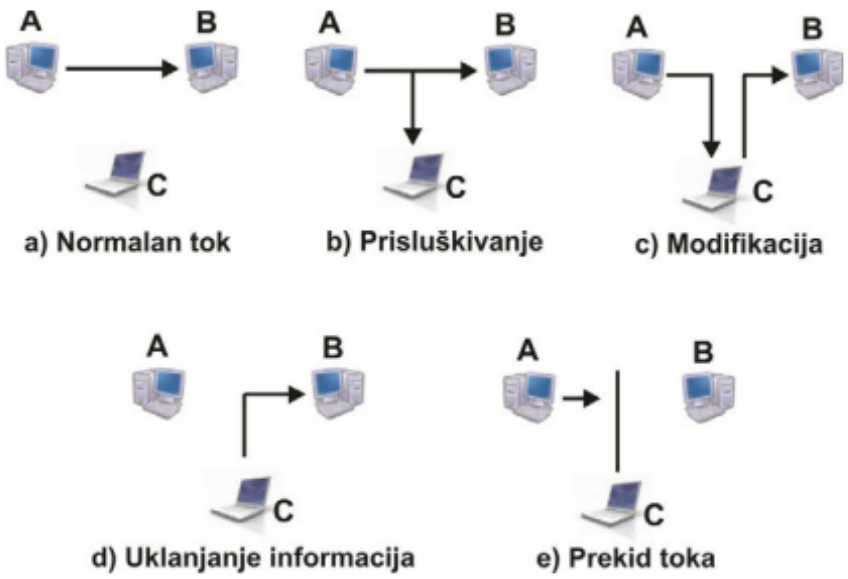
- javni podaci - podaci dostupni javnosti, koji nisu povjerljivi i čiji integritet nije važan, može ih koristiti bilo tko bez ikakvih posljedica (npr. javni servisi za pružanje informacija);
- interni podaci - pristup ovim podacima dozvoljen je samo za određene grupe korisnika, čije javno objavljivanje nije dozvoljeno, ali nije od kritične važnosti (npr. podaci u razvojnim grupama, firmama, radni dokumenti i projekti, interni telefonski imenici itd.);
- povjerljivi podaci - zaštićeni podaci od neovlaštenog pristupa unutar određene grupe (npr. podaci o plaćama, podaci o zaposlenicima, projektna dokumentacija, računovodstveni podaci, povjerljivi ugovori itd.);

- tajni podaci - podaci kod kojih je neautoriziran pristup strogo zabranjen, gdje broj ljudi s ovlaštenim pristupom takvim podacima treba biti ograničen (npr. vojni podaci, podaci o većim financijskim transakcijama, podaci od državnog značaja i sl.).

Kada se govori o zaštiti podataka na mreži, napadači se služe raznim tehnikama kako bi dobili pristup računalnom sustavu. Počinitelji uglavnom prvotno nastoje pribaviti podatke o računalnom sustavu i načinu na koji se on koristi, te je iz tog razloga važno koristiti mehanizme i mjere za zaštitu podataka na mreži. Kovačević (2010) navodi da se mjere za zaštitu podataka zasnivaju se na tri principa:

1. prevencija - odnosi se na poduzimanje preventivnih aktivnosti za zaštitu podataka i računalnih sustava od mogućih napada;
2. detekcija - odnosi se na otkrivanje kako je narušena zaštita računalne mreže, kada je narušena i tko je počinitelj;
3. reakcija - odnosi se na aktivnosti koje dovode do restauracije podataka ili do restauracije računalnog sustava.

Postoje različite vrste napada na podatke**.** Ugrožavanje podataka na računalnim mrežama odnosi se na prisluškivanje, analizu, mijenjanje, uklanjanje informacija kao i lažno predstavljanje (Slika 1). Svi napadi na podatke koji se prenose mrežom mogu se podijeliti na pasivne i aktivne napade.



Slika 1: Grafički prikaz vrsta napada na podatke na računalnoj mreži (Kovačević, 2010: 3).

„Pasivni napadi odnose se na sva prisluškivanja i nadgledanja informacija tijekom prijenosa bez ikakvih promjena podataka, pri čemu napadač na relativno jednostavan način dolazi do informacija“ (Kovačević, 2010: 2). Kao najčešće korišteni mehanizam zaštite od pasivnih napada primjenjuje se kriptiranje podataka koji se prenose putem komunikacijskih linija, tako da se podaci, do kojih se pokušava neovlašteno doći, modificiraju na način da postanu nerazumljivi ili besmisleni za one korisnike kojima nisu namijenjeni.

Aktivni napadi izravno utječu na promjenu sadržaja ili toka informacija. Ova vrsta napada kompliciranija je i teža za otkrivanje od pasivnih napada. Primjeri takvih napada modifikacije su paketa informacija koji se kreću putem mreže, slanje lažnih paketa, prekidi toka informacija kao i razne vrste preusmjeravanja paketa na mreži.

3.

Društvene mreže

Društvene su mreže u današnjem vremenu najposjećenije web lokacije, a njihova se upotreba svakodnevno povećava. Društvenim se mrežama koriste korisnici diljem svijeta, neovisno o kulturi, rasi, spolu ili dobi. Upravo zato, što se korisnike ne ograničava po kulturi, rasi, spolu ili dobi u pojedine i specifične grupe, zanimljivo je proučavati njihovu upotrebu iz više perspektiva. Na primjer, one bi mogle biti psihološke, sociološke ili kulturološke perspektive, no u ovom radu detaljnije će biti razjašnjena njihova upotreba iz informacijske perspektive. Društvene mreže predstavljaju najbolje platforme za stvaranje digitalnih otisaka i tetovaža upravo zbog svoje rasprostranjenosti i popularnosti.

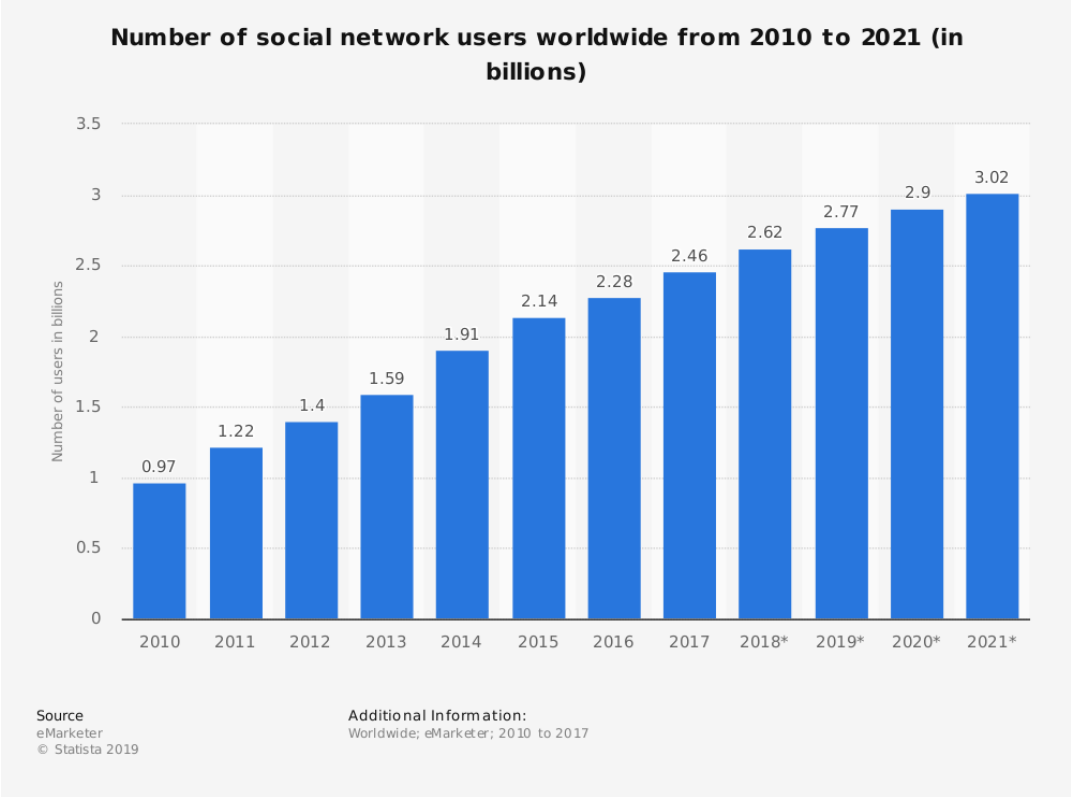
Kao što je već spomenuto, sudjelovanje u društvenim mrežama drastično se povećalo posljednjih godina, zbog sve većeg širenja i dostupnosti uređaja koji omogućuju pristup internetu, kao što su osobna računala, mobilni uređaji i ostale hardverske inovacije poput tableta. Usluge kao što su Facebook, Twitter, LinkedIn, Instagram, Youtube i sl. omogućuju milijunima pojedinaca da stvaraju online profile i dijele osobne podatke s velikim mrežama prijatelja i, često, nepoznatim brojem stranaca. Mnoge su iznimno bogate različitim sadržajem i obično sadrže velike količine podataka o međusobnom povezivanju korisnika i o sadržaju kojeg objavljuju, pritom se ti podaci mogu koristiti za razne analize u kontekstu društvenih mreža. Njihovi servisi stalno se poboljšavaju, dajući korisnicima nove mogućnosti. Pojavljuju se i nove društvene mreže s novim mogućnostima koje, pored prvobitne uloge komunikacije, imaju i ulogu marketinga, promovirajući druge web-stranice i niz različitih usluga.

Društveno umrežavanje jedna je od najpopularnijih online aktivnosti s visokim stopama angažmana korisnika i širenjem mobilnih mogućnosti. Prema stranici Statista[1] (2019d), Sjeverna Amerika zauzima prvo mjesto među regijama u kojima su društveni mediji vrlo popularni, sa stopom penetracije društvenih medija od 66%. U 2016. godini više od 81% stanovništva SAD-a imalo je profil na nekoj od društvenih mreža. Većina društvenih mreža također je dostupna u obliku mobilne aplikacije, dok su neke mreže optimizirane za mobilno pregledavanje interneta, što korisnicima omogućuje vizualno udoban pristup web-lokacijama kao što su Instagram ili Pinterest. Društvene mreže ne samo da korisnicima omogućuju komunikaciju izvan lokalnih ili društvenih granica, nego nude i mogućnost dijeljenja sadržaja

[1] Statista.com objedinjuje statističke podatke o preko 80.000 tema iz više od 22.500 izvora i čini ga dostupnim na četiri platforme: njemačkom, engleskom, francuskom i španjolskom.

koje generiraju korisnici, kao što su fotografije, videozapisi i značajke kao što su društvene igre.

U 2017. godini 71% korisnika interneta bili su korisnici društvenih mreža, a očekuje se da će taj postotak rasti. Prema stranici Statista (2019d), broj korisnika društvenih medija širom svijeta od 2010. do 2019. porastao je s 0,97 milijardi na 2,77 milijardi korisnika, s projekcijama do 2021 godine, kada se procjenjuje da će biti oko 3,02 milijardi korisnika društvenih medija diljem svijeta (Slika 2).



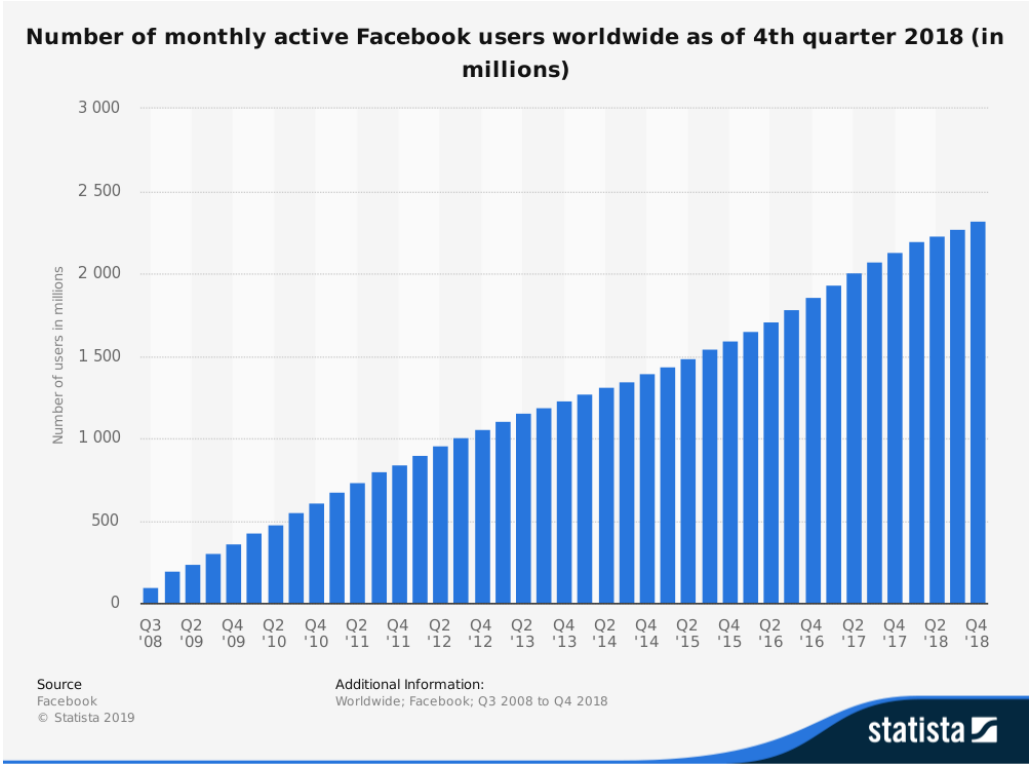
Slika 2: Broj korisnika društvenih mreža od 2010. do 2021. Godine (Statista, 2019d)

Prva društvena mreža koja je doživjela ogroman komercijalan uspjeh bila je MySpace. Pokrenuta je 2003. godine, a izdvajalo ju je to što, uz privatne profile korisnika, omogućuje i umjetnicima da stvore vlastiti profil te preko njega svoja djela učine dostupnima velikom krugu korisnika interneta, pa su time mnoge poznate ličnosti poput glazbenika, modela, glumaca i drugih profesija ubrzo postali korisnici ove mreže. Godinu kasnije, pojavljuje se današnja najpopularnija društvena mreža – Facebook.

Facebook, Inc. američka je tvrtka za online društvene mreže sa sjedištem u Menlo Parku u Kaliforniji. Facebook je nastao kao projekt tadašnjeg hardvarskog studenta Marka Zuckerberga, zajedno s kolegama Eduardom Saverinom, Andrewom McCollumom, Dustinom

Moskovitzom i Chrisom Hughesom, zamišljen i dizajniran kao sredstvo za povezivanje sa svojim fakultetskim kolegama. Ubrzo su Facebook prihvatili i studenti ostalih fakulteta, a nedugo se zatim raširio i po cijelom SAD-u te svijetu. Prije korištenja Facebook stranice, korisnici se moraju registrirati, nakon čega mogu stvoriti osobni profil, dodati druge korisnike kao prijatelje i razmijenjivati poruke, uključujući automatske obavijesti kada ažuriraju svoj profil. Osim toga, korisnici se mogu pridružiti grupama korisnika zajedničkog interesa, organiziranim po mjestu rada, školi ili fakultetu ili drugim značajkama, te kategorizirati svoje prijatelje na popise kao što su "Ljudi s posla" ili "Bliski prijatelji".

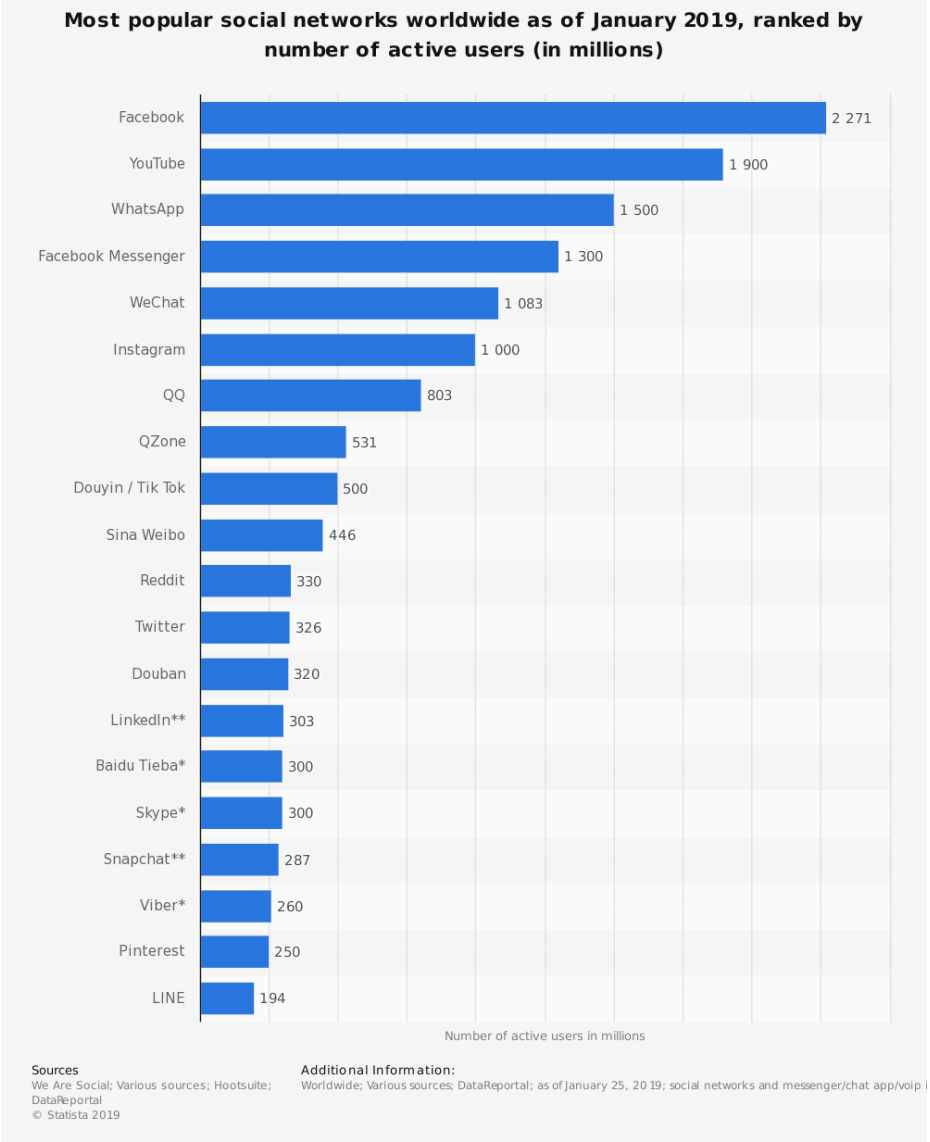
Prema stranici Statista (2019b) u trećem tromjesečju 2012. broj aktivnih korisnika Facebooka premašio je milijardu, što ga čini prvom društvenom mrežom ikada koja je prestigla milijardu korisnika, a od četvrtog kvartala 2018. godine Facebook je imao 2,32 milijarde aktivnih korisnika mjesečno. Aktivni korisnici oni su koji su se prijavili na Facebook tijekom posljednjih 30 dana. U posljednjem tromjesečju, tvrtka je izjavila da 2,7 milijardi ljudi koristi barem jedan od temeljnih proizvoda tvrtke (Facebook, WhatsApp, Instagram ili Messenger) svaki mjesec (Slika 3).



Slika 3: svjetski broj aktivnih korisnika Facebooka od 2008. do 2018. Godine (Statista, 2019b)

Vodeće društvene mreže obično su dostupne na više jezika i omogućuju korisnicima povezivanje s prijateljima ili ljudima preko geografskih, političkih ili ekonomskih granica.

Približno dvije milijarde korisnika interneta koristi se društvenim mrežama, a očekuje se da će te brojke i dalje rasti, budući da korištenje mobilnih uređaja i mobilne društvene mreže sve više dobivaju na snazi (Statista, 2019a). Najpopularnije društvene mreže obično prikazuju veliki broj korisničkih računa ili snažno angažiranje korisnika. Na primjer, tržišni lider Facebook bio je prva društvena mreža koja je nadmašila milijardu aktivnih korisnika mjesečno, dok je noviji Pinterest bio najbrža samostalna web stranica koja je dostigla 10 milijuna jedinstvenih mjesečnih posjetitelja.

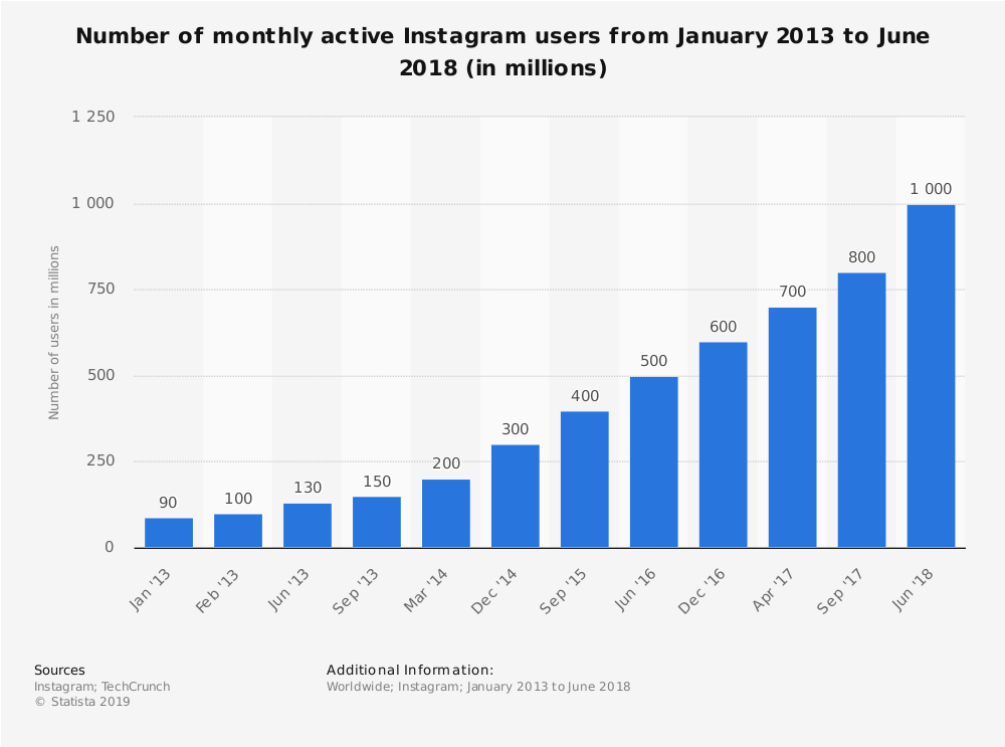


Slika 4: Globalno najpopularnije društvene mreže, od siječnja 2019. godine, po broju aktivnih korisnika (Statista, 2019a)

Korištenje društvenim mrežama vrlo je raznoliko: platforme kao što su Facebook ili Google+ vrlo su usredotočene na razmjene između prijatelja i obitelji te neprestano potiču

interakciju kroz značajke poput dijeljenja fotografija ili statusa i društvenih igara. Druge društvene mreže kao što su Tumblr ili Twitter bazirane su na principu brze komunikacije i prikladno se nazivaju mikroblogovi. Neke društvene mreže fokusiraju se na zajednicu; drugi ističu i prikazuju korisnički generirani sadržaj. Prema stranici Statista (2019a), neke od najpopularnijih mreža širom svijeta od siječnja 2019. godine, rangiranih prema broju aktivnih računa su: Facebook, Youtube, Whatsapp, Facebook Messanger, WeChat, Instagram itd. (Slika 4).

Možemo se osvrnuti na još jednu rastuću društvenu mrežu koju posjeduje Facebook.Inc. Instagram je mobilna društvena mreža koja korisnicima omogućuje uređivanje i dijeljenje fotografija, kao i videozapisa. U 2015. godini imala je više od 77,6 milijuna aktivnih korisnika u SAD-u. Ta će brojka premašiti više od 111 milijuna korisnika u 2019. godini. Globalno gledano, 41% korisnika ima 24 godine ili manje (Statista, 2019c). Instagram je omiljena društvena mreža tinejdžera u SAD-u, premašujući time Twitter i Facebook. Zahvaljujući vizualnoj prirodi aplikacije i visokoj stopi angažmana korisnika, Instagram je također vrijedan marketinški alat za društvene medije, gdje je primjerice od ožujka 2016. godine 98% modnih marki imalo Instagram profil. Prema stranici Statista (2019c), broj aktivnih mjesečnih korisnika Instagrama porastao je s 90 milijuna od 2013. godine, do preko milijardu korisnika od lipnja 2018 godine (Slika 5).



Slika 5: Broj aktivnih mjesečnih korisnika Instagrama, od 2013.-2018. Godine (Statista, 2019c)

3.1. Utjecaj društvenih mreža na digitalni identitet

Prema McPeaku (2013: 103), „društveni mediji višestrani su i interaktivni online alati koji omogućuju korisnicima međusobno povezivanje dok istovremeno obavljaju brojne funkcije na internetu. Na društvenim mrežama i ostalim internetskim stranicama prikupljaju se i pohranjuju velike količine osobnih podataka, bilo da su te informacije objavljene s namjerom dijeljenja ili su ih izradile same web-lokacije društvenih medija.“ Informacije koje korisnici dijele često se dotiču svih aspekata njihovog osobnog života. Društvene mreže prvenstveno služe za priopćavanje informacija drugim korisnicima, a isto tako većina društvenih mreža nudi i različite stupnjeve postavki privatnosti koje korisnicima omogućuju postavke ograničenja o tome tko vidi njihove osobne podatke. „Ove postavke privatnosti, međutim, mogu biti nepouzdane, a nedostaci u privatnosti ili tehničkim smetnjama mogu potkopati sposobnost korisnika da kontrolira publiku za svoj sadržaj“ (McPeak, 2013: 106).

McPeak (2013) nadalje opisuje web-mjesta društvenih medija kao višestruke platforme koje potiču korisnike da obavljaju druge funkcije preko interneta putem web-mjesta društvenih mreža ili putem aplikacija trećih strana koje su integrirane sa stranicama društvenih mreža. Rezultat toga je da web-lokacije društvenih mreža sadrže slojeve podataka koje je generirala web stranice ili ih je izradio korisnik. Drugim riječima, korisnikove aktivnosti na društvenoj mreži se arhiviraju, bilo da se radi o podijeljenom sadržaju od strane korisnika ili o drugim transakcijskim podacima na temelju svega što korisnik radi putem stranica.

3.2. Ostavljanje tragova na društvenim mrežama

Uz rastuću popularnost i korištenje online usluga društvenih medija, ljudi sada imaju račune (ponekad i nekoliko njih) na više različitih usluga kao što su Facebook, LinkedIn, Instagram, Twitter, YouTube itd. Javno dostupne informacije mogu se koristiti za stvaranje digitalnog otiska svakog korisnika koji ih koristi. Generiranje takvih digitalnih otisaka može biti vrlo korisno za personalizaciju, upravljanje profilom, otkrivanje zlonamjernog ponašanja korisnika. Primjerice, možete prenijeti slike na Facebook i Twitter. Kad kliknete sliku, ona bilježi metapodatke koji uključuju vaš zemljopisni položaj u smislu zemljopisne širine i dužine. Dok Facebook i Twitter imaju značajku za uklanjanje svih metapodataka povezanih sa slikama, oni to čine samo kada koristite njihovo web sučelje. Većina nas ima tendenciju da

koristimo mobitel i ažuriramo svoj status na društvenim mrežama putem mobitela. Facebook i Twitter s druge strane, najčešće neuspješno uklanjaju metapodatke dok se bave aplikacijama trećih strana za prijenos i dijeljenje fotografija.

4.

Digitalni identitet

Mnogi od nas imaju paralelni život u stvarnom i digitalnom svijetu. U stvarnom životu, svatko od nas ima identitet. Slično tome, postoji i identitet koji imamo u digitalnom svijetu. Identitet je jedinstveni podatak povezan s entitetom. Sam identitet je jednostavno skup obilježja koja su ili inherentna ili su dodijeljena. Trenutno ne postoji generički sustav za identifikaciju u kibernetskom prostoru. Nije moguće apsolutno identificirati entitet ili točno odrediti ima li objekt određenu karakteristiku. Digitalna okruženja imaju inherentne razlike od stvarnog prostora što uzrokuje tu razliku, a pri implementaciji sustava identiteta za kibernetički prostor treba uzeti u obzir više od arhitektonske prirode sustava - svaki odabrani sustav će imati društvene posljedice koje također treba uzeti u obzir (Covell et al., 1998).

Osobni podaci nisu jedini podaci koji oblikuju digitalni identitet. Digitalni identitet je također oblikovan našim online ponašanjem, kao što su slanje poruka, pisanje blogova, korištenje društvenih medija, e-trgovina itd. Te aktivnosti zahtijevaju račun elektroničke pošte, koji služi kao identifikator za svakog korisnika kada uđe u digitalni svijet. Mnoge web-lokacije i tražilice čuvaju informacije svojih korisnika, kao i njihovo ponašanje na internetu, jer su one visoko cijenjeni artikli u današnjoj digitalnoj ekonomiji (Covell et al., 1998). Elektroničko poslovanje koje se temelji na pružanju usluga, u prvi plan stavlja digitalni identitet korisnika usluga te cjelokupni proces upravljanja digitalnim identitetima. Takve su informacije vrijedne mnogim korporacijama koje ih prikupljaju te arhiviraju. Prikupljene i analizirane, arhive se koriste za stvaranje potpunog korisničkog profila u svrhe digitalnog marketinga.

Mnoge današnje web stranice društvenih mreža zahtijevaju da se na njih registrirate i pritom ostavljate svoje osobne podatke, s vremenom često zaboravite na njih, a one vas na to podsjete u, za vas često, nezgodnom trenutku. Upravo zbog toga poželjno je voditi evidenciju svih registracija koje svakodnevno obavljate. Zapišite podatke poput URL-a, korisničkog imena i lozinke, *e-mail* adrese korištene za registraciju, datuma i sata registracije. Na taj način uvijek ste u tijeku s vašim digitalnim tragovima i možete kvalitetnije upravljati vašim digitalnim identitetom. Poželjno je da svaki korisnik nakon nekog vremena provjeri stranice na koje se registrirao i, ako više ne želi biti korisnik određenih stranica, da ukloni vlastite profile. Većina web stranica društvenih mreža ima opciju uklanjanja ili deaktiviranja profila, a ako na nekoj web stranici ne postoji mogućnost samostalnog uklanjanja profila, dovoljno je kontaktirati korisničku podršku i zatražiti uklanjanje profila.

„Pojam digitalnog identiteta može se promatrati iz različitih perspektiva. Jedna od perspektiva jest perspektiva dobavljača programskih proizvoda koji služe za upravljanje identitetima, druga je perspektiva organizacija koje žele implementirati takva rješenja, a treća je perspektiva korisnika odnosno osobe čiji je digitalni identitet predmet upravljanja“ (CARNet, 2005: 4). Prilikom korištenja rješenja za upravljanjem identitetima stvaraju se brojne prijetnje, a jedna od najčešćih je krađa identiteta odnosno neovlašteno preuzimanje digitalnog identiteta. Prema CARNetu (2005), glavna zadaća upravljanja identitetima jest da se pravi identitet koristi u pravom kontekstu u pravo vrijeme.

U sljedećem pod-poglavlju pobliže će se razjasniti čimbenici upravljanja digitalnim identitetom koji su važni u procesima zaštite podataka radi sigurnosti i privatnosti. Jedan od najvećih rizika korištenja interneta jest krađa podataka, odnosno identiteta, pa tako slijedi pod-poglavlje o najčešćim vrstama krađe podataka u virtualnom svijetu.

4.1. Važni čimbenici upravljanja digitalnim identitetima

CARNet (2005) navodi da je za razumijevanje koncepta upravljanja digitalnim identitetima potrebno prije svega definirati neke osnovne pojmove:

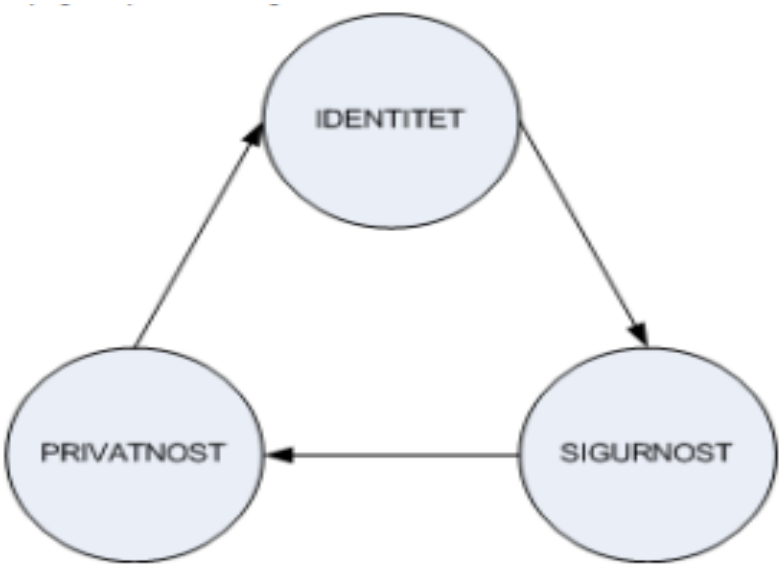
- subjekt, entitet (engl. *subject, entity*)
- resurs (engl. *resource*)
- identitet (engl. *identity*)
- atribut (engl. *attribut*)
- sklonost (engl. *preference*)
- značajka (engl. *trait*)
- identifikacijski podaci (engl. *credentials*)
- sigurnosni autoritet (engl. *security authority*)
- upravljanje digitalnim identitetom (engl. *identity management*).

Osoba, zajednica ljudi, organizacija, programski alat ili bilo koji drugi entitet koji zahtjeva pristup nekom određenom izvoru može biti **subjekt**, odnosno entitet. Web stranice, dio podataka u bazi podataka, transakcija kreditnom karticom, i sl., mogu biti neki **izvor**, odnosno resurs. Da bi dobio pristup resursu, subjekt polaže pravo na **identitet**. U ovom kontekstu, identiteti su zbirke podataka koji predstavljaju **atribute**, **sklonosti** i **značajke**.

„Identitet jest skupina podataka koji prezentiraju atribute, sklonosti i značajke subjekta. Jednom riječju, identitetom se smatra skup informacija koji je poznat o određenom entitetu“ (CARNet, 2005). Atributi su karakteristike povezane s entitetom subjekta, a smatraju se informacijama, kao što su godine, zdravstveni podaci, podaci o navikama naručivanja putem interneta, kreditna sposobnost, itd. Osobine su značajke subjekta koje su mu svojstvene.

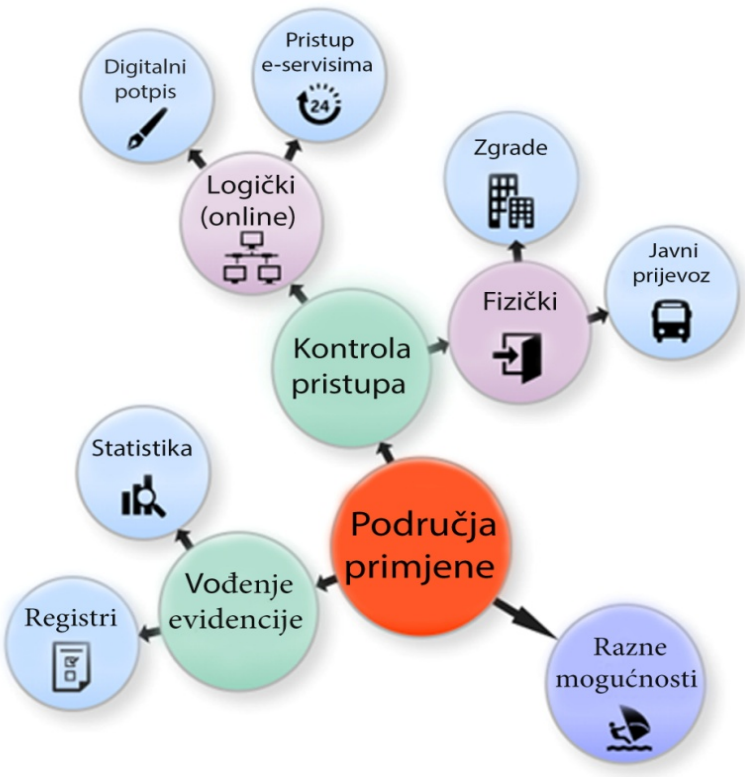
Da bi subjekt koristio identitet kako bi opravdao pristup resursu, mora se predstaviti **identifikacijskim podacima**. Identifikacijski podaci predstavljaju dokaz da određeni subjekt odgovara identitetu za koji se izdaje. Identifikacijski podaci se prezentiraju **sigurnosnom autoritetu** koji ih mora autentificirati. „Autentifikacija se može izvesti uporabom korisničkog imena i zaporke, pomoću X.509 certifikata ili biometrije“ (CARNet, 2005: 4). Potrebna razina autentičnosti obično je proporcionalna riziku koji se pojavljuje prilikom pristupa resursu. Ovisno o tome koji je potencijalni rizik za određeni resurs te vrijednost resursa, uvode se različite tehnike autentifikacije. Kada se potvrdi autentičnost uvjerenja, sigurnosni autoritet uspostavlja sigurnosnu politiku za resurs. Sigurnosna politika služi za dokazivanje da odgovarajući identitet ima određena prava i dozvole nad odgovarajućim resursom.

Digitalni identitet često se veže uz pojam sigurnosti. Iako je digitalni identitet važan dio sigurnosti, ima važniju ulogu od same zaštite informacija. Istovremeno sigurnost informacija podrazumijeva više od same autorizacije i autentifikacije, bavi se i zaštitom integriteta, tajnosti i povjerljivosti informacija. Privatnost zaštićuje atribute, preference i tragove vezane uz identitet (Slika 6).



Slika 6: Odnos identiteta, sigurnosti i privatnosti (CARNet, 2005)

Upravljanje digitalnim identitetima definira se kao proces kojim se postojeće tehnologije koriste za upravljanje informacijama o digitalnom identitetu entiteta te za kontrolu pristupa resursima. „Cilj upravljanja digitalnim identitetima jest poboljšanje produktivnosti i sigurnosti uz smanjenje troškova povezanih s upravljanjem entitetima i njihovim digitalnim identitetima“ (CARNet, 2005: 4). Sustav upravljanja digitalnim identitetom treba biti opće prihvaćen, kompatibilan i imati siguran način za identifikaciju pojedinaca na internetu. Sustavi za upravljanje digitalnim identitetom povezuju pojedince s njihovim internetskim identitetima. Takvi sustavi sastoje se od izdavanja i održavanja tokena (npr. identifikacijskih kartica) i certifikata s odgovarajućim informacijskim sustavima, te pružanja infrastrukture koja omogućuje provjeru mrežnih transakcija. Razumljiv sustav upravljanja digitalnim identitetom omogućuje vladi, građanima i tvrtkama pristup potpuno novom sloju pogodnosti (Slika 7).



Slika 7: Mogućnosti sustava za upravljanje digitalnim identitetom (prilagođeno iz Walter, 2019)

Raul Walter (2019), navodi neke pogodnosti koje nudi razumljiv sustav za upravljanje digitalnim identitetom:

- online provjera autentičnosti, za siguran i jednostavan pristup e-uslugama,
- digitalni potpis, izgrađen oko snažne enkripcije, pravno jednakovrijedno rukopisnom potpisu,
- fizički pristup javnom prijevozu, događajima ili određenim područjima ili zgradama.,
- vođenje evidencije (digitalne transakcije ostavljaju tragove koji se mogu upotrijebiti za poboljšanje odgovornosti i transparentnosti vlade i privatnog sektora te olakšavanje donošenja odluka).

Za bolje razumijevanje upravljanja digitalnim identitetima važno je spomenuti i razjasniti pojmove **identifikacije** i **autentifikacije**. Pojam identifikacije označava povezivanje entiteta sa stvarnom osobom, tvrtkom ili organizacijom, dok bi se autentifikacija mogla razumjeti kao metoda povezivanja fizičkog entiteta s digitalnim.

4.1.1. Identifikacija

Dok sve više i više tvrtki prodaje svoje proizvode i usluge putem interneta, od njih se sve više traži da definitivno procijene jesu li njihovi online kupci oni za koje kažu da jesu. To je osobito problem u procesima u kojima se razmjenjuje novac, vlasništvo ili osjetljive informacije, kao što su bankarske i financijske usluge, ali isto tako i za ostale segmente industrije, uključujući ekonomiju dijeljenja, putničke i ugostiteljske usluge, online igre i sl.

Jednako kao u stvarnom svijetu, dobro je koristiti i različite digitalne identitete u različitim slučajevima. „Identifikacija je povezivanje osobnog identifikatora s pojedinačnim prikazom atributa, npr., "Vi ste Ivan Horvat." Tako su se u Hrvatskoj nekada osobe identificirale po JMBG-u (jedinstveni matični broj građana). Ukoliko bi netko saznao JMBG određene osobe mogao bi iz njega očitati, datum i mjesto rođenja te spol vlasnika JMBG-a. Kako bi se takvi osobni podaci zaštitili, prije nekoliko godina uveden je novi identifikacijski broj koji se naziva OIB (Osobni Identifikacijski Broj) a koji se dodjeljuje računalom bez odavanja osobnih podataka o korisniku, kao što su datum i godina rođenja, spol ili mjesto rođenja.

Kao jedan od načina identifikacije možemo spomenuti JMBAG (jedinstveni matični broj akademskog građana) koji jedinstveno određuje svaku osobu akademske zajednice. Za razliku od JMBG-a, JMBAG se dodjeljuje upisom u neku visokoobrazovnu ustanovu. Sastoji se od 10 znamenki, gdje prve 4 znamenke određuju visoko učilište koje je dodijelilo taj JMBAG,

dok se zadnjih 6 znamenki dodjeljuju slijedno i određuju akademsku osobu unutar visokog učilišta. Osoba zadržava nepromijenjen svoj JMBAG do kraja života, čak i prilikom upisa na drugu visokoobrazovnu ustanovu ili ako je upisana na više ustanova istovremeno (MojFaks.com, 2019).

Prema Campu (2004), osim po identifikacijskom broju, osobe se mogu identificirati prema fizičkom, mentalnom, psihološkom, gospodarskom, kulturnom ili socijalnom identitetu. Primjeri uključuju prihvaćanje povezanosti između fizičke osobe i zaštićenog imena; utvrđivanje povezanosti između tvrtke i financijske evidencije; ili povezivanje pacijenta s fizičkim zapisom atributa. Jednostavnije rečeno, pretpostavimo da neki korisnik ima otvoren račun elektroničke pošte na Google servisu, prilikom kojeg se identificira pomoću adrese elektroničke pošte. Identifikacija zahtijeva identifikator (npr., VIN, broj putovnice i sl.). Medenjak (2008), navodi kako jedan korisnik istovremeno može imati više digitalnih identiteta kod različitih komercijalnih organizacija kao što su Amazon ili eBay zajedno s identitetom za Web stranice popularnog Facebook-a. Svaki od tih identiteta identificiran je korisničkim imenom koje korisnik sam odabire. Isto tako korisnici mogu imati digitalni identitet kao zaposlenici tvrtke u kojoj rade i kojeg koriste samo unutar tvrtke.

4.1.2. Autentifikacija

Zahtjevi za provjeru autentičnosti računalnih sustava i mrežni protokoli razlikuju se prema njihovoj namjeni, dostupnosti i mrežnim vezama. Postoji širok spektar tehnologija autentifikacije i razni prijedlozi protokola o tome koje vrste autentifikacije mogu biti prikladne za neke vrste protokola i aplikacije koje se koriste na internetu. Provjera autentičnosti je dokaz atributa, dok ovjera identiteta dokazuje povezanost između entiteta i identifikatora.

Autentifikacija može biti ostvarena na mnogo načina. Prilikom projektiranja određenog sigurnog sustava svakako najvažniju ulogu ima odabir odgovarajuće vrste autentifikacije za određeno okruženje. Prema Medenjaku (2008) autentifikacija se može odvijati pomoću jedne od metoda, kao što su lozinke, jednokratne lozinke, kriptografije javnog ključa, dokazi „bez znanja“, digitalni potpis itd.

4.2. Krađa identiteta

Prema CARNetu (2005), krađa identiteta sve je učestaliji zločin. Uobičajeni scenariji kojima se zlonamjernici služe su:

- kopanje po smeću (engl. *dumpster diving*),
- krađa poruka elektroničke pošte (engl. *mail theft*),
- krađa osobnih stvari (engl. *personal property theft*),
- unutarnji izvori (engl. *inside sources*),
- varalice (engl. *impostors*),
- online aktivnosti (engl. *online activities*).

Krađa identiteta podrazumijeva krađu osobnih podataka te njihovo korištenje za manipuliranje računima žrtava. Krađa identiteta obično uključuje financije žrtve i može uništiti njihovu kreditnu sposobnost i ugled. Prema CARNetu (2005), dokumenti koji sadrže informacije koje mogu poslužiti kradljivcima su računi kreditnih kartica, telefona, struje, itd., omotnice pristigle pošte pa i dokumenti o članstvu koji sadrže osobne podatke. Prilikom odlaganja ovakve vrste informacija treba izričito voditi računa o tome da su, prije odlaganja u smeće, takvi dokumenti pravilno uništeni.

Kada pošaljete bilo kakve informacije na internetu, morate biti svjesni načina na koje se može dogoditi krađa identiteta. Lopovi identiteta mogu postaviti lažne javne račune u tuđe ime, dobiti pristup tuđim zaporkama i računima e-pošte, kupovati usluge ili stavke, prijaviti se i koristiti bankovne račune i kreditne kartice na tuđe ime, koristiti vladine usluge kao što su putovnice i medicinska skrb na tuđe ime i sl. „Pretraživanje poštanskih sandučića i krađa poruka elektroničke pošte je scenarij u kojem kradljivci dolaze do informacija prije samog korisnika. Bilo kakva poruka elektroničke pošte koja sadrži podatke o financijskim transakcijama, poreznim obrascima ili sličnim informacijama koje se mogu iskoristiti i omogućuju krađu identiteta zanimljiva je ovoj vrsti ljudi“ (CARNet, 2005: 10).

Rastući trend u krađi identiteta jest posredovanje informacijama od strane unutarnjih izvora informacija. Primjerice, nezadovoljan ili nelojalan zaposlenik u nekoj tvrtki koji ima pristup osobnim informacijama, može prodati informacije onima kojima su te informacije potencijalno zanimljive ili korisne. Varanje je još jedan uobičajeni oblik krađe identiteta gdje se koriste bilo kakve prijevare kako bi se od žrtve izvukle osobne informacije. To se može ostvariti tako da korisnici unosom osobnih podataka putem formi na web stranicama te

ostalim transakcijama koje obavljaju online, ostavljaju prostora za mogućnost krađe identiteta.

5.

Digitalni otisci

Digitalni otisci su podaci koji nastaju kao nusprodukt interakcija koje činimo kao dio svakodnevnog života. Digitalni otisak je znak koji ostavljate kada upotrebljavate internet i koji mogu oblikovati vašu online reputaciju. Vaši digitalni otisci sastoje se od sadržaja koji stvorite, postavite i dijelite, kao i sadržaj koji drugi objavljuju i podijele, s vama i o vama (Treyvaud, 2018).

Digitalni tragovi[2] koje ostavljamo iza sebe, bilo na internetu, društvenim mrežama, na aplikacijama za mobilne telefone, mogu se koristiti za zaključivanje o tome kako se ponašamo, kako komuniciramo s okolinom i kako se osjećamo u različitim situacijama. Komercijalni sektor vrlo uspješno koristi digitalne otiske kao sredstvo za praćenje ponašanja potrošača u svrhu marketinga i prodaje. Praćenje raspoloženja korisnika, spavanja u stvarnom vremenu te fizičkih i društvenih aktivnosti, od velikog su značaja i za psihijatrijska istraživanja, kao što su prikupljanje podataka iz različitih izvora, analiza, izazovi etičkih i istraživačkih eksperimenta. Digitalni otisci mogu nenametljivo i longitudinalno osigurati ta mjerenja iz stvarnog okruženja (Bidargaddi i sur., 2016). Osim toga digitalni otisci su od velike koristi i kod zdravstvenog sektora, u kojem postoje sustavi osmišljeni tako da otkriju kontekstualne pokazatelje o tome kako osoba djeluje mentalno, socijalno, bihevioralno i fizički u svojoj vlastitoj okolini i prema tim kriterijima pomažu osobama s kroničnim bolestima u liječenju bolesti i pružanja potrebnih lijekova.

Prema Setyowati (2016), digitalne otiske možemo podijeliti na aktivne i pasivne otiske. Kako svi korisnici koji su uključeni u online aktivnosti ostavljaju vlastite digitalne otiske, svojim sudjelovanjem u tim aktivnostima, korisnici dobivaju i vlastitu digitalnu tetovažu koja postaje njihov identifikator, odnosno dio njihovog digitalnog identiteta. Digitalnu tetovažu važno je spomenuti u kontekstu usporedbe s digitalnim otiscima, no više o digitalnim tetovažama bit će navedeno i razjašnjeno u sljedećem poglavlju ovog rada. „**Aktivni digitalni otisci** obuhvaćaju sve aktivnosti namijenjene izradi informacija o sebi, uključujući dijeljenje osobnih podataka, stvaranje profila na stranicama društvenih mreža, postavljanje i komentiranje na blogovima ili društvenim mrežama, dijeljenje informacija o aktivnom

[2] Enriquez tvrdi da svi tragovi što ih sami ostavljamo online čine naše digitalne otiske, dok tragovi koje drugi ostavljaju o nama čine našu digitalnu tetovažu, a sve zajedno označuje našu online prisutnost (Ponderings, 2015).

sudjelovanju u grupi za raspravu i sl.“ (Setyowati, 2016: 3). Međutim, odgovornost za to nije isključivo na pojedincu.

Pasivni otisci su oni koje ostavljate bez namjere da to učinite ili, u nekim slučajevima, čak i ako znate da to činite. Na primjer, prilikom pristupa nekoj web stranici, korisnik nesvjesno ostavlja podatke kao što je njegova IP adresa. Također, pasivan otisak, iako radnja koju korisnik svjesno poduzima, može biti dijeljenje tuđeg, već postojećeg sadržaja na društvenim mrežama (engl. *sharing*). Korisnici nisu svjesni koliko ostavljanjem pasivnih otisaka mogu doprinijeti oblikovanju njihovih digitalnih tetovaža. „Dijeljenje sadržaja, označavanje (engl. *tagging*) na društvenim mrežama i sl. postaje alat za dijeljenje pojedinosti s imenima, mjestima, temama i datumima“ (Setyowati, 2016: 3).

I aktivni i pasivni otisci mogu se pratiti i promatrati na više načina i iz više izvora. Kada poduzmete korake kako biste kontrolirali svoj digitalni otisak, poduzimate korak za zaštitu vlastitog identiteta i ugleda. Iako nije u potpunosti moguće kontrolirati sve digitalne otiske koje korisnik ostavlja, poduzimanjem koraka za zaštitu identiteta smanjuje se nekontrolirano iznošenje osobnih podataka o korisniku. Neki od tih koraka podrazumijevaju korištenje i prilagođavanje postavka privatnosti na određenim web stranicama, provjeru uvjeta koje neka određena web stranica ili aplikacija postavlja, korištenje čuvara lozinke, i sl.

U sljedećim pod-poglavljima navode se i detaljnije razrađuju pojedini elementi sudjelovanja i korištenja internetskih stranica ili aplikacija, odnosno kako svaki od njih zasebno utječe na ostavljanje otisaka u digitalnom okruženju, te kako ih korisnik može kontrolirati.

5.1. Digitalni otisci kao podaci koje proizvode drugi korisnici

Digitalni otisci nisu samo proizvod aktivnog sudjelovanja kroz produkciju i dijeljenje sadržaja, već i pasivno sudjelovanje. Platforme društvenih medija omogućuju mnogo jednostavnih korisničkih radnji, kao što su *lajkanje*, favoriziranje, praćenje ili komuniciranje, koje se ne smatraju nužno aktivnim sudjelovanjem, ali svejedno doprinose digitalnom otisku. Platforme i online usluge čak generiraju podatke bez aktivnog sudjelovanja korisnika. Prema Büchi, Lutz i Micheli (2017: 2), „samo uključivanje uređaja s omogućenim pristupom internetu otkriva IP adresu, klikanje *like* gumba nije samo društveni signal drugom korisniku, nego i informiranje o profilima oglašavanja platforme i objavljivanje posta nije samo usluga za čitatelje, nego također utječe na indeksiranje tražilice.“

Korisnici interneta mogu biti tzv. „sudionici“ drugih korisnika. Primjeri uključuju označavanje, potvrde, ocjene i komentare na vidljivom kraju spektra te pretraživanja (npr. pretraživanje neke osobe u Googleu) i razne analize podataka na manje vidljivom kraju. Takvi oblici pasivnog sudjelovanja mogu proizvesti i poželjne i profitabilne posljedice, kao i neželjene ili neugodne posljedice. Primanje ocjena (engl. *raitings*), *lajkova* i dijeljenje (engl. *sharing*) može povećati nečiji status na mreži. Prema Büchi, Lutz i Micheli (2018), značaj podataka koje generiraju drugi korisnici posebno je očigledan za mikro-slavne osobe[3], kao što su web utjecatelji[4] i *YouTuberi*[5]. Zapravo, takvi iskusni korisnici interneta neprestano surađuju sa svojim sljedbenicima na nekoliko platformi u svrhu dobivanja povratnih informacija. Mikro-slavne osobe svjesne su da su aktivnosti njihovih sljedbenika temeljne za održavanje njihove popularnosti na internetu.

5.2. Kolačići

Većina ljudi je čula za internet kolačiće (engl. *cookies*), male datoteke koje sadrže informacije o web-lokacijama koje posjećujete i vašim navikama pregledavanja. Prema Khanseu (2013), internet kolačić je mali isječak informacija poslanih s web-poslužitelja na korisnički preglednik, koji ga zatim pohranjuje. Nakon naknadnog pristupa istom tom web poslužitelju, poslužitelj može zatim pročitati taj isječak informacija i upotrijebiti ga za "prepoznavanje" korisnika. To su proširenja HTTP protokola, koji omogućuje surfanje internetom tako da se tražena web stranica dostavi s relevantnog poslužitelja na vaše računalo i zatim ju prikazuje u vašem pregledniku.

Kad god posjetite web-lokaciju, ostavljate tragove u obliku kolačića. Osim kolačića koji mogu odati vašu IP adresu i vjerodajnice za prijavu, također možete ostaviti informacije za internetske marketinške agencije, koje mogu unovčiti vaše digitalne otiske. Postoje različiti tipovi internet kolačića:

- kolačići prve i treće strane,

[3] Mikro-slavna osoba gradi vlastiti kapital kao i svaki drugi brend, stvaraju vlastitu sliku i vode računa da njihova online prisutnost dobiva publiku izvan kruga prijatelja i poznanika.

[4] Web utjecatelj je osoba koja ima utjecaj na odluke drugih korisnika društvenih mreža i potencijalnih kupaca određenih proizvoda; koje web utjecatelj promovira, zbog svog autoriteta, znanja, položaja ili odnosa sa svojom publikom. To je pojedinac koji ima ulogu u određenoj branši, s kojom aktivno sudjeluje.

[5] Youtuber je vrsta internetske zvijezde i videografa koji je stekao popularnost od svojih videozapisa na web-lokaciji za dijeljenje videozapisa „YouTube“. Neki YouTuberi imaju korporativne sponzore koji ih plaćaju za plasman proizvoda u svojim isječcima ili za proizvodnju online oglasa.

- kolačići sesije i trajni kolačići,
- neophodni i ostali kolačići.

Kolačići prve strane (engl. *First-party cookies*) dolaze s web stranice kada ju posjećujete i često služe za pravilan rad web stranice te za pamćenje preferenci posjetitelja web stranice. **Kolačići treće strane** (engl. *Third party cookies*) su kolačići koji su postavljeni od strane druge web stranice ili usluge kao što je npr. YouTube. **Kolačići sesije** (engl. *Session cookies*) su privremeni kolačići koji istječu nakon što napustite web stranicu. Ti kolačići su obvezni za pravilan rad određenih aplikacija ili funkcionalnosti na stranici koju posjećujete. **Trajni kolačići** (engl. *Persistent cookies*) koriste se radi poboljšanja iskustva korisnika, kao primjerice pamćenje detalja prijave na nekoj web stranici, tako da ne morate upisivati potrebne podatke svaki put kada posjetite određenu web stranicu. Ti kolačići ostaju u kolačić datoteci vašeg preglednika duže vrijeme. Taj vremenski period ovisit će o izboru postavki na vašem internet pregledniku. **Neophodni kolačići** su nužni za rad web stranice i korištenje njegovih značajki i /ili usluga. Primjerice omogućuju navigaciju po web stranici i mogućnost prijave u sigurna područja. Korištenjem određene web stranice automatski dajete privolu na uporabu neophodnih kolačića bez kojih web stranica ne može funkcionirati. To su PHPSESSID kolačići[6] i _exp kolačići[7].

Prema All about Cookies.org, (2019) zbog svoje fleksibilnosti i činjenice da mnoga web-mjesta koriste kolačiće prema zadanim postavkama, kolačići su gotovo neizbježni. Onemogućavanje kolačića ograničit će korisnika na mnogim najčešće korištenim web-mjestima na internetu, kao što su Youtube, Gmail, Yahoo mail i drugi. Čak i postavke pretraživanja zahtijevaju kolačiće za postavke jezika. Uz jasno razumijevanje načina na koji funkcioniraju i kako vam pomažu u pretraživanju, možete poduzeti potrebne sigurnosne mjere kako biste sigurno provjerili internet. Kolačiće možete kontrolirati putem svojih pretraživačkih postavki te putem ostalih alata. Uvijek možete blokirati upotrebu nekih ili svih kolačića koji se koriste na određenoj web stranici, no to može utjecati na njenu funkcionalnost. Neki preglednici omogućuju surfanje u anonimnom načinu rada,

[6] PHPSESSID kolačići sadrže samo referencu na sesiji pohranjenu na web poslužitelju. Nijedan podatak nije pohranjen u korisnikovom pregledniku i ovaj kolačić se može koristiti samo na trenutnoj web stranici.

[7] exp_ kolačići su postavljeni od strane sustava za upravljanje sadržajem i sadrže podatke poput vremena kada ste posljednji put posjetili web stranicu, prethodne stranice koje ste pogledali, duljinu sesije za prijavljenog korisnika, ID sesije i sl. Ovim kolačićima se ne prikupljaju osobni podaci posjetitelja, nego se koriste samo za osnovnu funkcionalnost internet stranice.

ograničavajući količinu podataka postavljenih na vaš uređaj kada završite sesiju pregledavanja. Postoje i mnoge aplikacije trećih strana koje možete dodati u preglednik da biste blokirali ili upravljali kolačićima. Možete i izbrisati kolačiće koji su prethodno bili postavljeni na vašem pregledniku tako da odaberete opciju za brisanje povijesti pregledavanja i pritom uključite i opciju brisanja kolačića.

Ako ste zadovoljni s kolačićima i jedina ste osoba koja koristi vaše računalo, možda ćete htjeti postaviti vremenske okvire za dugi rok za pohranu vaših osobnih pristupnih informacija i povijesti pregledavanja. Ako dijelite pristup na računalu, možete postaviti svoj preglednik da briše privatne podatke o pregledavanju svaki put kada zatvorite preglednik. Ova opcija omogućuje pristup web-mjestima koja se temelje na kolačićima dok brišete osjetljive informacije nakon sesije pregledavanja.

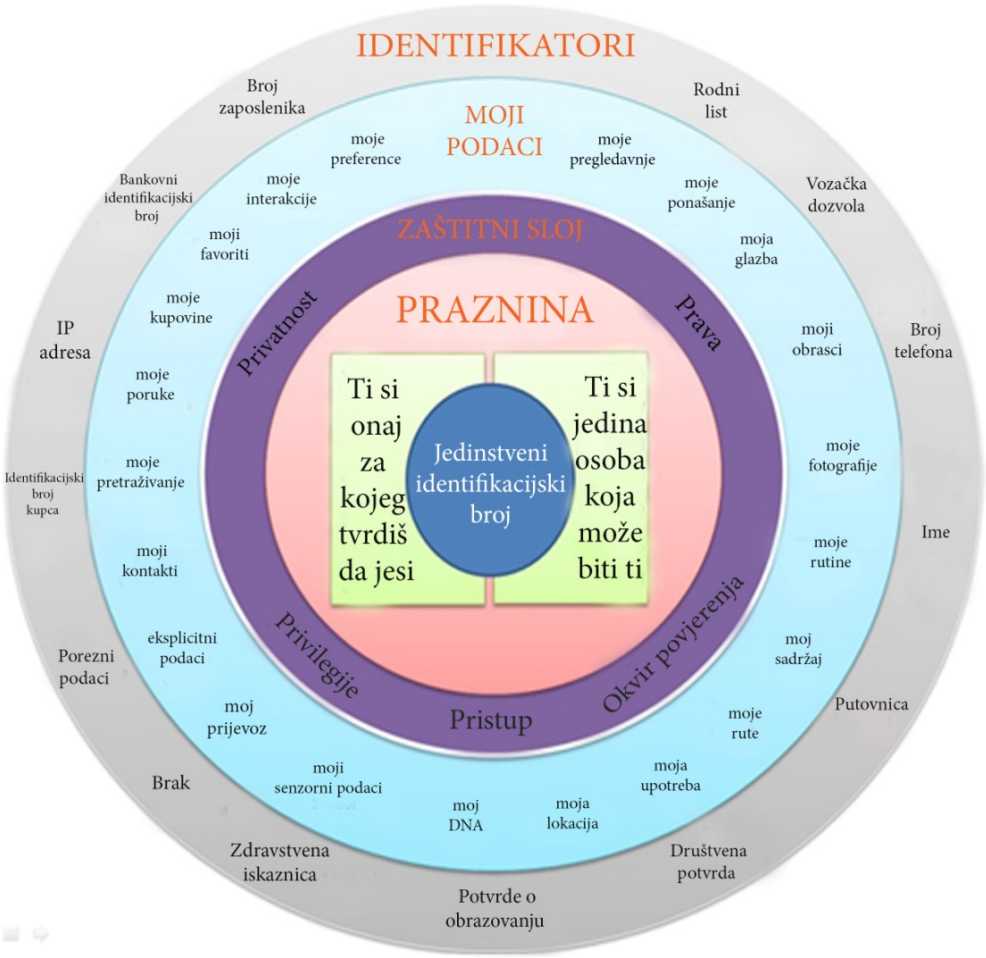
Ako se želite dodatno zaštititi, instalirajte i održavajte aplikacije za čišćenje i uklanjanje špijunskog softvera. One blokiraju pristup pregledniku web-stranicama dizajniranim za iskorištavanje ranjivosti preglednika ili preuzimanje zlonamjernog softvera. Ako to već niste učinili, postavite preglednik da se automatski ažurira. Time se eliminiraju sigurnosne ranjivosti uzrokovane zastarjelim preglednicima. Mnogi poduhvati koji se temelje na kolačićima temelje se na iskorištavanju sigurnosnih nedostataka starijih preglednika.

5.3. Praznina digitalnog otiska

Sve je veća upotreba algoritama i umjetne inteligencije u različitim životnim domenama i zahtijeva detaljno istraživanje digitalnih otisaka. Digitalni otisci ne odgovaraju samo podacima koji se stvaraju aktivnim stvaranjem internetskog sadržaja (ili podacima koji se na kraju mogu sakriti putem postavki privatnosti), nego također ovise o algoritamskim operacijama i pasivnom sudjelovanju. Mnogi se algoritmi u velikoj mjeri oslanjaju na osobne podatke, a ne nužno samo na mrežne podatke. Primjerice, automatizirano donošenje odluka putem algoritama temeljenih na osobnim podacima odvija se u kontekstu očuvanja sadržaja društvenih mreža, ocjenjivanja društvene kreditne sposobnosti, preporučenih sustava u online kupovini i zabavnim okruženjima (npr. *Ebay*, *Netflix* i sl.) (Büchi, Lutz i Micheli, 2018).

Algoritmi mogu postati problematični, podižući etička pitanja o transparentnosti, odgovornosti, pristranosti i diskriminaciji. Prema Büchi, Lutz, i Micheli (2017) pojam praznine digitalnog otiska (engl. *digital footprint gap*) prvi su razradili Robinson i sur. (2015)

u kontekstu digitalnih nejednakosti tijekom životnog ciklusa, pozivajući se na podatke koje su odrasle osobe objavile o (nesvjesnoj[8]) djeci. Unutar ovog pristupa, izraz praznine digitalnog otiska opisuje razlike u količini online tragova između pojedinaca ili različitih skupina stanovništva. Internetske platforme trebaju biti osmišljene ne samo da bi bile dostupne, već i da bi se spriječilo pojavljivanje tog koncepta. Konkretno, slabije povlaštene i nedovoljno zastupljene skupine trebale bi dobiti više glasa, dok bi one skupine koje su posebno osjetljive na uznemiravanje ili iskorištavanje putem svojih digitalnih otisaka bile bolje zaštićene. Prema Slici 8, identifikatori predstavljaju vanjski sloj, odnosno identitet koji nam je dodijeljen, naši podaci su sloj identiteta kojeg sami generiramo, zaštitni sloj predstavlja sloj koji štiti ono što želimo zaštititi. Praznina digitalnog otiska predstavlja sloj koji nedostaje između onoga što želimo, jedinstvenog identiteta i zaštitnog sloja, odnosno; privatnosti, privilegija, prava, pristupa i okvira povjerenja.



Slika 8: Grafički prikaz praznine digitalnog otiska (prilagođeno iz My digital footprint, 2013)

[8] Djeca čiji se identitet ili podaci o njima objavljuju na Internetu bez njihovog znanja i voljnog pristanka, od strane odraslih ljudi (bilo da se radi o njihovim roditeljima, rodbini, prijateljima ili slučajnim prolaznicima).

5.4. Uklanjanje digitalnog otiska

Možda nikada nećete biti u mogućnosti u potpunosti izbrisati vaš digitalni otisak, budući da je toliko toga već gotovo svugdje. Međutim, postoje načini da smanjite količinu informacija o vama i da se u nekim slučajevima, uklonite iz određenih baza podataka. Postoje dva načina čišćenja ili brisanja digitalnih otisaka. Prvi je prilično skup i uključuje angažiranje agencije za pronalaženje i čišćenje informacija o vama na internetu. Drugi način je korištenje mjera opreza tijekom pregledavanja, kao što je VPN (engl. *Virtual Private Network*) i proxy. (Khanse, 2014). VPN je mrežna tehnologija koja preko javne ili privatne mreže u vlasništvu pružatelja usluge izrađuje sigurnu vezu. Proxy, s druge strane je računalo koje se nalazi između korisnika interneta i web poslužitelja kao posrednik. U suštini i VPN i proxy služe kao posrednici između korisnika i određene web adrese, no proxy u tom odnosu nije ništa više no posrednik, dok VPN prikuplja sve podatke s korisnikovog računala koje potom šifrira i upotrebljava u korist subjekta.

Osim navedenog mogu se koristiti i posebni preglednici kako bi se izbjeglo prikupljanje osobnih podataka, odnosno digitalnih otisaka. Postoji nekoliko proširenja za različite preglednike koji vam omogućuju da spriječite web-lokacije i povezane marketinške agencije u prikupljanju podataka o vama. Takva proširenja su specifična za preglednik i ne odnose se na računalo pa ih je potrebno instalirati u svakom pregledniku. Dostupna su mnoga proširenja koja ne blokiraju sadržaj web-mjesta, a sprečavaju stvaranje digitalnog otiska. Neki preglednici, kao što su Internet Explorer, Firefox i Google Chrome, imaju opciju za onemogućavanje praćenja geolokacije koja, kada je omogućena, šalje web-lokacijama poruku da odobravate da određene stranice koje pregledavate prikupljaju vaše podatke. Prema Sadler (2017), neki od načina uklanjanja vlastitih digitalnih otisaka su:

- deaktivacija svih računa društvenih mreža,
- deaktivacija ili brisanje starih računa elektroničke pošte,
- pretraživanje informacija o sebi na internetu, gdje možete pronaći svoje stare račune, profile i druge informacije,
- brisanje rezultata pretraživanja informacija o sebi, možete tražiti zahtjev da tražilice uklone sve informacije o vama koje ne želite tamo,
- poništavanje pretplata na sve popise elektroničke pošte i upozorenja SMS-om,

- brisanje starih poruka elektroničke pošte koje mogu sadržavati bilo kakve osobne ili osjetljive informacije o vama poput lozinka ili brojeva računa koje ste zaboravili,
- zahtijevanje od svoje telefonske tvrtke da vas učini "nenavedenim" kako vaši podaci ne bi bili dostupni na mreži.

Internet korisnici trebali bi voditi računa o tome koje web stranice posjećuju, na kojim web-lokacijama ostavljaju osobne podatke i koje podatke sve ostavljaju kako bi imali kontrolu nad vlastitim digitalnim otiscima. Međutim, nema jamstva da će web-lokacije prestati prikupljati podatke o vama, ako i poduzmete sve navedene mjere uklanjanja digitalnih otisaka.

6.

Digitalna tetovaža

Digitalna tetovaža se u većini slučajeva poistovjećuje s definicijom digitalnog otiska, no postoje i oni koji vide razliku između ta dva koncepta. Prema Treyvaudu (2018), pošteno je reći da u bilo kojem trenutku kada koristimo internet ostavljamo trag, stazu podataka ili digitalni trag iza nas. Međutim, upotreba riječi "otisak" (engl. *footprint*) suptilno podrazumijeva da taj trag nestaje nakon nekog vremena, što nije slučaj. To je zato što je iz raznih razloga gotovo nemoguće ikada doista izbrisati nešto u potpunosti s interneta. Zato je riječ 'tetovaža' koja ostaje kao trajni otisak na našem tijelu, precizniji prikaz oznake koju ostavljamo kada koristimo internet.

Tetovaža je slikovna umjetnost koja koristi kožu kao medij. To nije samo boja nanesena na površinu kože, već boja trajno unesena u dublji sloj kože. Jednom napravljenu tetovažu teško je ukloniti. Oni koji se tetoviraju svjesni su trajnosti tetovaže, što je u stvari razlog zašto se ljudi i tetoviraju. Žele trajno obilježiti svoje uspomene ili staviti potpis koji predstavlja vrijednosti u koje vjeruju. Dakle, tetovaža je i jedinstvena i osobna zbog vrijednosti za vlasnika. Budući da je jedinstvena i osobna, tetovaža se ponekad koristi kao oznaka za identifikaciju nekoga. Zbog trajnosti posljedica tetovaže u stvarnom svijetu, pojam digitalne tetovaže ima svoju težinu u virtualnom svijetu.

Araoz (2016) navodi neke ključne razlike između pojma digitalnog otiska i digitalne tetovaže (Slika 9). Ono što je karakteristično za digitalnu tetovažu je da je ona trajna, aktivno se stvara, može se kontrolirati, nastaje često svjesno za razliku od digitalnog otiska koji je privremen, pasivno stvaran, teško ga je kontrolirati i često odražava nedostatak izbora za korisnika kod pretraživanja određenog sadržaja.

Slika 9: Razlike između digitalnog otiska i digitalne tetovaže (prilagođeno iz Lee Araoz, 2016.)

TeleWare (2015) navodi kako utjecajni akademik Juan Enríquez spominje frazu "digitalna tetovaža" 2013. godine na konferenciji TED (Technology, Entertainment, Design). Fraza "tetovaža" bila je dokaz online utiska koje poslovne organizacije ostavljaju iza sebe. Bez obzira radi li se o profilu društvenih mreža, blogu ili informacijama na web-lokaciji, ideja digitalne tetovaže jest da će digitalne informacije zauvijek živjeti na mreži s organizacijom. Enriquez tvrdi da smrt više nije najveća prijetnja ljudskom biću, nego je ugrožena prijetnjom besmrtnosti - besmrtnom prijetnjom digitalne tetovaže. Digitalna tetovaža izgleda kao relevantnija metafora za opisivanje online prisutnosti nego digitalni otisak. Međutim, tetovaža je u stvarnom životu vidljiva sve dok je čovjek živ. To znači da ni digitalni otisak niti digitalna tetovaža nisu vječno trajni, iako besmrtnost zvuči prikladno za opisivanje tragova koje ostavljamo za sobom online.

Mi nismo jedini koji stvaramo našu vlastitu online prisutnost. Jednom kada smo prisutni na internetu, imamo publiku, sljedbenike koji nas dijele i spominju. Naši će se online predmeti dijeliti, mijenjati, koristiti, možda čak i prodavati od strane drugih korisnika. Iako kontroliramo ono što ostavljamo iza sebe, ne kontroliramo ono što drugi ostavljaju o nama, to je ono što našu digitalnu tetovažu čini toliko trajnom; nemogućnost kontrole našeg online identiteta i naših aktivnosti od upravljanja i korištenja od strane drugih korisnika (Slika 10).

Prema tome, Enriquez tvrdi da svi tragovi što ih sami ostavljamo online čine naše digitalne otiske, dok tragovi koje drugi ostavljaju o nama čine našu digitalnu tetovažu, a sve zajedno označuje našu online prisutnost (Ponderings, 2015).

Slika 10: Grafički prikaz ostavljanja digitalnih tragova, prilagođeno iz Ponderings (2015)

Kada je život ljudi u velikoj mjeri ovisan o digitalnoj tehnologiji, mnoge od njihovih svakodnevnih aktivnosti, uključujući komuniciranje i pronalaženje informacija, obavljaju se pomoću digitalnih medija. „Račun e-pošte koji se koristi kao "kućna adresa" više se ne koristi samo za primanje elektroničke pošte, već i kao "pristupna šifra" koja je potrebna za mnoge aktivnosti korištenja društvenih medija ili obavljanje transakcija putem e-bankarstva ili komercijalnih web-lokacija itd.“ (Setyowati, 2016: 3). Tako dobrovoljno dijelimo mnoge osobne podatke na web-lokacijama koje posjećujemo. Te podatke zatim čuva svaka posjećena web-lokacija. Možemo ostaviti informacije tamo, uključujući i naše aktivnosti tijekom posjeta. Na taj način stvaramo našu digitalnu tetovažu.

Drugi način da se formira digitalna tetovaža je putem web preglednika. Mnogi možda nisu svjesni pasivne digitalne tetovaže. Tražilice poput Googlea arhiviraju sve aktivnosti

svojih korisnika tijekom pregledavanja mreže, kao što su korisnički pojmovi za pretraživanje, adresa računala i jedinstveni identifikator za njihov web-preglednik. Ne samo da mnoge web-lokacije koje posjećujemo, prate i čuvaju sve informacije o posjetitelju, opremljene kolačićima, te web-lokacije arhiviraju digitalne tragove koje smo ostavili prilikom pristupa njima. Svaka online aktivnost, pretraživanje, online transakcije, gledanje slika i videozapisa, označavanje, slanje poruka, *lajkanje* i sl. ostaje zapisana i čini našu digitalnu tetovažu.

Nadalje, društveni mediji i fotografije korisnika, mogu potencijalno izazvati neugodu za poslodavce. Disciplinske mjere mogu se poduzeti u slučaju neprimjerenih mrežnih aktivnosti. Poslodavci sve češće koriste društvene medije kako bi provjerili zaposlenike prije nego što ih pozovu na intervju za posao, što služi kao upozorenje svima koji traže posao. Prema TeleWareu (2015), živimo u doba u kojem je svaki zaposlenik predstavnik posla i tvrtke za koju rade, pa tako zaposlenikova digitalna tetovaža postaje dio digitalne tetovaže tvrtke koju predstavljaju. Na primjer, ako zaposlenik postavi nešto na Facebook ili LinkedIn, naziv tvrtke automatski se povezuje s tom porukom, negativno ili pozitivno. Slično tome, postoji mnogo web stranica za ocjenjivanje tvrtki i usluga, kao što su Trust Pilot i FeeFo, gdje zaposlenik može objaviti štetno mišljenje o tvrtki i njenim proizvodima. Neuspješno reagiranje na takve komentare može biti jednako štetno kao izvorni komentar.

Za organizacije, pitanje digitalnih tetovaža je sve složenije zbog sve veće sklonosti zaposlenika da donose i koriste vlastite uređaje na poslu, potencijalno izlažući poslovnu aktivnost i veze širem razmatranju. Mogu postojati ozbiljne posljedice za tvrtke koje ne osiguravaju postojanje procesa za ublažavanje rizika i odgovarajućih rješenja na negativne učinke. Organizacije moraju biti odgovorne za svoj vlastiti digitalni identitet i uspostaviti institucionalnu promjenu kulture kako bi omogućile osnaženu i pozitivnu radnu snagu koja djeluje kao svakodnevni ambasador tvrtke (TeleWare, 2015).

6.1. Svijest o digitalnoj tetovaži

Postoje barem dva glavna razloga zašto je potrebno razumjeti digitalnu tetovažu: osobni brending[9] i filter mjehurić (engl. *filter bubble*). Osobni brendovi brinu se o tom kako drugi korisnici vide nekoga, na temelju njegovog znanja o toj osobi. U digitalnom svijetu, gdje se identiteti oblikuju u računalnom okruženju kao što su društvene mreže, blogovi, osobne web

[9] Brendiranje (engl. branding) je proces kojim se definira što neki proizvod jest, što ga razlikuje od drugih, koje su njegove koristi i što proizvod znači korisniku (Creative Solutions, 2019).

stranice i sl., osobne podatke je lakše pronaći, što drugima olakšava upoznavanje osobnog branda. Dokle god su pronađene informacije pozitivne, koristi se osobni brend. Naprotiv, ako su pronađene informacije negativne, onda je njegov ugled oštećen.

Prema Setyowati (2016), internetski aktivist Eli Pariser u svojoj knjizi *Filter bubble: What Internet hides from you* (2011) prvi spominje i definira pojam filter mjehurića. Mjehurić dolazi od engleske riječi *bubble* koja je u ovom kontekstu sinonim za izolaciju, kao što je naprava zvana izolator bila plastični balon koji se koristio kod pacijenata s autoimunim bolestima (Jugkala, 2018). „Filter mjehurić je učinak interneta da se prilagodi osobnom identitetu pojedinca, te ga izolira od drugih perspektiva“ (Setyowati, 2016: 3).

Filter mjehurić se može pojaviti kada web-lokacije koriste algoritme za selektivno preuzimanje informacija koje korisnik želi vidjeti, a zatim daju korisniku informacije prema toj pretpostavci. Web-lokacije izrađuju te pretpostavke na temelju informacija povezanih s korisnikom, kao što su prijašnje ponašanje klikova, povijest pregledavanja, povijest pretraživanja i lokacija. Zbog toga je vjerojatnije da će web-lokacije prikazivati samo informacije koje će se pridržavati prethodnih aktivnosti korisnika. Personalizirani rezultati pretraživanja dio su marketinške strategije, gdje bi određeni proizvod trebao zadovoljiti potrebe korisnika. Jugkala (2018), navodi da se filtriranje informacija razvilo iz potrebe za izlučivanjem važnih i relevantnih podataka iz gomile koja je počela dosizati nestvarne brojke. Posebno je važno istaknuti neke od njih (Domo, 2017):

- u zadnje dvije godine je proizvedeno više od 90% svih podataka na svijetu;
- dnevno nastaje 2,5 kvintilijuna (10^{30}) bajtova podataka;
- 3,7 milijarde ljudi koristi internet.

Prema korisnikovim potrebama, informacije su prilagođene na temelju njihovog profila, povijesti pretraživanja, što im se sviđa, što kliknu itd. Setyowati (2016) navodi da uz pomoć algoritma, informacijske tvrtke kao što su Yahoo, Google, Facebook, Youtube i Microsoft Live primjenjuju takvo personalizirano filtriranje. Čini se da personalizirano filtriranje nudi idealnu prilagodbu. Svaki korisnik će dobiti informacije na temelju onoga što obično traži, što voli ili onoga što je volio čitati. Prema tome ako dva različita korisnika pretražuju isti pojam, svatko će dobiti drugačiji rezultat za točno iste uvjete pretraživanja. Na neki način, takvo filtriranje također znači da su nam informacije skrivene, čime se perspektive sužavaju ograničavanjem informacija. Drugim riječima, informacijsko okruženje određeno je načinom na koji koristimo medije.

6.2. Projekt digitalne tetovaže

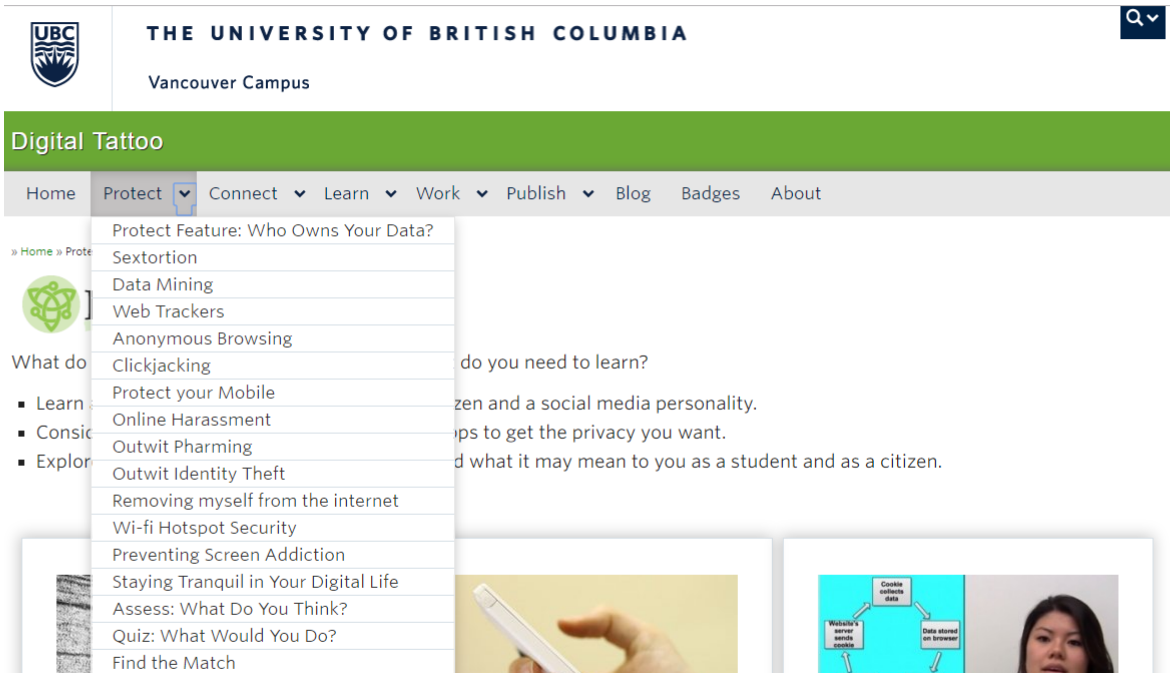
Projekt digitalne tetovaže (engl. *digital tattoo project*) je suradnja knjižnice UBC, centra za učenje Irvinga K. Barbera, Centra za podučavanje, učenje i tehnologiju UBC-a i Fakulteta za informatiku Sveučilišta u Torontu i Inforum knjižnice. Glavni cilj ove online inicijative je poticanje internet korisnika na razmišljanje o svojoj prisutnosti na internetu i educiranje korisnika o oblikovanju i preoblikovanju vlastitog digitalnog identiteta (The Digital Tattoo Project, 2019). Sadržaj stranice razvijaju studenti. S vremena na vrijeme radna skupina (studenti i projektno osoblje) uređuje sadržaj stranice, kako bi bila pravodobna i relevantna. Projekt digitalne tetovaže postavlja pitanja, dijeli priče, razgovara sa stručnjacima i potiče nas da razmotrimo naše digitalne živote.

Primarna navigacija (Slika 11), odnosno glavni izbornik stranice, sastoji se od sljedećih sekcija: naslovnica (engl. *home*), zaštita (engl. *protect*), povezivanje (engl. *connect*), učenje (engl. *learn*), posao (engl. *work*), objavljivanje (engl. *publish*), blog, značke (engl. *badges*) i o nama (engl. *about*). Projekt digitalne tetovaže potiče kritičku raspravu o temama koje se tiču digitalnog državljanstva i internetskog identiteta. Sekcija „zaštite“ orijentirana je na moguće prijeteće rizike i usredotočena je na neke nedostatke digitalnog života, dok su sekcije „povezivanje“ i „učenje“ fokusirane na prednosti digitalnog života.

Slika 11: Primarna navigacija projekta digitalne tetovaže (Digital tattoo project, 2019)

Sekcija „zaštite“ educira čitatelje o njihovim odgovornostima kao digitalnim građanima i o karakteristikama društvenih medija. Potiče na razmišljanje o tome kako upravljati aplikacijama na temelju lokacije kako biste dobili željenu privatnost. Nudi razni izbor aktualnih tema vezanih uz nadzor i što bi to moglo značiti za vas kao studenta i kao građanina (The Digital Tattoo Project, 2019). Neke od teme koje obuhvaća su: tko posjeduje vaše

podatke, rudarenje podataka[10], web *trekeri*[11], anonimno pretraživanje[12], online zlostavljanje[13], uklanjanje sebe s interneta itd. (Slika 12).



Slika 12: teme sekcije „zaštite“ projekta digitalne tetovaže (Digital tattoo project, 2019)

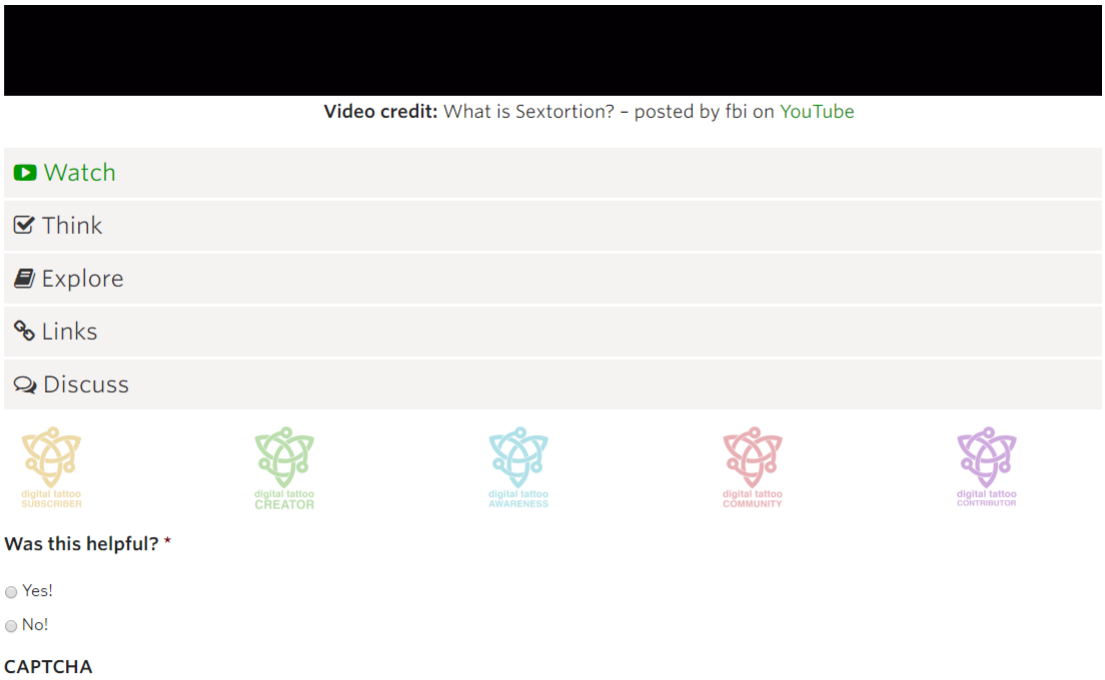
Svaka od navedenih tema u sekciji „zaštite“, sadrži edukacijske video klipove o navedenoj temi (engl. *watch*), pitanja o zadanoj temi u obliku kratkih kvizova (engl. *think*), detaljnije i podrobnije informacije o zadanoj temi (engl. *explore*), poveznice na slične teme ili na stranice koje govore više o zadanoj temi (engl. *links*) i na kraju sekciju u kojoj čitatelji mogu postavljati pitanja, ostavljati komentare i voditi diskusije o zadanim temama (engl. *discuss*) (Slika 13).

[10] Rudarenje podataka definira se kao sortiranje, organiziranje ili grupiranje velikog broja podataka i izvlačenje relevantnih informacija, odnosno otkrivanje znanja iz velike količine podataka (Živković, 2016).

[11] Web praćenje (engl. *tracking*) je praksa kojom web-lokacije identificiraju i prikupljaju informacije o korisnicima. To je općenito u obliku nekog podskupa povijesti pregledavanja weba (FreeCodeCamp, 2018).

[12] Anonimno pretraživanje je online pretraživanje tako da se zaštiti i sakrije vlastiti identitet.

[13] Online zlostavljanje je novi oblik agresije, koji se događa kroz moderne tehnološke uređaje, posebno mobilne telefone ili internet, ali također pokazuje neke karakteristike tipične za tradicionalno nasilje, primjerice, agresivne i namjerne radnje koje je poduzela skupina ili pojedinac (više puta tijekom vremena) protiv žrtve (Gorzig, 2012).



Slika 13: Grafički prikaz izbornika pojedinih tema u sekciji "zaštita"(Digital tattoo project, 2019)

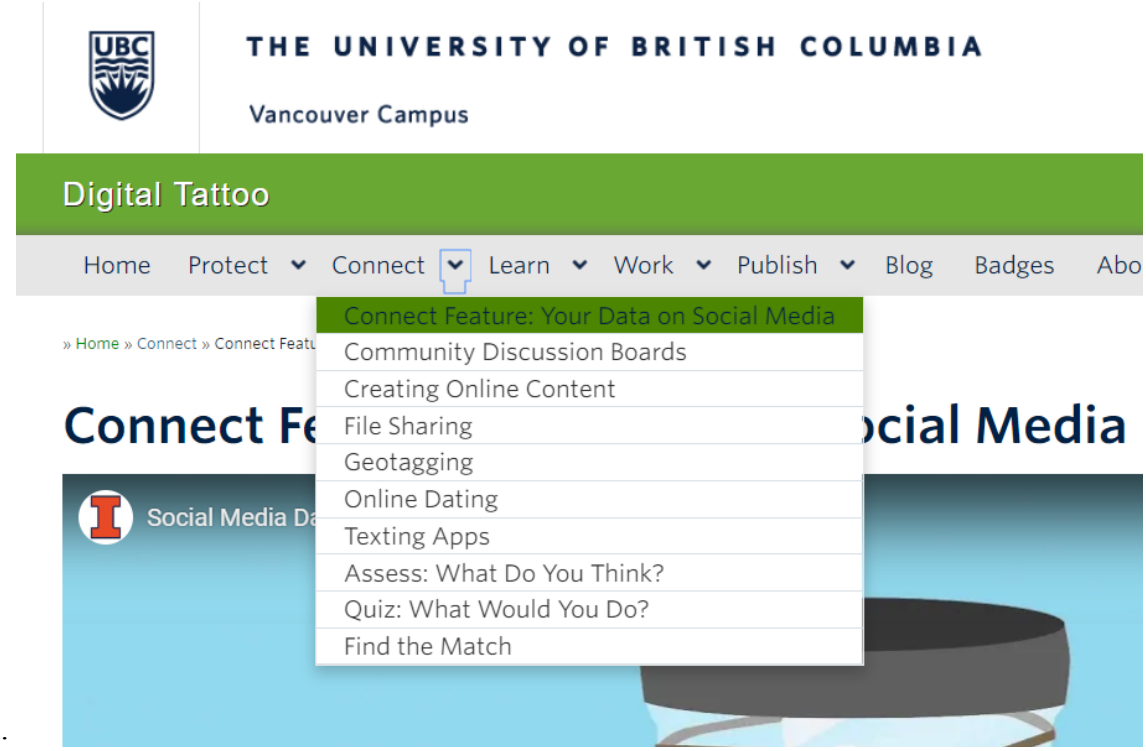
Kao i „zaštita“, i ostale sekcije se sastoje od različitih tema koje se tiču pojmova u glavnom izborniku. Tako se „povezivanje“ referira na neke od sljedećih tema:

- vaši podaci na društvenim mrežama
- diskusijska ploča za zajednicu
- dijeljenje podataka
- geo-označavanje
- online *dating*[14] i sl. (Slika 14).

Tema „vaši podaci na društvenim mrežama“ educira korisnike kako dijeljenje njihovih podataka utječe na njihovu online prisutnost te koje preventivne korake za zaštitu osjetljivih podataka treba poduzeti. Diskusijska ploča za zajednicu navodi korisnicima negativne i pozitivne strane društvenih medija. Potiče se korisnike na sudjelovanje u javnim platformama za komunikaciju, gdje pritom treba razumjeti zajednicu i kako ona prihvaća i reagira na vaš digitalni identitet i aktivnosti. Sekcija dijeljenje podataka upućuje korisnike kada i u kojem slučaju je legalno dijeliti tuđe podatke. Geo-označavanje govori o potencijalnim rizicima

[14] Online dating- način pokretanja romantične veze na internetu, davanje informacija o sebi ili odgovaranje na tuđe informacije (Cambridge dictionary, 2019)

odavanja GPS lokacije[15] uređaja kojeg koristimo i na koji način se zaštititi prilikom označavanja svoje lokacije. Online *dating* podučava korisnike o prednostima i nedostacima korištenja stranica i aplikacija za online *dating* i na koje potencijalne probleme korisnici moraju biti spremni te kako se s njima nositi.



Slika 14: Teme sekcije „povezivanje“ projekta digitalne tetovaže (Digital tattoo project, 2019)

Projekt digitalne tetovaže osim educiranja korisnika o opasnostima prilikom korištenja interneta i važnosti razumijevanja ostavljanja digitalnih otisaka, upućuje čitatelje na to kako njihova online aktivnost utječe na njihovu karijeru te kako se pravilno oglašavati na mreži. Ono što ovaj projekt čini još više zanimljivim je mogućnost dobivanja znački, odnosno nagrada, od same pretplate i prijavljivanja na web-lokaciju, pa sve do nagrađivanja na temelju doprinosa sadržaja od strane korisnika, te nagrađivanje korisnika za rješavanje jednostavnih kvizova na zadane teme.

7.

[15] GPS je kratica za ***G**lobal **P**ositioning **S**ystem*. To je mreža satelita koja kontinuirano odašilje kodirane informacije, s pomoću kojih je omogućeno precizno određivanje položaja na Zemlji (Lapaine, Tutić, god?).

Djeca na internetu

U ovom poglavlju koristila sam za reprezentativni primjer djecu kao najmlađe korisnike interneta, te opisala kako njihovo ponašanje može utjecati na stvaranje njihovih digitalnih tetovaža i digitalnih otisaka. Djeca kao najneiskusniji korisnici mogu poslužiti kao odličan primjer kako se ponašanje na internetu može odraziti na njihovu budućnost i koje su posljedice nesvjesnog korištenja interneta. Iako je snažno oblikovano prošlošću, djetinjstvo u ranom 21. stoljeću vrlo je različito od onog kakvog danas pamte odrasli. Promijenile su se mnoge značajke društvenog, političkog i ekonomskog života, koje su preobrazile čak i život djece posljednjih desetljeća. Korištenje web stranica društvenih mreža jedna je od najčešćih komunikacijskih aktivnosti današnje djece. Prema UNICEF-u (2017), 71% mladih u svijetu ima pristup internetu, u usporedbi s 48% ukupne populacije. Smatra se da je jedan od tri korisnika interneta širom svijeta dijete ili adolescent mlađi od 18 godina. Sve je više dokaza da djeca pristupaju internetu u sve ranijoj dobi. U nekim zemljama djeca mlađa od 15 godina vjerojatno koriste internet kao odrasli iznad 25 godina.

„Sve takve pojave uzrokovale su nastanak pojma "digitalne revolucije“, odnosno široko rasprostranjenog pristupa personaliziranim, interaktivnim, konvergentnim, sveprisutnim tehnologijama za umrežavanje informacijskih i komunikacijskih procesa“ (Gorzig, Haddon, Livingstone, 2012: 1). Pojavljuju se još i novi nazivi kao: „digitalna generacija“ ili „Google generacija“, pritom misleći na generaciju koja većinu slobodnog vremena provede na internetu, a ponajviše na društvenim mrežama.

„Internet je ključan proizvod društva, izmišljen, oblikovan, monetiziran i promoviran od strane glavnih medijskih konglomerata kako bi se mnogima donijelo bogato informacijsko i komunikacijsko okruženje“ (Gorzig, Haddon, Livingstone, 2012: 2). Ali posljedice, iako često nenamjerne, predstavljaju izvor znatne brige i straha među mnogim „običnim“ ljudima koji to ne mogu točno razumjeti, odnosno, procijeniti kvalitetu onoga što nudi ili predvidjeti ishode prakse svojeg korištenja interneta. „Bilo koja web stranica koja omogućuje društvenu interakciju smatra se web-lokacijom društvenih medija, uključujući društvene mreže tj. web mjesta kao što su Facebook, MySpace i Twitter, web mjesta za igranje i virtualni svjetovi kao što su Club Penguin, Second Life i Sims, web mjesta s videozapisima kao što je YouTube te blogovi“ (Schurgin, Clarke-Pearson, 2011: 800). Takve stranice nude mladima mjesto za zabavu i komunikaciju i eksponencijalno su porasli posljednjih nekoliko godina.

Djeca su nerazmjerno pogođena mrežnim opasnostima, a time i gubitkom privatnosti. Kod djece je neophodno računati na to da je mala vjerojatnost da razumiju kakvim se sve opasnostima na internetu izlažu i da razumiju koji im sve rizici prijete. Zbog toga je važno da roditelji postanu svjesni prirode stranica društvenih mreža, s obzirom na to da neke od njih ne predstavljaju zdravu okolinu za njihovu djecu.

7.1. Rizici izlaganja na internetu

Glavni rizici za djecu na internetu danas su neprikladne uporabe tehnologije, nedostatak privatnosti, dijeljenje previše informacija, ili postavljanje lažnih podataka informacije o sebi ili drugima. Ove vrste ponašanja ugrožavaju korisnikovu privatnost. Kada posjećujemo razne web-stranice ostavljamo za sobom dokaze o tome koje smo web-lokacije posjetili, odnosno ostavljamo digitalne tragove. Djeca, kojoj nedostaje svijest o pitanjima privatnosti, često objavljuju neprikladne poruke, slike i videozapise bez razumijevanja da ono što ide na mrežu, ostaje na mreži. Takve aktivnosti nose razne rizike sa sobom, kao što su utjecanje na buduće prijave za škole, fakultete i poslove ili sama činjenica da takvim ponašanjem djeca postaju lake žrtve prevaranata na internetu.

Prema Schurgin i Clarke-Pearson (2011), mnoge web-lokacije društvenih mreža prikazuju više reklama kao što su *banner* oglasi[16], oglasi ponašanja (oglasi koji ciljaju na ljude na temelju njihovog web-pregledavanja) i oglasi na temelju demografije (oglasi koji ciljaju na ljude na temelju određenog faktora kao što je dob, spol, obrazovanje, bračni status itd.) koji ne utječu samo na tendencije kupnje korisnika, već i njihova stajališta o tome što je normalno. To je posebno važno za roditelje čija se djeca koriste internetom jer moraju biti svjesni utjecaja oglasa na djecu, pošto su oglasi uobičajene pojave na društvenim stranicama i skupljaju informacije o osobi koja koristi te stranice. Iako danas mnoge društvene stranice zabranjuju oglase na web-lokacijama na kojima djeca i adolescenti sudjeluju, važno je educirati roditelje i djecu da bi se djeca mogla razvijati u takvoj okolini i razumjeti kako ih oglasi lako mogu manipulirati. Sva se djeca suočavaju s mogućnošću susretanja s prijetnjama koje su posljedica internetske tehnologije. Prema UNICEF-u (2017: 21-22), „postoji široki raspon rizika koji se pojavljuju na internetu koje možemo podijeliti u tri kategorije: rizici sadržaja, rizici kontakta i rizici ponašanja.“

[16] Banner oglasi su ujedno i linkovi pa klikom na banner oglas otvara se web stranica tvrtke ili nas banner oglas vodi na micro web stranice marketing kampanje za određeni proizvod, uslugu ili brend.

- **Rizici sadržaja**, podrazumijevaju izlaganje djece neprikladnim i nepoželjnim sadržajima na netu, kao primjerice, seksualne, pornografske i nasilne slike; određeni oblici oglašavanja; rasistički i diskriminacijski sadržaji, stranice koje promoviraju nezdrava ili opasna ponašanja, poput samoozljeđivanja, samoubojstava i anoreksije.
- **Rizici kontakta**, podrazumijevaju sudjelovanje djece u rizičnoj komunikaciji, primjerice s odraslom osobom koja traži neprikladan odnos s djetetom ili s pojedincima koji nastoje uvjeriti dijete da sudjeluje u nezdravim i opasnim ponašanjima.
- **Rizici ponašanja**, odnose se na ponašanje djece na određeni način koji doprinosi nastanku rizičnog sadržaja ili odnosa, primjerice djeca koja negativno pišu o drugoj djeci ili stvaraju materijale pune mržnje prema drugoj djeci, potičući rasizam, ili objavljivanje i dijeljenje seksualnih slika, uključujući materijal koji su sami kreirali i sl.

Razumijevanjem ovih ranjivosti i odgovaranjem na njih možemo bolje štititi djecu i na internetu i izvan njega, te omogućiti djeci da uživaju u prilikama koje nudi povezivanje s digitalnim svijetom (UNICEF, 2017: 22).

7.2. Cyberbullying

Prema UNICEF-u (2017: 4), „informacijske i komunikacijske tehnologije povećavaju tradicionalne rizike u djetinjstvu (poput nasilnog ponašanja) i potiču nove oblike zlostavljanja i iskorištavanja djeteta (poput kreiranja materijala o seksualnom zlostavljanju djeteta po narudžbi i direktnog prijenosa snimaka seksualnog zlostavljanja djece).“ Iako se pojam cyberbullying sve češće koristi i u akademskim istraživanjima, ne postoji standardna definicija ovog fenomena. „Većina opisa smatra da je cyberbullying novi oblik agresije, koji se događa kroz moderne tehnološke uređaje, posebno mobilne telefone ili internet, ali također pokazuje neke karakteristike tipične za tradicionalno nasilje, primjerice, agresivne i namjerne radnje koje je poduzela skupina ili pojedinac (više puta tijekom vremena) protiv žrtve“ (Gorzig, Haddon, Livingstone, 2012: 141).

Međutim, neki aspekti tradicionalnog vršnjačkog nasilja mogu biti manje izravno preneseni u online kontekstu, a manje pouzdani za određivanje slučajeva internetskog zlostavljanja, za razliku od zlostavljanja izvan mreže. S obzirom na to da se okrutnost preko

interneta može pojačati razmakom između počinitelja i žrtve, mijenja se koncept zlostavljanja. Djeca više nemaju sigurnost da odu kući i izbjegnu uznemiravanje.

Nasilje putem interneta uključuje poticanje grupne mržnje, napade na privatnost, uznemiravanje, uhođenje, vrijeđanje, neovlašten pristup štetnom sadržaju i širenje nasilnih i uvredljivih komentara. To može uključivati slanje okrutnih, zlih, ponekad prijetećih poruka, kao i stvaranje web stranica koje sadrže priče, crteže, slike i šale na račun vršnjaka (Centar za sigurniji Internet, 2019). Ne postoji jasan konsenzus o tome kako različiti sociodemografski i osobni čimbenici utječu na cyber zlostavljanje. Na primjer, Smith i sur. (2006) ne nalaze nikakav učinak u dobi među 11 i 16 godina, gdje, Ybarra i Mitchell (2004) smatraju da su učenici stariji od 15 godina češće internet agresori nego djeca mlađe dobne skupine od 10-14 godina. Rodni učinci su manje jasni, neke studije navode da su djevojčice češće žrtve internetskog zlostavljanja, a da su dječaci češće počinitelji (Smith i sur., 2006.; Li, 2007) (Gorzig, Haddon, Livingstone, 2012).

U Hrvatskoj, prema policijskim podacima iz 2015. godine, 25% djece i adolescenata proživljava neki oblik cyberbullyinga.

Postoje dvije vrste online nasilja, izravni i napad preko posrednika. Prema Centru za sigurniji Internet (2019), do izravnog napada dolazi kada maloljetnik:

- šalje uznemirujuće poruke na vaš mobilni telefon, e-poštu, chat, forum, razne internetske stranice i sl.,
- krade ili mijenja zaporku za e-poštu ili nadimak,
- objavljuje osobne podatke ili lažne podatke na chatu , blogu ili web-lokaciji,
- šalje uznemirujuće slike putem e-pošte ili MMS-a na vašem mobilnom telefonu,
- postavlja online ankete o žrtvi,
- šalje viruse na e-poštu ili mobitel,
- šalje pornografiju i *spam* na e-poštu ili mobilni telefon,
- predstavlja se lažnim identitetom.

Nasilje preko posrednika nastaje kada počinitelj napada žrtvu preko treće osobe, koju najčešće ne poznaje. Ovakva se vrsta virtualnog nasilja najčešće manifestira izradom anonimnog profila, ili profila koji je izrađen na temelju lažnih podataka počinitelja na nekoj određenoj aplikaciji, forumu ili blogu preko kojeg se napada žrtva.

7.3. EU Kids Online

Projekt *EU Kids Online* temelji se na jedinstvenom istraživanju provedenom u 25 europskih zemalja. „*EU Kids Online* projekt provela je mreža s više od 100 istraživača iz različitih akademskih disciplina, s raznovrsnom metodološkom i stručnom ekspertizom“ (Gorzig, Haddon, Livingstone, 2012: 3). Članovi mreže radili su zajedno kako bi obuhvatili obrise polja, njegove jake strane i nedostatke, te svoje metodološke izazove i prioritete. Na temelju toga osmislili su i proveli upitnik s 25.000 djece koja koriste internet (u 25 zemalja[17] i što više jezika[18]) u dobi od 9 do 16 godina, s kojima su također vodili i intervju.

Ovaj projekt otkriva sličnosti i razlike u istraživanju različitih skupina djece, sličnosti i razlike djece i njihovog ponašanja na internetu u različitim zemljama, razvijenosti korištenja interneta u navedenoj dobi, te rizike i opasnosti koje im donosi korištenje interneta. U ovom slučaju sličnosti omogućuju razmjenu najboljih praksi, dok razlike upozoravaju na uvoz rješenja iz jednog konteksta u drugi. Prema Gorzig, Haddon i Livingstone (2012), projekt *EU Kids Online* polazi od 3 glavne rasprave:

- djetinjstvo u digitalnom svijetu,
- rizik,
- odgovornost.

Nedvojbeno je da se sadašnja generacija djece susreće s novim situacijama koje proizlaze iz tehnoloških promjena. Web-mjesta društvenih mreža postavljaju nova pitanja o društvenim normama koje treba razmotriti. Na društvenim mrežama javljaju se statusi kao *najbolji prijatelji* i opcije brisanja prijatelja. Promjene su evidentne i u procesu učenja kod današnje djece, koji više ne zahtijeva fizički odlazak u knjižnicu, već se bazira na procesima pretraživanja, navigacije i procjenjivanja dostupnih izvora na internetu.

Kako mrežne digitalne tehnologije postaju sve konvergentnije, mobilnije i individualizirane, priroda i značaj promjena u djetinjstvu općenito upućuju manje na tehnologiju, a više na društveno-povijesne promjene. Prema Gorzig, Haddon i Livingstone

[17] Države koje su sudjelovale u projektu u 2010. godini su Austrija, Belgija, Bugarska, Cipar, Češka, Danska, Estonija, Finska, Francuska, Njemačka, Grčka, Mađarska, Irska, Italija, Litva, Nizozemska, Norveška, Poljska, Portugal, Rumunjska, Slovenija, Španjolska, Švedska, Turska i Ujedinjeno Kraljevstvo

[18] Jezici upotrebljavani u projektu: njemački, danski, francuski, bugarski, grčki, češki, estonski, ruski, španjolski, katalonski, finski, mađarski, engleski, talijanski, litvanski, norveški, poljski, portugalski, rumunjski, slovenski, turski, kurdski.

(2012: 4), „pedesetih godina 20. stoljeća pojavila se kultura mladih iz manjih nuklearnih obitelji, rast potrošačke kulture, dugogodišnjeg obrazovanja i pokreti za ljudska prava.“ Važnost dječjih prava, sloboda igranja i istraživanja te izazov autoriteta odraslih oblikovali su naše današnje razumijevanje korištenja interneta. Takvo poimanje također je mobiliziralo društvene resurse za podršku obrazovnim i participativnim perspektivama djece u digitalnom dobu. Čini se da se neke stvari doista mijenjaju u stilovima učenja mladih ljudi i da se načini na koje se znanje predstavlja ili kako učenici vole učiti preoblikuju prema dostupnosti tehnologija.

Međutim, važno je da je vremenski raspon tih promjena duži i daleko varijabilniji. Kontinuitet u iskustvima djece lako se zanemaruje, a u procesima socijalizacije uloge roditelja, nastavnika, susjedstva, prijatelja i kulturne vrijednosti ostaju važni. Glavna pitanja koja zanimaju ovaj projekt orijentirana su prema ispitivanju o tome jesu li djeca zaista više digitalno vješta od svojih roditelja, razlikuje li se to po sociodemografskim faktorima ili po zemljama? Koliko je današnja generacija djece inovativna i kreativna te kako su njihove kreativne aktivnosti ponekad ograničene okolnostima? Druga rasprava koja je okvir ovog projekta odnosi se na konceptualizaciju rizika i opasnosti s fokusom na djecu kao najizloženije skupine internet korisnika.

Drugim riječima, uz prepoznavanje raspona rizika, također se proučava uloga djece i njihovih aktivnosti u suočavanju s tim rizicima. Traže se odgovori na pitanja o tome koji su rizici, odakle dolaze ili kakve posljedice imaju, kakav utjecaj ti rizici imaju i kako djeca reagiraju kada naiđu na rizike?

7.4. Tko treba sudjelovati

Kako mediji ulaze u život djece i tko je odgovoran za reguliranje njihovih potencijalnih rizika ili koristi? Roditelji, nastavnici i mediji, svi imaju zasebno mišljenje. Međutim, uloga roditelja istaknuta je budući da se većina medija koristi unutar kuće. „Strukturne promjene u obiteljskom životu mogu objasniti određene transformacije unutar obiteljske dinamike (od manje do više 'demokratskih' stilova roditeljstva) i objasniti promjene u roditeljskim stilovima posredovanja online aktivnosti“ (Gorzig, Haddon, Livingstone, 2012: 219). Čini se da novi mediji potkopavaju učinkovitost nekih roditeljskih strategija kroz individualizaciju i segmentaciju medijske potrošnje unutar doma. Iako se većina autora slaže da posredovanje kod djece na internetu uključuje neku vrstu napora za upravljanje odnosima djece s medijima, oni se ne slažu u potpunosti o tome koje vrste praksi treba razmatrati i kako ih treba

klasificirati. Većina teorijskih rasprava usredotočena je na roditelje kao primarne uloge koje bi trebale imati najveći utjecaj na ponašanje djece na internetu.

Privatni sektor (posebice u industriji tehnologija i telekomunikacija) ima posebnu odgovornost i jedinstvenu sposobnost oblikovanja utjecaja digitalne tehnologije na djecu. Moć i utjecaj privatnog sektora trebali bi se iskoristiti za unapređenje etičkih standarda vezanih za podatke i privatnost, kao i za unapređenje drugih praksi koje koriste djeci i štite ih na internetu. Vlade mogu promovirati tržišne strategije i poticaje koji potiču inovativnost i konkurenciju među pružateljima usluga kako bi se smanjila cijena usluge povezivanja s internetom, čime bi se omogućio pristup internetu većem broju djece i obitelji, tj. onima koji se nalaze u nepovoljnom položaju zbog za njih preskupe usluge.

Tehnologije i tvrtke koje pružaju internetske usluge trebaju poduzeti korake kako bi spriječile počinitelje da koriste njihove mreže i usluge za prikupljanje i distribuciju slika seksualnog zlostavljanja djece ili da uzrokuju druga kršenja prava djece. Medijske priče o mogućem utjecaju interneta na zdrav razvoj i dobrobit djece trebaju biti utemeljene na empirijskom istraživanju i analizi podataka. Industrija povezana s tvrtkama koje pružaju internetske usluge trebala bi raditi s partnerima kako bi stvorili više lokalno razvijenog i lokalno relevantnog sadržaja, posebno sadržaja za djecu koja govore manjinskim jezicima, žive na udaljenim lokacijama i pripadaju marginaliziranim skupinama.

Postoje brojni razlozi zbog kojih različite zemlje imaju različita očekivanja o tome je li primarna odgovornost osiguranja djece na internetu na vladi, školama ili roditeljima. Mnogi također vide industriju koja pruža sadržaj i usluge s kojima se djeca ponašaju kao odgovornu. Potrebno je osigurati usklađenost između promicanja internetskih mogućnosti te mjere za smanjenje rizika, koje mogu smanjiti pozitivne internetske mogućnosti.

Prema Gorzig, Haddon i Livingstone (2012: 8), „uvjeti o tome kada i kako intervenirati uvelike će ovisiti o tome što djeca sama odluče učiniti putem interneta i kako se nose sa sadržajem na internetu koji smatraju problematičnim, posebice s mogućnošću odlaska na internet na privatnim mjestima ili na mobilnim uređajima, izvan neposrednog vođenja ili zaštite roditelja, učitelja ili čak vršnjaka.“ Odnosno, što su djeca više sposobna za rad, što veću svijest imaju o mogućim opasnostima na internetu, veću otpornost ili pristup online resursima da ih podrže, manje će se trebati uključiti u vođenje ili ograničavanje svoje online aktivnosti.

Podučavanje djece uključuje doprinose oba roditelja i svih uključenih u internetsku industriju. Roditelji imaju primarnu odgovornost za zadovoljavanje potreba za zaštitu djece,

ali u odnosu na poznavanje novih tehnologija, može doći do potencijalnih problema, ako roditelji sami nemaju dovoljno znanja o tome. Koje su najbolje solucije od strane roditelja, koje zaštitne mjere trebaju poduzeti, trebaju li instalirati tzv. roditeljski nadzor i koliko su djelotvorne takve mjere? Sprječavaju li te zaštitne mjere štetu ili imaju upravo suprotan efekt na djecu? Unatoč mogućnosti da bi djeca mogla izbjeći roditeljski autoritet, vlade i industrija preporučuju potonji pristup unatoč činjenici da se to sukobljava sa sklonostima mnogih roditelja da vjeruju svom djetetu i vjeruju u njegovu ili njezinu sposobnost procjenjivanja vlastitih odluka. Budući da su roditelji odgovorni za obrazovanje svoje djece, oni igraju ključnu ulogu u ograničavanju rizika i štete kojoj su djeca izložena. Međutim, većina roditelja očekuje da država, industrija i školstvo sudjeluju u tom procesu, nadajući se da će ih djelomično osloboditi odgovornosti. Prema Gorzig, Haddon i Livingstone (2012), mnogi očekuju od škola da podučavaju djecu o digitalnoj pismenosti, dok se konkretno u Hrvatskom kurikulumu još uvijek ne nalaze teme koje bi usmjerile djecu i adolescente prema sigurnijem korištenju interneta. Uloge nastavnika zbog toga su često vrlo ograničene i to na sljedeći način:

- strukturalno, prema školskim vlastima, nastavnim planovima i programima;
- normativno, gdje moraju jednako tretirati svu djecu i održavati odnose s autoritetima;
- praktično, na temelju nedostatka vremena ili neadekvatne tehnologije.

EU Kids Online projekt dokumentira ograničenu mjeru u kojoj se djeca obraćaju svojim učiteljima ako se nađu pred negativnim iskustvima na internetu. Važno pitanje postaje, pod kojim uvjetima djeca, roditelji i učitelji kao i drugi koji imaju posla s djecom u svakodnevnom životu primaju osnaživanje, podršku i zaštitu? Odnos djeteta s internetom oblikuje više čimbenika. Individualne karakteristike (demografske, psihološke), nacionalni kontekst (socioekonomska stratifikacija, pravni okvir, tehnološka infrastruktura, obrazovni sustav, kulturne vrijednosti) i socijalna medijacija utječu na način na koji djeca koriste internet i time, rizike i mogućnosti koje im pružaju.

U konkretnom slučaju interneta, treba imati na umu da iako dječja uporaba ručnih uređaja raste, kućanstvo je i dalje glavno mjesto pristupa internetu. *EU Kids Online* projekt razlikuje različite vrste strategija roditeljske medijacije:

- posredovanje gdje roditelj dijeli aktivnosti s djetetom;

- aktivno posredovanje, gdje roditelj raspravlja o sadržaju s djetetom (npr. tumači ili kritizira sadržaj);
- restriktivno posredovanje, gdje se koriste pravila koja propisuju ograničenje djetetove uporabe (npr. vremensko ograničenje ili ograničenje aktivnosti);
- nadgledanje, gdje roditelj provjerava dostupne zapise o djetetovim internetskim aktivnostima;
- tehnička ograničenja, gdje se koriste razni softveri za filtriranje, ograničavanje ili praćenje djetetove uporabe (Gorzig, Haddon, Livingstone, 2012).

Sveukupno, svi tipovi medijacije prilično su raširenи među djecom. „Gotovo 90% europske djece izjavilo je da njihovi roditelji provode neku vrstu aktivnog posredovanja u korištenju interneta, 85% djece kaže da roditelji postavljaju neku vrstu ograničenja za korištenje interneta, pa čak i najmanja opsežna vrsta medijacije, nadzor, utječe na 50% djece“ (Gorzig, Haddon, Livingstone, 2012: 221). Posebna značajka *EU Kids online* upitnika je da su roditelji, učitelji i kolege ispitane djece, imali priliku utjecati na online aktivnosti i odabire djece dok su koristila internet. Pretpostavka je da ta tri agenta, zbog različitih društvenih odnosa s djecom igraju različite uloge u utjecaju na dječja iskustva na internetu, pozitivno i negativno.

Roditelji često očekuju od nastavnika da djeluju kao treneri u odnosu na internetsku uporabu svoje djece. Istraživanja pokazuju da se nastavnici uglavnom bave internetskom sigurnošću. Umjesto aktivnog posredovanja, nastavnici imaju tendenciju primjenjivati pravila koja ograničavaju korištenje interneta, koja s druge strane ometaju razvoj dobrih praksi sigurnosti na internetu i djeci smanjuju šanse da istražuju online mogućnosti.

Uloga koju igraju vršnjaci također je važna za oblikovanje online prakse mladih, iako se relativno malo zna o njihovom utjecaju. U usporedbi s roditeljima i učiteljima, vršnjaci su možda manje važni za pomoć vezanu uz korištenje interneta, ali mogu imati značajan utjecaj na motivaciju mladih za odlazak na internet. Vršnjaci su također glavni izvori informacija o novim mogućnostima na internetu. Tako primjerice, najviše utječu na uspostavu profila na društvenim mrežama. Međutim u nekim slučajevima, ovaj pozitivni utjecaj može postati ograničen uobičajenijim pritiskom vršnjaka.

7.5. Kako zaštititi djecu na internetu?

Odgovornost za osnaživanje i zaštitu djece na internetu odnosi se na odgovornost za sigurnost na internetu. Bez oslanjanja na moć, bilo političkih ili ekonomskih interesa, očekuje se raspodjela odgovornosti u svim državnim tijelima, obrazovnim ustanovama, industriji, trećem sektoru, obiteljima i drugima kako bi osnažili i zaštitili djecu na internetu. UNICEF (2017) navodi šest prioritetnih aktivnosti za iskorištavanje moći digitalizacije, a koje pritom trebaju biti od koristi ugroženoj djeci te ograničiti štetu među najugroženijima:

1. osigurati svoj djeci pristup visokokvalitetnim mrežnim resursima;
2. zaštititi djecu od rizika na internetu, uključujući zlostavljanje, eksploataciju, trgovinu, internetsko zlostavljanje i izloženost neprikladnim materijalima;
3. zaštititi privatnost i identitet djeteta na mreži;
4. poučavati digitalnu pismenost kako bi djeca bila informirana, uključena i sigurna na internetu;
5. iskoristiti moć privatnog sektora kako bi se unaprijedili etički standardi i prakse koji štite i unapređuju korištenje interneta kod djece;
6. staviti djecu u središte digitalne politike.

Justament (2017) inzistira da roditelji, kako bi zaštitili djecu, moraju biti informacijski pismeni te da primarno s djetetom dogovore vrijeme korištenja računala. Također, roditelji se moraju pobrinuti da djeca shvate kako internet ne služi samo za zabavu, već i kao sredstvo informiranja i komunikacije. Dijete mora shvatiti kako postoje različite opasnosti i da ne ostavlja osobne podatke na internetu.

Prema Središnjem državnom portalu (2019), u Hrvatskoj postoje zakoni kojima se teži sprječavanju zločina nad djecom putem interneta pa je tako zabranjeno:

- predlaganje susreta djeci mlađoj od 15 godine putem interneta, elektroničke pošte i mobilnih telefona u svrhu stupanja u spolni odnos s djecom;
- prikupljanje, davanje drugima i prijenos podataka o osobama mlađima od 15 godina radi stupanja u spolni odnos;
- iskorištavanje djece za pornografiju, što uključuje i pristupanje takvim sadržajima na internetu i njihovo posjedovanje;
- iznošenje ili prenošenje nečega iz osobnog ili obiteljskog života djece, objavljivanje njihovih fotografija ili otkrivanje njihovog identiteta, što bi kod djece izazvalo

uznemirenost, porugu vršnjaka ili drugih osoba ili na drugi način ugrozilo njihovu dobrobit.

U travnju 2019. godine u organizaciji A1 Hrvatska osmišljen je televizijski oglas za sigurnost djece na internetu, koji je u vrlo kratkom periodu od svega 2 dana dostigao iznimno veliku gledanost (Habek, 2019). Brojni roditelji nisu dovoljno svjesni svega onog što može naškoditi njihovom djetetu, radilo se tu o neprimjerenom sadržaju ili o raznim online predatorima, te često djeci prepuste uređaje i nadaju se da će se sami educirati. To potvrđuje i IPSOS-ovo istraživanje za A1 Hrvatska koje pokazuje da čak 92% roditelja ne koristi aplikaciju za zaštitu djece i njihov siguran pristup internetu, a čak ih 93% ni ne želi koristiti. Istovremeno, prema Habek (2019) kad se ispitane roditelje izložilo internetskim sadržajima od kojih njihovu djecu dijeli nekoliko klikova, većina je odraslih bila negativno iznenađena.

8.

Zaključak

Internet, elektronička pošta, tekstualne poruke, društveni mediji, pametni telefoni, aplikacije, razne tehnologije prožimaju svaki aspekt života ljudi te predstavljaju nusproizvod naših svakodnevnih digitalnih aktivnosti. Aktivnosti kao što su komuniciranje, pronalaženje i dijeljenje informacija i sl. nekoć su se provodile putem analognih medija, a danas se provode digitalno.

Mnogi od nas nisu svjesni posljedica koje online aktivnosti nose sa sobom. Aktivnost u digitalnom okruženju ima utjecaj i na stvarni život, u kojem svatko od nas ima identitet. Slično tome, naš identitet postoji i u digitalnom svijetu. Osobni podaci, naše online ponašanje kao što su slanje poruka, korištenje društvenih medija, e-trgovina, itd., čimbenici su koji oblikuju naš digitalni identitet. Snimljene i arhivirane, ove će aktivnosti biti naša digitalna tetovaža.

Mnoge tražilice i web-lokacije bilježe svaku aktivnost na mreži. Svi korisnici koji su uključeni u online aktivnosti imaju vlastitu digitalnu tetovažu koja postaje njihov identifikator, odnosno dio njegovog digitalnog identiteta. Digitalni identitet ima važniju ulogu od same zaštite informacija, osobni podaci nisu jedino što oblikuje naš digitalni identitet, već to činimo i našim online ponašanjem i aktivnostima koje provodimo na mreži.

Postoje razne metode za dokazivanje vlastitog digitalnog identiteta, odnosno autentifikacije, koje korisnici koriste, poput lozinki, kriptografija javnog ključa, digitalnog potpisa i sl. Takve metode štite nas od mogućnosti krađe identiteta od zlonamjernih napadača koji krađom osobnih podataka žele manipulirati računima žrtava. Digitalni otisci puno govore o vašem digitalnom identitetu, sastoje se od sadržaja kojeg stvorite, postavite i dijelite, kao i sadržaja koji drugi objavljuju i dijele s vama i o vama.

Društvene mreže pokazale su se kao primarno sredstvo ne samo za komunikaciju već i za priopćavanje informacija drugim korisnicima o vama i vašim aktivnostima. Iako većina društvenih mreža nudi različite postavke privatnosti, koje korisnicima omogućuju postavke ograničenja o tome tko vidi njihove osobne podatke, takve postavke imaju nedostatke i često su se pokazale nepouzdanima. Postoje načini kako ukloniti, odnosno barem djelomično izbrisati vaše digitalne otiske, međutim, gotovo je nemoguće u potpunosti izbrisati vašu digitalnu tetovažu.

Djeca, kao najugroženija skupina korisnika interneta, zahtijevaju različite mjere opreza prilikom provođenja svojih online aktivnosti. Ulogu u zaštiti i učenju pravilnog korištenja interneta kao i raspoznavanju mogućih opasnosti koje im prijete imaju roditelji, učitelji,

vršnjaci, vlada kao i industrija koja pruža sadržaj na internetu. Najveću odgovornost dakako imaju roditelji, koji bi trebali biti informatički pismeni kako bi efektivno mogli podučiti svoju djecu kako biti uključeni i sigurni na internetu. Osim toga, posebno je važno da se djetetova okolina pobrine o zaštiti privatnosti i identiteta djeteta na mreži te je potrebno iskoristiti moć privatnog sektora kako bi se unaprijedili etički standardi i prakse koji štite i unapređuju korištenje interneta kod djece.

9. Literatura

1. All about Cookies.org, (2019). URL:https://www.allaboutcookies.org/
2. Araoz, L., (2016). *The golden age of education: Highly effective tools and strategies for educators. Your online presence is a digital tattoo, not a footprint*. URL: https://thegoldenageofeducation.com/2016/03/12/your-online-behavior-is-a-digital-tattoo-not-a-footprint/
3. Bidargaddi, N.; Musiat, P.; Makinen, V.; Ermes, M.; Schrader, G.; Licinio, J., (2016). *Digital footprints: facilitating large-scale environmental psychiatric research in naturalistic settings through data from everyday technologies*. Molecular Psychiatry, 164–169.
4. Brautović, M., (2007). *Zaštita privatnosti kod hrvatskih online medija*, Medijska istraživanja, 51-67.
5. Buckbee, M., (2018). *Data Privacy: Definition, Explanation and Guide*. Varonis. URL: https://www.varonis.com/blog/data-privacy/
6. Büchi, M.; Lutz, C.; Micheli, M., (2018). *Digital footprints: An emerging dimension of digital inequality.* Journal of Information, Communication & Ethics in Society.
7. Büchi, M.; Lutz, C.; Micheli, M., (2017). *Life Online: The Digital Footprint Gap.* Position Paper for the Partnership for Progress on the Digital Divide 2017 International Conference, 24–26 May 2017, San Diego, California, USA.
8. Cambridge Advanced Learner's Dictionary & Thesaurus, (2019). *Definition of "online dating"*. URL: https://dictionary.cambridge.org/dictionary/english/online-dating
9. Camp, L., (2004). *Digital Identity*, IEEE Technology and Society Magazine.
10. CARNet, Hrvatska Akademska i istraživačka mreža, (2005). *Osnovni koncepti upravljanja digitalnim identitetima*. URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2005-08-132.pdf
11. Centar za sigurniji Internet, (2019). *Što je internetsko zlostavljanje?* URL: http://www.sigurnijiinternet.hr/djeca/sto-je-cyberbullying
12. Covell, P.; Gordon, S.; Hochberger, A.; Kovacs, J.; Krikorian, R.; Schneck, M., (1998), *Digital Identity in Cyberspace: White Paper Submitted for 6.805/Law of Cyberspace:*

Social Protocols. URL: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall98-papers/identity/linked-white-paper.html

13. Creative Solutions, (2019). *Brendiranje*. URL: https://creative-solutions.hr/brendiranje/
14. Domo. (2017). *Data Never Sleeps 5.0* | URL: https://www.domo.com/learn/data-never-sleeps5?aid=ogsm072517_1&sf100871281=1
15. FreeCodeCamp, (2018). *Web Tracking: What You Should Know About Your Privacy Online*. URL: https://www.freecodecamp.org/news/what-you-should-know-about-web-tracking-and-how-it-affects-your-online-privacy-42935355525/
16. Gorzig, A.; Haddon, L.; Livingstone, S., (2012). *Children risk and safety on the Internet.* Research and policy challenges in comparative perspective.
17. Habek, I. (2019). *Domaća reklama za sigurnost na internetu u dva dana ima preko 200.000 pogleda*. Srednja.hr. URL: https://www.srednja.hr/zabava/geek-kutak/tech-web/video-domaca-reklama-sigurnost-internetu-dva-dana-200-000-pogleda/
18.
19. Jugkala, F. (2018). *Personalizacija Weba : Život u filter mjehuriću*. Sveučilište u Zagrebu, Filozofski fakultet, odsjek za informacijske i komunikacijske znanosti. URL: http://darhiv.ffzg.unizg.hr/id/eprint/10604/1/Jugkala_zavr%C5%A1ni.pdf
20. Justament, D., (2017). *Zaštita Privatnosti Na Internetu*. Hrvatski Studiji, odjel za Komunikologiju. Sveučilište U Zagrebu. URL: https://repozitorij.unizg.hr/islandora/object/hrstud:1036/preview
21. Khanse, A., (2013). *Different types of Internet Cookies*. The Windows Club. URL: https://www.thewindowsclub.com/types-of-internet-cookies
22. Khanse, A., (2014*). What are Digital Footprints and how to stay safe?* The Windows Club. URL: https://www.thewindowsclub.com/remove-digital-footprints-traces
23. Kovačević, V., (2010). *Zaštita podataka primenom kriptografskih metoda*. Elektronski fakultet, Univerzitet u Nišu. URL: http://es.elfak.ni.ac.rs/Papers/Zastita%20podataka.pdf
24. Lapaine,M., Tutić, D. *GPS za početnike*. URL: http://www.kartografija.hr/old_hkd/obrazovanje/prirucnici/gpspoc/gpspoc.htm
25. McPeak , A., (2013). *The facebook digital footprint: Paving fair and consistent pathways to Civil discovery of social media data*. 48 Wake Forest L. Rev. 887. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2246990##

26. Medenjak, I., (2008). *Sustav za web autentifikaciju*, diplomski rad. Fakultet elektotehnike i računarstva, Sveučilišta u Zagrebu. URL: http://sigurnost.zemris.fer.hr/ns/websec/2008_medenjak/Diplomski%20rad%201753.htm#_Toc208387022
27. MojFaks.com, (2019). *Portal za studente: X-ica*. URL: www.mojfaks.com/x-ica
28. Ponderings, (2015). *About elt, languages, learning design, and digital education. Digital footprint, digital tattoo, or digital immortality*. URL: https://yvetteinmb.com/2015/01/31/digital-footprint-digital-tattoo-or-digital-immortality/
29. Raul Walter, (2019). *Government Services, Digital IdentityManagement*. URL: https://www.raulwalter.com/government/digital-identity-management/
30. Sadler, A., (2017). *How to reduce, or even erase, your digital footprint*. Clark Howard Inc. URL: https://clark.com/technology/how-to-reduce-or-delete-your-digital-footprint/
31. Schurgin O'Keeffe, G.; Clarke-Pearson, K., (2011). *Clinical Report: The Impact of Social Media on Children, Adolescents, and Families.* Pediatrics April 2011, voL. 127 / 4. American Academy of Pediatrics. URL: https://pediatrics.aappublications.org/content/127/4/800
32. Setyowati , L., (2016). *Digital life, digital tattoo and the filter bubble: raising the awareness and the cautions on online activities through information literacy education*. Faculty of Engineering, Diponegoro University.
33. Središnji državni portal, (2019), *Zaštita djece na internetu*. URL: https://gov.hr/print.aspx?id=1649&url=print
34. Statista, (2019a), *The Statistics Portal: Global social networks ranked by number of users*. URL: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
35. Statista, (2019b), *The Statistics Portal: Number of monthly active facebook users worldwide*. URL: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/
36. Statista, (2019c), *The Statistics Portal: Number of monthly active Instagram users from January 2013 to June 2018 (in millions).* URL:https://www.statista.com/statistics/253577/number-of-monthly-active-instagram-users/

37. Statista, (2019d), *The Statistics Portal: Number of worldwide social network users*. URL: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/
38. TeleWare: Think Beyond, (2015). *Your digital tattoo*. URL: https://www.teleware.com/what-does-your-digital-tattoo-look-like/
39. The Digital Tattoo Project, (2019). University of British Columbia, Vancouver Campus. URL: https://digitaltattoo.ubc.ca/
40. Treyvaud, R., (2018). *What Is A Digital Tattoo & Why Does It Matter? Family Insights, Kepping your family safe Online*. URL: https://familyinsights.net/advice/what-is-a-digital-tattoo-and-why-does-it-matter/
41. UNICEF (2017). *Stanje djece u svijetu 2017. − Djeca u digitalnom svijetu*. UNICEF, Odjel za komunikacije 3, Ujedinjeni narodi, Plaza New York, NY 10017, SA. URL: https://www.unicef.hr/wp-content/uploads/2015/09/Izvjestaj-HR_12-17_web.pdf
42. Živković, Š. (2016). *Imef: Što je to rudarenje podataka (eng. Data mining)*. URL: http://imef.hr/sto-to-rudarenje-podataka-eng-data-mining/

Sažetak

U ovom diplomskom radu prikazani su rezultati istraživanja o digitalnim otiscima i digitalnim tetovažama s posebnim naglaskom na ostavljanje digitalnih tragova kod djece predškolske dobi. Svrha i cilj ovog rada bili su definiranje ključnih pojmova koji ulaze u okvir digitalnog ostavljanja tragova na internetu, posebice na društvenim mrežama; ukazivanje na posljedice ostavljanja tragova online te istraživanje i detaljno iznošenje zaključaka o zaštiti osobnih podataka na internetu, s posebnim osvrtom na djecu predškolske dobi kao najviše izložene skupine korisnika.

Ključne riječi: *digitalni otisak, digitalna tetovaža, digitalni identitet, društvene mreže, zaštita podataka.*

Digital footprints and digital tattoos

Abstract

This thesis is showing the results of the research on digital footprints and digital tattoos with special emphasis on leaving digital records in pre-school children. The purpose and main goal of this paper is to define the keywords that mark the digital tracing on the Internet, especially on social networks; point to the consequences of leaving traces online and explore and elaborate the conclusions on the protection of personal data on the Internet, with particular reference to pre-school children as the most exposed group of users.

Key words: *digital footprint, digital tattoo, digital identity, social networks, data protection.*