Privatnost korisnika na internetu

Kranjec, Ana

Sveučilište u Zagrebu

Filozofski fakultet

Odsjek za sociologiju

Ana Kranjec

Privatnost korisnika na internetu

Diplomski rad

Mentor: red. prof. dr.sc. Krunoslav Nikodem

Zagreb, 2021.

Sadržaj

UVOD

Osnivanjem interneta 1969. godine od strane Američkog ministarstva obrane počinje razvijanje novog načina života koji vrhunac dostiže 90-ih godina prošlog stoljeća te postaje digitalni život. Kroz nadolazeće godine internet i tehnologija su napredovali, a njihovi korisnici su se prilagodili novim obrascima ponašanja. Modernizacijom industrijskog društva mijenja se shvaćanje proizvodnje i potrošnje te se stavlja naglasak na hedonistički način života. Pa tako razvijanje interneta pogoduje i razvitku potrošačke kulture u Zapadnom društvu. Danas je gotovo nemoguće zamisliti život bez interneta. Iako uvelike olakšava svakodnevni život pojedinca, uz to donosi i niz negativnih posljedica, a jedna od ozbiljnijih je kršenje privatnosti korisnika.

Pravo na privatnost je jedno od temeljnih ljudskih prava i zajamčeno je Ustavom Republike Hrvatske koji nalaže da „zaštita privatnosti mora biti osigurana svakoj osobi bez obzira na državljanstvo i prebivalište, neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili osobinama“. Kada je riječ o digitalnoj privatnosti, ona podrazumijeva zaštitu osobnih podataka, odnosno osnovnih ljudskih prava u virtualnoj stvarnosti koju internet obuhvaća. Ipak, digitalna privatnost sukladno s razvojem internetske kulture poprima druge dimenzije i postavlja se pitanje trajne održivosti te privatnosti. Kroz godine digitalna privatnost postaje važno pitanje u područjima sociologije, psihologije, filozofije i prava. Problemi oko privatnosti na internetu nastaju jer je razlika između privatnog i javnog u stvarnom svijetu vrlo jasna, a u online svijetu dolazi do zamagljenja tih granica. Anonimnost na internetu je skoro pa nemoguća u današnje vrijeme jer se sve osobne informacije mogu pretraživati i iskoristiti bez znanja korisnika, no svaka web stranica posjeduje postavke privatnosti u kojima je djelomično moguće upravljati dijeljenjem svojih podataka. Iako nekim korisnicima interneta podaci

koje ostavljaju na njemu ne predstavljaju ni problem ni priliku, drugim stranama odnosno pružateljima usluga pružaju upravo to, priliku, to jest mogućnost zarade. Najčešći odgovor koji se očekuje od ispitanika glasi „Svejedno mi je, nemam što skrivati“, odnosno da korisnici nisu pretjerano zabrinuti. Kao što je rekao Edward Snowden, bivši zaposlenik CIA-e i Nacionalne službe sigurnosti SAD-a, na premijeri svog biografskog filma „Tvrditi da vam nije stalo do prava na privatnost jer nemate što skrivati nije ništa drugačije od toga da kažete da vam nije stalo do slobode govora jer nemate što reći“. [1] S obzirom da je internet neizostavni dio današnjeg života od velike je važnosti upozoriti i osvijestiti korisnike, no da bi to bilo moguće potrebno je saznati njihove stavove i mišljenja. Stoga, cilj ovog rada je uvidjeti u kojem smjeru ide briga korisnika interneta o njihovim podacima i zaštiti istih.

U svrhu ovog rada je provedeno kvalitativno istraživanje o shvaćanju privatnosti na internetu, dozvoljavanju „kolačića“, personaliziranim reklamama, zlouporabi podataka i svjesnosti o tome. Ispitanici su od 15 do 50 godina starosti te su svakodnevni korisnici interneta i društvenih mreža te različitih geografskih područja. Iz toga će se u raspravi izvući odgovarajući zaključci.

PRIVATNOST I ZAŠTITA PODATAKA

Internet svojim stalnim razvojem i napretkom postaje vrlo dostupan građanstvu, kako u pogledu pristupa tako i cjenovno. 2007. godine je zabilježeno da većina (55%) kućanstava u EU-28 ima pristup internetu, to predstavlja prekretnicu i već 2008. godine internet bilježi 1,463 milijarde korisnika.[2] Razliku između pojma privatnosti na internetu i u stvarnom svijetu dobro objašnjava Waldman u svojoj knjizi „Privatnost kao povjerenje - privatnost podataka u informacijskom dobu“. Ari Ezra Waldman (2018:2) objašnjava kako smo navikli shvaćati privatnost na određene načine. Često

[1] Edward Snowden upravo je iznio strastveni argument zašto je privatnost najvažnije pravo. https://www.businessinsider.com/edward-snowden-privacy-argument-2016-9

[2] Statistički podaci o informacijskom društvu – kućanstva i pojedinci. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:Statisti%C4%8Dki_podaci_o_informacijskom_dru%C5%A1tvu_%E2%80%93_ku%C4%87anstva_i_pojedinci&oldid=216793

mislimo da je privatnost odvajanje od znatiželjnih pogleda drugih ili zadržavanje stvari u tajnosti; zato spuštamo rolete kada ne želimo da ljudi gledaju. Ponekad privatnost povezujemo s određenim prostorima ili imovinom; što radimo "u privatnosti vlastitih domova" ili "iza zatvorenih vrata“. Privatnost je povezana i s intimnošću, to je ono što čini teme poput seksa i novca osobno. Ali autor tvrdi da takvo razmišljanje ograničava naše razumijevanje privatnosti. Jer se pojam privatnosti razlikuje u stvarnom i online svijetu. Argumenti poput „nemam što sakriti“ nastaju jer se ne razumije priroda privatnosti. Privatnost se ne svodi samo na „loše“ stvari i ne radi se o „skrivanju“ koliko o autonomiji i određenom stupnju kontrole. Često su najprivatnije stvari najdragocjenije i najintimnije, a ne vrste mračnih tajni ili loših priča koje ta logika pretpostavlja. Ako privatnost shvaćamo samo kao koncept koji se koristi u stvarnom svijetu, naša digitalna privatnost će polako nestati i svi naši podaci će biti dostupni svima koji to požele. Stoga se privatnost na internetu definira kao sposobnost kontroliranja podataka koje netko o sebi otkriva putem interneta i nadzora nad tim tko može pristupiti navedenim podacima. Mnogi autori poput stručnjaka za odnose s javnošću Scotta Robertsona tvrde da je „privatnost iluzija", pišući o promjenama u konceptu privatnosti u eri interneta, "privatnost je mrtva" (Currie, 2013:9). Mark Zuckberg, osnivač Facebook-a, rekao je da je „doba privatnosti prošlo“. Thomas Friedman je 2014. godine u New York Times-u napisao je da je „privatnost nestala“. Toliko dugo se govori o tome da je privatnost nepostojeća, a velik broj korisnika i dalje svakodnevno upotrebljava internet i društvene mreže. Dakle, i dalje smatraju da privatnost postoji te ju štite ili ju zanemaruju. Zaštita privatnosti i podataka postaje globalni izazov, koji premašuje lokalne ili stručne razine. Razvoj interneta i novih tehnologija koje omogućuju brzu i efikasnu komunikaciju velikog broja korisnika i razmjenu velike količine različitih podataka u digitalnom svijetu počinju izazivati nesigurnost u korisnicima. Novonastale tehnologije kao što su Internet stvari (IoT), umjetna inteligencija (AI) i „Veliki podaci“ (Big Data) otvaraju nove mogućnosti ili ugroze upravljanja i obrade velikih količina podataka. Nije riječ samo o osobnim podacima, već i o podacima o načinu života, navikama, preferencijama, okolini i tako dalje. Prvu definiciju Velikih podataka navodi Didebold (2000) koji govori da je „U zadnje vrijeme dosta dobre znanosti, bez obzira je li u pitanju fizika, biologija ili sociologija, bilo prisiljeno suočiti se – od čega je često i profitirala –

s fenomenom Velikih podataka. Veliki podatci odnose se na eksploziju u količini (a katkad i kvaliteti) dostupnih i potencijalno relevantnih podataka, uglavnom kao posljedica skorih i besprimjerenih napredaka u tehnologiji zapisivanja i pohranjivanja podataka“. Dakle, Veliki podaci je tehnologija koja prikuplja velike količine podataka, ali njezina moć je zapravo u sposobnosti da te podatke obradi i analizira te pohranjuje za daljnju upotrebu. “Veliki se podatci obično opisuju služeći se pojmom 3V-a koji se odnosi na volumen (velika količina podataka), varijantnost (raznolikost tipova podataka: tradicionalne baze podataka, fotografije, dokumenti) i velocitet tj. brzinu kojom se akumuliraju novi podatci (iz sličnih izvora podataka, iz prethodno arhiviranih podataka, iz podataka koji stalno pridolaze iz različitih izvora – streamed data), ali i brzina kojom se očekuje da pristigli podatci budu dostupni za analizu“ (Kocijan, 2014:3). No, Paul Bernal u svojoj knjizi iz 2020. godine„Što znamo i što bismo trebali učiniti u vezi privatnosti na Internetu?“ (2020:33) tvrdi da napetost između Velikih podataka i privatnosti ima dvije glavne dimenzije. Prva, prikupljanje podataka koji će se uključiti u skupove Velikih podataka vjerojatno će samo po sebi biti u sukobu s privatnošću. Te druga, uvidi koji se mogu steći analizom Velikih podataka također mogu predstavljati narušavanje privatnosti. Na primjer, ako analiza kupovnih navika otkrije vezu između kupnje određenog proizvoda i zauzimanja određenog političkog stajališta, tada bi, upotreba te veze za zaključivanje neizgovorenih političkih mišljenja pojedinca uvidom u njihove kupovne navike zapravo bila narušavanje privatnosti. Internet stvari (Internet of Things) je tehnologija koja povezuje uređaje poput satova, zvučnika, vozila i drugih stvari, koje prikupljaju i razmjenjuju podatke putem interneta. Spajanje tih uređaja može biti bežično ili žično te omogućuje sasvim nove mogućnosti za uzajamnu interakciju (komunikaciju) između ljudi i različitih sustava, odnosno uređaja. Na takav način mogu komunicirati sustavi, uređaji i sustavi/uređaji s ljudima, uz opći cilj olakšavanja i pojednostavljivanja života ljudi.[3] Bernal govori da takvi uređaji ugrožavaju privatnost na najmanje dva značajna načina. Prvi je putem različitih senzora, od kojih mnogi moraju biti uvijek uključeni. Glasovno aktivirani uređaji imat će uvijek uključene mikrofone ako ih se po

[3] Koliko nam IoT pomaže, ali i mijenja svakodnevicu, Službene internetske stranice Europske unije, 2021, https://ec.europa.eu/croatia/How_IoT_is_helping_and_changing_our_everyday_life_hr

zahtjevu mora uključiti. Sustavi opremljeni kamerom također mogu uvijek biti uključeni ili se mogu aktivirati češće nego što korisnici zapravo shvaćaju. To ima očit utjecaj na privatnost, instaliranje pametnog zvučnika aktiviranog glasom znači instaliranje uređaja koji stalno sluša u vašoj dnevnoj sobi, na primjer. Drugi utjecaj na privatnost je kroz podatke. Ne samo da instalirate sustav senzora, već također instalirate sustav za samoprofiliranje i dopuštate da se vaš profil koristi u korist onih od kojih ste kupili svoj pametni uređaj. Internet stvari također generira podatke o lokaciji. Budući da svaki uređaj fizički postoji, ima i fizičku lokaciju. Često je to fizičko mjesto ključno za način rada uređaja: zvono na vratima, sustav grijanja, automobila i tako dalje. Postoji cijela vrsta internetskih uređaja koji rade izravno s zdravstvenim podacima, različiti nosivi predmeti poput pametnih narukvica (Fitbitova). Dok neki uređaju posjeduju i zdravstvene i lokacijske podatke s prethodno navedenim značajkama.
Miller (2003:266) pojašnjava kako se virtualni svijet u nekim segmentima ne razlikuje previše od stvarnog svijeta. Na primjer, kupujete li preko trgovačkog kataloga ili preko online trgovine, u oba slučaja vaši će podaci, poput imena i prezimena, adrese ili broja telefona, ostati zabilježeni u njihovoj bazi podataka. Mnoge kompanije prodaju osobne podatke drugim kompanijama pa tako kupci često završe s raznolikom neželjenom poštom, kako u poštanskom sandučiću, tako i na e-mailu. S druge strane, podaci mogu biti i ukradeni na virtualnom putu od računala do njihovog odredišta ili iz baza podataka web stranica i trgovačkih kompanija. Agencija za zaštitu osobnih podataka[4] pojašnjava da se osobni podaci u nekim slučajevima zloupotrebljavaju za počinjenje kaznenih djela, poput prijevare ili u svrhu sklapanja lažnih ugovora. S današnjom tehnologijom, praćenje na internetu može se usporediti s praćenjem u stvarnom svijetu. Internetski preglednici spremaju male datoteke pod nazivom „kolačići“ (*cookies*) na računalo pri posjetu pojedinim web stranicama. Ti „kolačići“ sadrže podatke za prijavu korisničkom računu ili ključne informacije kao na primjer osobne podatke, povijest pretraživanja ili artikle u košaricama internetskih trgovina (Miller, 2003:268). „Kolačići“ su male tekstualne datoteke koje internetska stranica putem vašeg internetskog preglednika pohranjuje na vašem računalu ili mobilnom uređaju. „Kolačići“ se posvuda upotrebljavaju za

[4] Što je krađa identiteta?, Agencija za zaštitu osobnih podataka, u daljnjem tekstu AZOP http://azop.hr/aktualno/detaljnije/kradaidentiteta-i-kako-se-zastititi

spremanje vaših preferencija kako bi internetske stranice radile učinkovitije. Upotrebljavaju se i za praćenje vaše uporabe interneta i izradu korisničkih profila, a potom za prikaz prilagođenih internetskih oglasa na temelju vaših preferencija.

Zahvaljujući „kolačićima“, navodi Miller (2003:269), online trgovine kroje personalizirane oglase i usluge ciljajući na interese kupaca, odnosno njihovu povijest pretraživanja određene kategorije proizvoda. Mato Brautović u svome radu „Zaštita privatnosti kod hrvatskih online medija“ (2007:28) nadodaje da se „kolačići“ također upotrebljavaju kako bi online mediji, bilježeći ponašanje i interese, skupili što veći broj korisnika, pa tako bili zanimljiviji oglašivačima.

Brautović također navodi „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“ (2007:28). Kako bi korištenje usluga internetskih tražilica i društvenih mreža bilo što sigurnije, važno je ne zaboraviti da sve što se putem njih objavi može u nekom trenutku postati javno, a time i dostupno svakome. „Bit je da se ne možete osloniti na web stranicu da vodi brigu o vašoj privatnosti. Ustvari, možete očekivati da će mnoge web stranice namjerno koristiti podatke koje imaju o vama. Oni paze na svoje poslovanje, a ne na vašu privatnost. […] Na kraju, jedina sigurna zaštita privatnosti je vaš razum i samodisciplina“, zaključuje Miller (2003:274).
Paul Bernal govori kako je privatnost ponekad opisivana kao svojevrsna povijesna anomalija, trenutna popustljivost. Nismo ju imali u prošlosti niti ćemo ju imati u budućnosti. Želimo ju tek sada jer su nam sve ostale bitne stavke uvedene u red. Ova logika sugerira da nisu imali privatnost u srednjem vijeku, a kamoli još ranije. Isto tako, često se sugerira da privatnost neće postojati u budućnosti - ili da je već mrtva, bilo da ju je ubila tehnologija ili da su je napustile nove generacije. Mark Zuckerberg, glavni osnivač Facebooka, predložio je 2010. godine da privatnost više nije društvena norma, da je trebamo napustiti i iskoristiti prilike koje bi njezino napuštanje moglo pružiti. Prema ovakvom pogledu, privatnost doista nije toliko važna, a mi smo je ionako izgubili, pa bismo trebali prihvatiti novo okruženje bez privatnosti. No, to baš i

nije tako. Privatnost nije luksuz ili popustljivost niti je „individualna“ u bilo kojem stvarnom smislu. Novinarima je potrebna privatnost za izvore, a za intimnu vezu potrebna je privatnost da bi uopće funkcionirala. Sigurnosne i obavještajne službe same se oslanjaju na privatnost i povjerljivost u obavljanju svog posla. Poduzećima je za rad potrebna povjerljivost informacija. Bez privatnosti sve su te stvari besmislene.

TRGOVANJE PODACIMA – SLUČAJ *CAMBRIDGE ANALYTICA*

U ovom poglavlju se govori o trgovanju podacima, to jest o tome kako postoje legalne i dozvoljene tvrtke koje se time bave. No, razvojem tehnologije dolazi do zlouporabe i neovlaštenog korištenja podataka od raznih strana. Najpoznatiji slučaj je *Facebook – Cambridge Analytica* o kojem se govori nešto kasnije u tekstu.

Kako navodi autorica Kristina Kocijan „Zadnjih godina osnovale su se razne tvrtke koje omogućavaju trgovanje podatcima kao na primjer: *DataMarket* (Island) – od 2008. omogućava pristup besplatnim bazama podataka iz različitih izvora (Ujedinjeni narodi, Svjetska banka, Eurostat) i zarađuje na postocima preprodaje podataka marketinškim tvrtkama.

Factual – omogućava pristup velikim bazama za čije je kompajliranje potrebno više vremena.

Windows Azure Marketplace – prodaje podatke (dajući pritom prednost visoko-kvalitetnim podatcima).

Tvrka *Import.io* - savjetuje licenciranje podataka kako ih drugi ne bi mogli samo besplatno prikupiti s mreže“ (2014:8).

Najveći skandal nezakonitog trgovanja, odnosno neovlaštenog korištenja podacima jest *Facebook – Cambridge Analytica*. *Cambridge Analytica Ltd* (CA) je bila britanska tvrtka za političko savjetovanje koja je osnovana 2013. godine kao podružnica privatne obavještajne tvrtke i samoopisana "globalna agencija za upravljanje izborima". Prvenstveno su se koristili „Velikim podacima“, odnosno prikupljali su velike količine podataka, obrađivali ih, analizirali i koristili u

marketinškim kampanjama. Empirijsko istraživanje uloge Facebooka, Twittera, Googlea i Microsofta na predsjedničkim izborima 2016. pokazalo je aktivnu suradnju između osoblja u tvrtkama i u političkim kampanjama. Istraživači su primijetili da su tehnološke tvrtke motivirane za rad u političkom prostoru radi marketinga, prihoda od oglašavanja i izgradnje odnosa u službi lobističkih napora te da predstavnici u tim tvrtkama služe kao kvazi-digitalni konzultanti za kampanje, oblikujući digitalnu strategiju, sadržaj i izvršenje (Kreiss i McGregor, 2018). Ovakve suradnje imaju prednosti i za tvrtke i za političke kampanje, ali potencijalno vrlo značajne implikacije na ljudsku autonomiju i integritet političkog procesa. Nakon što je 2017. godine objavljeno da je CA uzimala osobne podatke korisnika Facebooka te da im je Facebook to dopustio, dolazi do skandala u kojem bivši zaposlenici tvrtke iznose sve činjenice i tajne u javnost. Otkriveno je kako su analitičari koristili podatke ilegalno pribavljene od Facebooka, stvarali profile milijuna korisnika, te ih koristili za ciljano oglašavanje i manipulaciju javnim mnijenjem. Tako su utjecali na izbore u mnogim državama svijeta, a zbog izbijanja ovog skandala cijeli je slučaj završio i na sudu. Facebook je nakon toga uveo nove postavke privatnosti te je korisnicima postalo transparentnije s kojim aplikacijama surađuju. Mark Zuckerberg je na saslušanju izjavio da Facebook ne prikuplja podatke s mobitela svojih korisnika putem mikrofona i da ne prodaje podatke oglašivačima (već ih samo koristi za ciljano pozicioniranje oglasa). Tvrtka CA je zatvorila poslovanje 2018. godine zbog tog skandala s podacima. Već 2019. godine izlazi dokumentarni film naziva „*The Great Hack*“ koji se bavi upravo ovim skandalom, pokušavajući društvu prikazati kako se sve može upravljati podacima i što se njima sve može postići.

KREIRANJE PERSONALIZIRANIH OGLASA I REKLAMA

„Mnoge od najvećih svjetskih kompanija u stvari su internetske tvrtke - ne samo Google i Facebook, već Amazon, Apple i Microsoft, a u Kini Tencent i Alibaba. Internet zahvaća svu našu tehnologiju - ne samo komunikaciju i izvore informacija, već i automobile, energiju i grijanje, televizore i glazbu. Naši kalendari su online, kondicija se prati online, kupujemo, pronalazimo poslove i

izlazimo na internetu. Putovanja i zabavu rezerviramo putem interneta. Teško je pronaći dio našeg života koji nema značajnog internet elementa. Zbog prirode interneta to znači da ostavljamo trag, zapis o svojim postupcima, u obliku podataka. Ti se podaci po svojoj prirodi mogu koristiti za analizu, profiliranje, skupljanje, stvaranje više podataka i za predviđanje više potencijalnih informacija o gotovo svemu. Iz perspektive privatnosti to je važno jer znači da su informacije dostupne putem naših veza i radnji na internetu te se mogu koristiti za otkrivanje ogromne količine informacija o nama na razne načine“ (Bernal, 2020:3).

Ciljani marketing ima za ulogu određivanje segmenta ili dijela tržišta kojem ćete se obratiti. On prema Philipu Kotleru, ima tri glavne faze:
1. segmentacija tržišta koja podrazumijeva podjelu tržišta u različite grupe kupaca koji bi mogli zahtijevati posebne proizvode i/ili usluge;

2. izbor ciljanog tržišta koji podrazumijeva procjenu i odabir jednog ili više tržišnih segmenata u koje će se ući;

3. pozicioniranje proizvoda koje podrazumijeva formuliranje konkurentnog pozicioniranja određenog proizvoda i/ili usluge za svako pojedino ciljno tržište.

Osnovna pretpostavka ciljanog marketinga jest da je potražnja za određenim proizvodom raznolika. Različite grupe kupaca od istog proizvoda i/ili usluge očekuju različite koristi odnosno zadovoljenje različitih potreba i želja. Stoga, autori knjige „Sigurnost i privatnost sljedeće generacije bežične mreže“ objašnjavaju „Društvene mreže privlače veliki broj korisnika, a podaci društvenih mreža sadrže osjetljive podatke korisnika, poput društvenih odnosa, društvenih navika i osobnih podataka, koje mogu iskopati istraživači treće strane, što može dovesti do rizika otkrivanja privatnosti korisnika. Podaci društvenih mreža uglavnom se pohranjuju u obliku grafikona. Uobičajena metoda zaštite privatnosti podataka društvenih mreža je jednostavna anonimnost, odnosno anonimna obrada vrha (korisnika) u grafu društvenih mreža“ (Zhong, S. i H., Yang, X., Shi, J., Xie, L., Wang, K, 2019:40). Dakle, društvene su mreže izvrsna podloga za ciljani marketing i personalizirane oglase i reklame. No, Google je prvi počeo iskorištavati mogućnost zarade. Kako tvrdi

Paul Bernal (2020:21) pojmovi za pretraživanje prikupljaju se i analiziraju kako bi se znalo koliko ljudi traži što - i, u konačnici, koji ljudi traže što - i zatim koje veze slijede. Time Google ne prikazuje samo ono što je na internetu - web stranice - već i ljude na internetu, njihovo ponašanje, njihove navike i još mnogo toga. Koji su se podaci točno prikupljali promijenilo se tijekom godina kako se tehnologija razvijala, a mogućnosti su rasle. Podaci se prikupljaju na način koji nije jasan za korisnika. Googleovo sučelje vrlo je jednostavno: gotovo prazna stranica s jednim okvirom u sredini za unos pojma za pretraživanje. Ništa ne govori da se prikupljaju podaci, da se generira dnevnik pojmova za pretraživanje, povijest pretraživanja, da se profilira korisnik. Google nije započeo ovu vrstu profiliranja, već je na njemu izgradio poslovni model i iz temelja promijenio prirodu interneta. Googleov poslovni model koristio je ovo profiliranje za ciljano oglašavanje, koje je okruživalo rezultate pretraživanja. To je preraslo u oglašivački posao koji nije dominirao samo u mrežnom oglašavanju, već u cijelom oglašavanju. Spektakularan uspjeh ovog modela oglašavanja ovisio je prvenstveno o dvije stvari. Prije svega, pružanje usluge koja je doista radila i zadovoljavala potrebe korisnika. Drugo, o sposobnosti dovoljno preciznog ciljanja kako bi se zadovoljile potrebe oglašivača, a to je ovisilo o kvaliteti profiliranja. To je pak ovisilo o količini i kvaliteti prikupljenih podataka i sposobnosti analize tih podataka. Google je to učinio na način na koji nitko nikada prije nije pokušao, koristeći prednost same prirode interneta i ljudi koji ga koriste, odnosno korisnika. Personalizacija je odgovorna za neuspjeh u zaštiti osobnih podataka. Proizvod ili usluga mogli bi se ponuditi po različitim cijenama različitim korisnicima. Sustav profiliranja će predložiti, odnosno pretpostaviti, korisniku najvišu cijenu po kojoj bi on bio spreman platiti određeni proizvod ili uslugu. Zahvaljujući tome, možemo primijetiti da proizvodi koji su nam potrebni i koje pretražujemo će biti skuplji dok će proizvodi koji nam ne trebaju biti jeftiniji i personaliziraniji na temelju našeg profila kako bi se povećala vjerojatnost da ih kupimo. Proizvodi ili usluge koje bi nam možda bolje odgovarali, ali su jeftiniji, mogu biti skriveni od nas. Mogućnosti su beskrajne. Tako je Google brzo počeo dominirati poslovima pretraživanja s više od 90% svjetskog tržišta pretraživanja (osim Kine).
Ključ za razvoj Facebooka kao najpopularnije društvene mreže je isto tako bilo profiliranje, tvrdi Paul Bernal. Facebook je tome dodao i svoju posebnu crtu, te

je natjerao ljude da se sami profiliraju. Tamo gdje je Google to učinio prikriveno, profilirajući korisnike na temelju onoga što su tražili, Facebook je većinu toga radio otvoreno, uvjeravajući korisnike da unesu svoje osobne podatke, ukuse, navike i još mnogo toga. Facebook je također radio prikriveno: neke od najranijih aplikacija na Facebooku uključivale su kvizove i igre u kojima su korisnici unosili pojedinosti kako bi vidjeli kojoj slavnoj osobi najviše nalikuju, koja životinja bi mogla biti njihova duhovna životinja i tako dalje. Izgledali su kao igre, ali svrha im je bila prikupljanje podataka i samoprofiliranje. Drugi ključni izvor podataka bila je društvena karta. S kim su bili prijatelji. S kim su komunicirali i kako. S kim su vaši prijatelji komunicirali. Kakvi su vam prijatelji bili zajednički. Kako su izgledali svi njihovi profili. Ono što vam se svidjelo - i u stvarnom i u Facebook životu. Razine i bogatstvo ovih podataka imali su ogroman potencijal i ako u početku nije bilo jasno kako će Facebook zaraditi novac, bilo je jasno da će zaraditi. Ideja da bi podaci, profiliranje, društvene karte i sve ostale veze bile vrijedne i da bi Facebooku omogućile zaradu bila je uvjerljiva i model koji se slijedi čak i ako se detalji tek trebaju razraditi. To je samo po sebi imalo ogromne implikacije na privatnost jer je poticalo sve više prikupljanja podataka, često spekulativnih. Nakon što se prikupe podaci, bilo koje poduzeće prirodno bi tražilo načine za korištenje tih podataka - što je opet imalo velike posljedice za privatnost. Manipulacija je bit većine oglašavanja, odnosno uvjeravanje korisnika da donesu odluke koje inače možda ne bi donijeli, na primjer da kupe nešto što inače ne bi kupili ili da izaberu jedan brend umjesto drugog. Ono što internet čini ili barem ima potencijal, jest učiniti ovo profiliranje i personalizaciju još učinkovitijim i izravnijim. To nije nešto sasvim novo, ali to ne znači da ne bi trebali brinuti o tome. Jačanje takvog načina marketinga koje internet pruža starim tehnikama znači da ga treba shvatiti mnogo ozbiljnije.

VRSTE ZAŠTITE PRIVATNOSTI I PODATAKA

Kao što je prethodno već spomenuto, jedina sigurna zaštita privatnosti i podataka je razum i samodisciplina korisnika interneta. Michael Miller (2003:287) navodi nekoliko preporuka kojih bi se trebali pridržavati korisnici

interneta, a to su da se osobni podaci ne bi smjeli otkrivati putem interneta, na neželjenu poštu nikada se ne bi trebalo odgovarati, postaviti internetski pretraživač tako da ne prima „kolačiće“ bez prethodnog upita, uvjeti privatnosti internetskih stranica trebali bi se proučiti, a reklamne ponude odbijati, koristiti uslugu virtualne privatne mreže (VPN) kako bi se osigurala potpuna anonimnost i tako dalje. S obzirom na ubrzani način života i jednostavnost upotrebe razvijene su mnoge tehnologije koje se trude zaštititi taj dio digitalnog života umjesto da korisnici to rade sami. Cynthia J. Alexander i Leslie A. Pal (2001:200) navode dva primjera tehnologija zaštite privatnosti. Jedan od njih je „slijepi potpis“, odnosno elektronički ekvivalent vlastoručnog potpisa. On služi kao verifikacija vjerodostojnosti elektroničke transakcije te osigurava pošiljatelju anonimnost. Druga tehnologija zaštite privatnosti je biometrijsko šifriranje. Biometrijska mjerenja su najsigurniji dokaz nečijeg identiteta zato što nude biološki dokaz vezan uz točno određenu osobu. „Bioskript“ je metoda biometrijskog šifriranja otisaka prstiju kojom se identitet korisnika utvrđuje, ali ne i otkriva. Najčešći oblik biometrijskog mjerenja je metoda uzimanja otisaka prstiju. Otisak prsta se ne pohranjuje jer „bioskript“ ne sadrži niti jedan podatak, sliku ili šablonu pojedinčeva otiska. Umjesto toga, u njega se pohranjuju određene značajke koje na šifriran način opisuju sam otisak. Tako prst postaje jedinstven privatan ključ koji služi za otključavanje ili zaključavanje informacija, anonimno i štiteći privatnost korisnika. Šifriranje je također od vitalne važnosti i za privatnost i za sigurnost, a vladini pokušaji da ga potkopaju redoviti su i duboko razočaravajući. Umjesto toga, vlade bi trebale podržavati i poticati razvoj jače enkripcije i njezinu primjenu na internetu. Nažalost, to nije tako.

ZAKONI I PREPORUKE

Zakonska regulativa Republike Hrvatske

U odnosu na privatnost na internetu, pravna zaštita dolazi u dvije glavne kategorije. Prva je izravna zaštita privatnosti, a posebno privatnosti podataka i komunikacija. Dok je druga, u ograničenjima i kontroli nad zakonskim

narušavanjem privatnosti, na primjer u nadzoru i odgovornostima ugrađenim u vladin zakon o nadzoru. Ustavom Republike Hrvatske, člankom 37. „Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Zakonom se uređuje zaštita podataka te nadzor nad djelovanjem informatičkih sustava u državi. Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihovoga prikupljanja“. Hrvatski sabor je potvrdio 2005. godine Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka. „Svrha je ove Konvencije svakoj fizičkoj osobi, bez obzira na njezino državljanstvo i boravište, na području svake stranke, osigurati poštovanje njezinih prava i temeljnih sloboda, a osobito njezino pravo na privatnost glede automatizirane obrade osobnih podataka koji se na nju odnose (zaštita podataka)“ (čl. 1.).[5] Nakon toga je donesen Zakon o informacijskoj sigurnosti 2007. godine zbog važnosti informacijske sigurnosti u očuvanju zaštite privatnosti. Alen Rajko u svojoj knjizi „Informacijsko upravno pravo“ (2011:134) navodi: „Područja informacijske sigurnosti, prema Zakonu o informacijskoj sigurnosti, jesu sigurnosna provjera, fizička sigurnost, sigurnost podataka, sigurnost informacijskog sustava te sigurnost poslovne suradnje“. Nadležno državno tijelo koje regulira donošenje i primjenu mjera informacijske sigurnosti Republike Hrvatske je Ured Vijeća za nacionalnu sigurnost (čl. 14). Na zaštiti i prevenciji od računalnih ugroza sigurnosti informacijskih sustava, zajedno rade CERT (ustrojstvena jedinica Hrvatske akademske i istraživačke mreže) i Zavod za sigurnost informacijskih sustava (čl. 21).

2018. godine na snagu stupa Opća uredba o zaštiti podataka (*General Data Protection Regulation*), odnosno novi zakon o zaštiti privatnosti i osobnih podataka koji se primjenjuje u svih 28 država članica Europske Unije pa tako i Republici Hrvatskoj. GDPR jača prava ispitanika i donosi opsežnije definicije novih pojmova važnih za privatnost. U Republici Hrvatskoj također djeluje Agencija za zaštitu osobnih podataka. Agencija je samostalno i neovisno

[5] Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka.

državno tijelo koje nadzire provedbu Opće uredbe o zaštiti podataka i na svojoj internetskoj stranici navodi prava građana. „Zaštita osobnih podataka u RH ustavna je kategorija te je svakom građaninu zaštita ljudskih prava i temeljnih sloboda zajamčena bez obzira na državljanstvo i prebivalište te neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili drugim osobinama. Svi građani imaju Pravo na pristup osobnim podacima, Pravo na ispravak osobnih podataka, Pravo na brisanje osobnih podataka „pravo na zaborav“, Pravo na ograničenje obrade osobnih podataka, Pravo na prigovor, Pravo na prenosivost podataka i Pravo u vezi automatiziranog pojedinačno donošenje odluka, uključujući izradu profila“.

Preporuke i direktive Vijeća Europe

Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda od 4. studenoga 1950. godine u članku 8. navodi „kako svatko ima pravo na štovanje svog osobnog i obiteljskog života, prebivališta i dopisivanja. Vlasti se neće uplitati u to pravo osim u skladu sa zakonom i kad je to potrebno u interesu javne sigurnosti, sprječavanja kaznenih djela i slično“ (AZOP, 2017).

Zakon o zaštiti podataka europskog je podrijetla. Europski parlament i vijeće donijeli su 2002. godine Direktivu o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija. „Nove napredne digitalne tehnologije uvode se u ovom trenutku u javne komunikacijske mreže u Zajednici, što dovodi do posebnih zahtjeva u vezi sa zaštitom osobnih podataka i privatnosti korisnika. Razvoj informacijskog društva karakterizira uvođenje novih elektroničkih komunikacijskih usluga. Pristup digitalnim pokretnim mrežama postao je dostupan i prihvatljiv široj javnosti. Ove digitalne mreže imaju ogromne kapacitete i mogućnosti obrade osobnih podataka. Uspješan prekogranični razvoj ovih usluga djelomice ovisi o povjerenju korisnika da njihova privatnost neće biti ugrožena. Internet mijenja tradicionalne tržišne strukture pružajući zajedničku globalnu infrastrukturu za dostavu širokog raspona elektroničkih komunikacijskih usluga. Javno dostupne elektroničke

komunikacijske usluge preko interneta otvaraju korisnicima nove mogućnosti, ali također i nove opasnosti za njihove osobne podatke i privatnost“.[6] Navedenom se Direktivom usklađuju odredbe država članica Europske Unije kako bi se zaštitilo pravo na privatnost vezano uz obradu osobnih podataka pri elektroničkoj komunikaciji (čl. 1). Ovom Direktivom propisuje se da davatelji usluga elektroničkih komunikacija moraju poduzeti odgovarajuće mjere kako bi zaštitili sigurnost svojih usluga i mreže (čl. 4). Također, države članice putem svojih zakonodavstava moraju osigurati povjerljivost komunikacija. Sukladno tome, bez pristanka korisnika moraju zabraniti slušanje, prisluškivanje, pohranjivanje i slične oblike nadzora nad komunikacijama, osim kada imaju zakonsko dopuštenje za navedeno (čl. 5). „Svatko ima pravo na zaštitu osobnih podataka koji se na njega ili nju odnose. Takvi podaci moraju se obrađivati pošteno, u utvrđene svrhe i na temelju suglasnosti osobe o kojoj je riječ, ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom. Svatko ima pravo na pristup prikupljenim podacima koji se na njega ili nju odnose i pravo na njihovo ispravljanje“.[7]

Nakon toga, 2018. godine na snagu stupa već spomenuti GDPR. „Općom uredbom o zaštiti podataka (eng. General Data Protection Regulation, poznatija pod akronimom GDPR), koja se izravno primjenjuje u svim državama članicama Europske unije od 25. svibnja 2018. godine, moderniziran je regulatorni okvir kako bi išao u korak s brzim razvojem tehnologije i postao učinkovit u današnje digitalno doba, a ujedno i ojačao povjerenje pojedinaca u elektroničke usluge i jedinstveno digitalno tržište. Zakonom o provedbi Opće uredbe o zaštiti podataka osigurava se provedba Opće uredbe o zaštiti podataka“ (AZOP, 2018). „Analiza RSA Securityja, koja je pokazala da korisnici zaista drže do svoje privatnosti. Ispitano je preko 7500 osoba iz Francuske, SAD-a, Italije, Njemačke i Ujedinjenog Kraljevstva. Naime, 80 % ispitanika povrede financijskih i bankovnih podatka smatra iznimno zabrinjavajućom, a tri četvrtine strahuje od gubitka lozinki i podataka s osobnih dokumenata. Tvrtkama će zanimljiv biti podatak da bi 62% korisnika za gubitak podataka prije okrivilo tvrtku kojoj su

[6] DIREKTIVA 2002/58/EZ EUROPSKOG PARLAMENTA I VIJEĆA od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (5), (6).

[7] Povelja Europske unije o temeljnim pravima.

dali podatke nego hakere koji su podatke ukrali. Kako navode autori istraživanja, „Korisnici postaju sve upućeniji i u problematiku privatnosti pa očekuju veću razinu transparentnosti i odgovornosti od skrbnika njihovih osobnih podataka“. Ključno je, dakle, da korisnici ne opraštaju tvrtkama koje gube njihove podatke“ (AZOP, 2018). Najveće stvarne razlike koje su ostvarene uvođenjem GDPR-a odnose se na provedbu i kažnjavanje (masovno se povećavaju novčane kazne za one koji krše zakon) i „doseg“ (GDPR izričito navodi da treba biti poštovan u bilo kojoj tvrtki bilo gdje u svijetu koja svoje usluge usmjerava na korisnike u Europskoj Uniji). Načela zaštite podataka relativno su jasna. GDPR je postavio niz mogućih zakonitih osnova za obradu podataka:

1. Pristanak
2. Ispunjenje ugovora
3. Zadovoljavanje zakonske obveze
4. „Vitalni interesi“ ispitanika (na primjer, njihovo održavanje u životu)
5. Obavljanje zadatka od javnog interesa (uglavnom od strane vlasti ili onih koji rade za tijela)
6. „Legitimni interesi“ bilo obrađivača bilo treće strane.

SOCIOLOŠKA PERSPEKTIVA

Jedan od najbitnijih predstavnika postmodernizma i poststrukturalizma koji se bavio analizom sociokulturnih promjena u informatičkom dobu jest Jean Baudrillard. Postmodernizam karakterizira osjećaj fragmentiranog i decentraliziranog jastva, odnosno višestrukih i konfliktnih identiteta. Alternativni životni stilovi te višestruki identiteti zajedničkog života i skrbi za djecu. Internet pruža privid trenutnog preuzimanja određenih informacija koji inače može trajati dugo, te su sadržaji na njemu napravljeni da se mogu što brže i lakše pročitati. Internet je uvijek uključen, ubrzan i pun slika i tekstova koji mogu rezultirati izgubljenošću korisnika te mu možemo pristupiti u bilo koje

vrijeme. To dovodi do mogućnosti radnog vremena 24 sata dnevno, odnosno neograničenog radnog i slobodnog vremena. Uz to, mogućnost istovremenog otvaranja različitih sadržaja, odnosno virtualnih svjetova, dovodi do višestrukosti identiteta jer se digitalni identitet izmišlja i pravila normalne, stvarne interakcije se ne prihvaćaju. Virtualna realnost termin je koji se u širem značenju odnosi na svaki prostor dematerijalizirane komunikacije/informacije, poput telefonskoga razgovora ili igranja igara u virtualnom svijetu. Virtualna se realnost odnosi na precizno definirane tehnologije (Nikodem, 2019:5). Stoga, francuski sociolog Jean Baudrilliard u svojoj teoriji posebno ističe pojmove simulacije, simulakruma i hiperrealnosti. Za njega je osnovna karakteristika postmodernog stanja društva upravo dominacija simulakruma, to jest simulacije koja predstavlja stvaranje zbilje po modelima bez stvarnosti i bez porijekla te tako stvara hiperrealnost. U ovom istraživanju, simulakrum bi predstavljao društvene mreže i ponašanje njihovih korisnika koji na njima grade svoj drugi identitet. Baudrillard opisuje postmoderni svijet kao svijet u kojem se život odvija na televiziji i postaje video, odnosno skup slika. Građani tog svijeta postaju zabavljači vlastitih života te ih tako predstavljaju, kao i na društvenim mrežama. Postmoderno stanje društva oblikuje potpunu virtualizaciju ljudskog života u kojem oblik kontrole postaju reklame, Baudrillard također smatra da je posjedovanje televizije u domu oblik društvenog nadzora koji nameće govor bez odgovora. Reklame i oglasi za proizvode u današnjem svijetu postaju sve personaliziraniji i rašireni, dostupni u svakom trenutku. Za razliku od modernističke metafore „ogledala“, postmoderna metafora „zaslona“ nema drugu stranu, nema dubine, postoji samo površina. Pa se stoga i u digitalnom životu više cijeni i poštuje površina, odnosno identitet koji je tamo prikazan, a nema poveznice sa stvarnim svijetom (Nikodem, 2019:10). Jean Baudrillard označava tradicionalno društvo simboličkom razmjenom, moderno proizvodnjom, a postmoderno vraća na simboličku razmjenu, ali u drugačijim uvjetima. Dominantna roba za razmjenu u postmodernom stanju društva je informacija, to znači da danas prevladava potrošnja znakova roba. Informacije postaju oružje kojim se lako upravlja i svima je dostupno. Kroz višestrukost identiteta stvorenih na internetu, korisnici imaju iskrivljenu sliku stvarnosti. Zbog nemogućnosti prepoznavanja stvarnosti i jave, javlja se dominacija simulakruma. Drugačije norme, opća pravila i načini komunikacije koji su

utvrđeni na internetu, stvarnost prerasta u hiperrealnost. Odnosno, ono što je stvarno postaje manje važno, a virtualnost, to jest digitalni život postaje sve važniji. U sličnom svjetlu i španjolski sociolog, Manuel Castells, također promatra postmoderno društvo te u svojim djelima „Uspon umreženog društva" i „Informacijsko doba" konceptualizira pojmove koji bi ga što bolje opisali. Jedan od njih, a značajan za ovaj rad, jest „kultura stvarne virtualnosti" koja se sastoji od protoka informacija, fleksibilnosti i raznolikosti hiperteksta. Ona se odnosi na kulturno područje koje je također umreženo, fleksibilno i sadrži simboličku interakciju i komunikacijske mreže. Odnosno, internet i njegovi korisnici koji stvaraju tu kulturu. O politikama Castells govori kao o rezultatu medija, koji su veoma bitni za prostor politike. To znači da ljudi svakodnevno primaju poruke od medija i na temelju tih informacija (s radija/Tv-a i slično) formiraju svoje mišljenje i ponašanje te usvajaju nove navike i obrasce. Kao na primjer, manipuliranje izbornim glasovima u raznim državama od strane *Cambridge Analytics* tvrtke. „Bezvremensko vrijeme" je pojam koji također vežemo uz društvenu mrežu kao društvenu strukturu koja se pojavljuje u informacijskom dobu, a organizira se oko novih oblika vremena i prostora, oko bezvremenskog vremena i prostora tokova. Ono što se nudi novo u tom informacijskom dobu jesu nove reproduktivne tehnike u kojima ljudi imaju veći raspon mogućnosti, što bi značilo da mogu koristiti nove informacijsko-komunikacijske tehnologije u svrhu uništenja vremena. Sve je konstantno dostupno i aktivno, ne postoji vremensko ograničenje na internetu. „Prostor tokova" je pojam koji Castells navodi, te govori kako prostor mjesta i dalje nastavlja biti dominantan prostor iskustava, svakodnevnog života i društvene političke kontrole, ali kako taj prostor tokova zapravo strukturira i oblikuje prostor mjesta. Može se reći kako prostor tokova stvara nove granice prostornog istraživanja koje onda dovode u pitanje interakciju između prostora tokova, prostora mjesta, funkcija, značenja i dominacija sve više složenih obrazaca. Tvrdi da internet ima vlastitu geografiju koja se sastoji od mreža i čvorova što obrađuju tokove informacija koje su generirane i kojima se upravlja s mjesta u fizičkom svijetu. Castells definira i pojam stvarne virtualnosti, ona se stvara kroz komunikacijski sustav kojeg autor definira kao „sustav u kojem je sama stvarnost (to jest ljudsko materijalno/simboličko postojanje) u potpunosti obuhvaćena, posve uronjena u virtualnu postavu slika, u izmišljeni svijet, u

kojemu pojave ne postoje samo na ekranu pomoću kojeg se iskustvo komunicira, već same postaju iskustvo“ (Castells, 2000:400). Slično kao i Baudrillardova hiperrealnost. Radno vrijeme više nije toliko fiksno kao u industrijskom dobu te postaje sve fleksibilnije što radnika stavlja u nezgodnu poziciju. On mora biti stručno obrazovan, ali mu to ne jamči stalno zaposlenje. Također, ovakav je proces potisnuo utjecaj sindikata koji se bore za prava radnika. Ovo nam jasno daje doznanja koliko je život u umreženom društvu i digitalnom svijetu nepredvidiv i rizičan za radnika, ali isto tako i za svakog drugog pojedinca. Kako bi se prilagodio i identificirao te stupio u kontakt s drugim akterima u mreži, on mora usvojiti određene kulturne kodove koji se stalno mijenjaju i redefiniraju, poput informacija na internetu. Ono što je ustvari virtualno, za nas postaje realno. To se lako može dovesti u vezu s masovnim medijima koji djeluju u vlastitom referentnom okviru te na taj način nameću vlastitu viziju stvarnosti. Zaključno s tim, umreženo društvo autor shvaća kao društvo strukturirano putem dominantnih funkcija i procesa oko mreža, pri čemu se manifestira kroz kapitalističko društvo. Naznačuje da su društva mreža kapitalistička društva, ali njihov oblik kapitalizma se jasno razlikuje od industrijskog kapitalizma. Ona nisu stvorena od strane informacijske tehnologije, ali bez nje ne bi postigla svoj društveni oblik (Nikodem, 2019:7). Riječ je o morfološkoj transformaciji. „Izazov društvenoj dominaciji u društvima mreža okreće se oko redefiniranja kulturnih kodova, predlaganja alternativnih značenja i mijenjanja pravila igre, zato je afirmacija identiteta toliko važna, jer popravlja značenje samostalno u odnosu na apstraktnu, instrumentalnu logiku mreža“. „ Implikacija logike društva mreža naizgled završava povijest, zatvarajući je u ponavljajući obrazac strujanja/protoka. Ali kao i sa bilo kojim drugim društvenim oblikom, u stvari otvara nova područja kontradikcije i sukoba.“ (Castells, 2002/2007). Castellsova teorija se s vremenom pokazala sve važnijom za adekvatno analiziranje raznih fenomena koji se pojavljuju danas u društvu i njegov doprinos društvenim znanostima je postao neupitan kao i Baudrillardov.

RANIJA ISTRAŽIVANJA O PRIVATNOSTI I ZAŠTITI PODATAKA

Istraživanje „Percepcija zaštite podataka i pitanja privatnosti među djecom i mladima“ Izvršne agencija za obrazovanje, audiovizualnu djelatnost i kulturu (EACEA) u suradnji s Agencijom za zaštitu osobnih podataka provedeno je među učenicima dvadeset i pet osnovnih i srednjih škola u Republici Hrvatskoj (2012:3). Kao ciljevi istraživanja navedeni su, između ostalog, ispitivanje percepcije zaštite osobnih podataka i privatnosti na internetu, objavljivanje vlastitih i tuđih osobnih podataka na internetu te mišljenja, stavovi i preporuke ispitanika o tom pitanju (2012:2).
Rezultati su pokazali kako ispitanici provode značajan dio slobodnog vremena na internetu. Većina svakodnevno koristi internetske tražilice, društvene mreže, komunikacijske programe i slično. Najčešće se internet koristi kao platforma za zabavu, ali i socijalizaciju. Društvene mreže, poput Facebooka, popularne su zato što ispitanici imaju sklonost virtualnom upoznavanju nepoznatih osoba. Dokazana je hipoteza o dijeljenju osobnih podataka ispitanika bez njihovog saznanja o mogućnim opasnostima i zloupotrebi. Nadalje, više od trećine ispitanika otkriva svoje zaporke i korisnička imena, a više od pola njih ostavlja svoje osobne podatke na internetu (fotografije, brojeve mobilnih telefona, adrese i slično). Također neki od ispitanika su iskusili da se netko lažno predstavlja njihovim imenom. Velika većina ispitanika (92%) nije educirana o zaštiti osobnih podataka i privatnosti na internetu te ne znaju kome se obratiti u slučaju zlouporabe (2012:18).

Istraživanje u sklopu diplomskog rada „Etika i zaštita privatnosti“ Marijane Ivanušić na Studiju Poslovne ekonomije iz Varaždina 2017. godine provedeno je putem društvenih mreža i elektroničke pošte na 93 ispitanika (2017:29). Svrha rada je istražiti koliko su ispitanici upoznati sa zaštitom privatnosti i etikom na internetu. Istraživanje je pokazalo kako većina ispitanika dobrovoljno dijeli osobne podatke, na primjer za potrebe elektroničke trgovine, pa samim time pokazuju kako nisu dobro upoznati s mogućim ugrozama njihove privatnosti (2017:49).

EMC Corporation (danas: *Dell EMC*) 2014. godine provelo je istraživanje naziva „*EMC Privacy Index*“, globalnu studiju o stavovima korisnika vezanih uz privatnost na internetu. Istraživanje je obuhvatilo petnaest zemalja, odnosno petnaest tisuća korisnika. Studija je pokazala kako stavovi

korisnika variraju ovisno o geografskom položaju i sadržaju koji konzumiraju na internetu. Kao rezultate istraživanja, autori su naveli tri paradoksa:

Paradoks želimo sve (*We Want It All*)

Bez obzira na osobnost i vrstu koristi, korisnici interneta gotovo da i nisu spremni dijeliti osobne podatke zbog povlastica digitalne tehnologije; 91% ispitanika cijeni to što digitalna tehnologija omogućuje jednostavniji pristup informacijama; samo 27% ispitanika tvrdi kako je voljno podijeliti privatnost na internetu zbog praktičnosti i jednostavnosti; 85% ispitanika cijeni korištenje digitalne tehnologije za zaštitu od kriminalnih i terorističkih aktivnosti, no samo 54% njih je spremno podijeliti svoju privatnost u tu svrhu.

Paradoks ništa ne poduzeti (*Tako No Action*)

Više od polovice ispitanika bilo je žrtvom internetskog kriminala (hakiranje računa emaila ili društvenih mreža i slično), a mnogi od njih ne poduzimaju mjere za zaštitu; 62% ispitanika ne mijenja lozinke redovito; 40% ispitanika ne prilagođava postavke privatnosti na društvenim mrežama.

Paradoks društvenog dijeljenja (*Social Sharing*)

Korištenje društvenih medija naglo se širi unatoč: očekivanjima ispitanika da će njihovu privatnost na društvenim medijima biti teško očuvati u narednih pet godina; mišljenju korisnika kako institucije koje bi trebale štititi njihovu privatnost na društvenim mrežama to ne rade efektivno (51% ispitanika ima povjerenja u vještine tih institucija, a 39% u njihovu etiku); 84% ispitanika tvrdi kako ne želi da su njihovi osobni podaci dostupni ikome, ako ih nisu sami odlučili podijeliti. Istraživanje je još pokazalo kako 59% ispitanika smatra da se unutar jedne godine razina njihove privatnosti smanjila, a 81% njih očekuje da će se u narednih pet godina smanjiti još više.

Istraživanje u sklopu diplomskog rada „Zaštita privatnosti na internetu“ Domagoja Justamenta na Hrvatskim studijima, odjel za komunikologiju iz 2017. godine provedeno je na uzorku od sto pedeset i tri ispitanika, kvantitativnom metodom eksploratorne ankete. Rezultati istraživanja pokazali su kako su korisnici interneta zabrinuti za svoju privatnost te da zbog toga rijetko objavljuju osobne podatke (prilikom online trgovine, korištenjem društvenih mreža ili upisivanjem podataka u internetske tražilice) na internetu. Također, korisnici

interneta smatraju se adekvatno medijski pismenima, te zaključuju da hrvatski zakoni nedovoljno štite njihovu privatnost. Također, većina ispitanika smatra kako društvene mreže i usluge internetskih tražilica u određenoj mjeri narušavaju njihovu privatnost. Što se tiče upotrebe društvenih mreža i usluga internetskih tražilica, ispitanici uglavnom ne čitaju uvjete korištenja, no ipak je većina njih upoznata s mogućnošću isključivanja opcija privatnosti na navedenim servisima. Dio ispitanika zna na koje načine društvene mreže i usluge internetskih tražilica oglašavaju, a velika većina ih zna da tako i zarađuju. Dio ispitanika preferira personalizirane oglase jer tako lakše dolaze do željenog proizvoda ili usluge, a drugi dio ne voli da se na ovaj način zadire u njihovu privatnost. No, i jedni i drugi rijetko otvaraju ponuđene oglase. (2017:50).

METODOLOGIJA

Kako bi se ispitalo u kojem smjeru ide briga korisnika o svojim podacima i privatnosti na internetu, postoji li uopće digitalna privatnost te koliko zakoni i preporuke djeluju u svojoj svrsi, provedeno je kvalitativno istraživanje metodom strukturiranog intervjua na uzorku od 10 sugovornika. Poziv za sudjelovanje u istraživanju, uz kriterije, bio je podijeljen na Facebook stranici profila istraživačice. Sugovornici koji su pristali sudjelovati u istraživanju su obaviješteni putem e-maila o dodatnim informacijama o provedbi. Intervjui su provedeni online putem preko platforme Zoom uz audio snimanje, zatim transkribirani te obrađeni radi uočavanja svjesnosti o digitalnoj privatnosti. Dakle, uzorak sačinjavaju svakodnevni korisnici interneta i društvenih mreža, različitih dobnih skupina te različitih geografskih područja. Dobne skupine sugovornika su podijeljene u dvije grupe, od 15 do 35 godina te od 35 do 50 godina starosti kako bi se ustvrdilo brinu li više o temi mlađa dobna skupina ili starija. Različite dobne skupine i različita geografska područja imaju svrhu proširivanja slike o brizi korisnika interneta o svojim podacima na njemu. Strukturirani intervju je konstruiran za potrebe provedbe istraživanja za ovaj diplomski rad. Pitanja su konstruirana konzultirajući rezultate ranijih kvalitativnih i kvantitativnih studija o srodnoj tematici kao što su „Percepcija zaštite podataka i pitanja privatnosti među djecom i mladima“ (EACEA, 2012),

„Etika i zaštita privatnosti“ (Marijana Ivanušić, 2017), „*EMC Privacy Index*“ (*Dell EMC*, 2014) i „Zaštita privatnosti na internetu“ (Domagoj Justament, 2017). Strukturirani protokol sadrži pitanja koja slijede tematske odrednice istraživanja (Podaci o sugovornicima, Uvod, Zaštita podataka, Zlouporaba podataka, Reklame, Kraj). Nastojalo se svakog sudionika izložiti identičnom iskustvu intervjua, tako da se za eventualne razlike može pretpostaviti da su rezultat varijacija među ispitanicima, a ne razlika u samom procesu intervjua. Vrijeme trajanja intervjua jest 30-45 minuta, zavisno o komunikaciji i zainteresiranosti sugovornika. Od sugovornika su se tražile opće sociodemografske informacije poput spola, dobi, zanimanja kojim se bave, mjesta u kojem žive. Intervjui su se provodili individualno te u istraživačkom izvještaju/tekstu rada nisu otkriveni bilo koji identificirajući podaci o ispitanicima istraživanja. Ako se u radu prikazuje citati iz transkripata, identitet sugovornika istraživanja je zamijenjen šifrom, odnosno brojem, tako da identitet ostane zaštićen. Transkripcijom su podaci pročišćeni od identificirajućih podataka.

REZULTATI ISTRAŽIVANJA

Prikupljeni podaci u istraživanju su obrađeni kvalitativnom analizom sljedećim koracima:

1. transkribiranje odgovora i slušanje audio zapisa o stavovima privatnosti na internetu

2. podcrtavanje odgovora sudionika ovisno o 6 primarno određenih kategorija

3. kodiranje izdvojenih odgovora sugovornika

4. obrađivanja i analiziranje dobivenih odgovora i rezultata intervjua

5. interpretacija rezultata istraživanja prema dobivenim odgovorima sugovornika

Podaci o sugovornicima

Većina sugovornika je muškog spola, njih 6, dok je njih 4 ženskog spola. Najčešća dob sugovornika je između 25 godina starosti do 35 godina. Najstariji sugovornik ima 45 godina, a najmlađi 16 godina. 2 sugovornika su kao mjesto stanovanja navela selo, dok su 3 navela manji grad, a ostatak, njih 5, veći grad. Od 10 sugovornika u istraživanju zastupljeno je 3 zanimanja (student, IT struka i ostala zanimanja).

Uvod u intervju

Svi sugovornici su izjavili da svakodnevno koriste internet i društvene mreže i u poslovne svrhe i za zabavu, što je ujedno i bio kriterij za sudjelovanje u istraživanju. Najčešće riječi koji ih asociraju na privatnost na internetu su GDPR, nesigurnost, kolačići, skepticizam, lozinke i anonimnost te svi smatraju da su upoznati s pojmom privatnosti. Na pitanje što njima predstavlja pojam privatnosti na internetu većina sugovornika je odgovorila nešto poput „*Mogućnost da koristim Internet bez da druga ili neka treća osoba može pristupiti mojim podacima*"(1).[8] Dok je jedan sugovornik, IT struke, rekao da mu taj pojam „*Predstavlja mi nešto što je trenutno nedostižno u svijetu*"(2). Svi sugovornici smatraju da se pojam privatnosti razlikuje u stvarnom i digitalnom svijetu, ali da ipak ima sličnosti i preklapanja u spomenutim pojmovima. „*Nikad nisam razmišljao o tome, ali vjerojatno se neki temeljni koncepti poklapaju. Ako u stvarnom svijetu imamo neku privatnost to se većinom odnosi na to da ti nitko ne gleda kroz prozor u kuću i tako. A to se onda prenosi na Internet da ti nitko ne bulji u tvoju nekakvu sferu u kojoj ti boraviš, mislim da se nekako metaforički preslikava taj koncept privatnosti. Naravno, kad se to pretvori u stvarnost drugačije izgleda jer Internet i stvarnost nisu isti, ali se koncepti prenose. Mislim da se pokušava premostit tu razliku između privatnosti u stvarnom i*

[8] Brojevi u zagradama označavaju sugovornika o čijoj se izjavi radi. Budući da je sudionicima istraživanja
osigurana anonimnost, u istraživanju nisu korištena osobna imena sugovornika.

digitalnom svijetu“(3). Već spomenuti sugovornik IT struke (2) razliku između privatnosti u stvarnom i privatnosti u digitalnom svijetu objašnjava kao „*Digitalni svijet nije realan, sve se to pohranjuje u neke vanjske softvere i nikad ne nestaje. A ovako u stvarnom svijetu bi možda bila realna privatnost gdje ti možeš kontrolirati tko će što znati o tebi. U stvarnom svijetu si svjesniji privatnosti i možeš više utjecat na nju*“. Na pitanje o „kolačićima“ svi sugovornici su odgovorili da su upoznati s pojmom, da su čuli za njega, a samo ih je nekoliko, odnosno 3, koji pripadaju IT struci, uspjelo točno definirati taj pojam.

Zaštita podataka

Većina sugovornika se izjasnila kako smatraju da nisu zaštitili svoje podatke na internetu jer „*mislim da to nije ni moguće do kraja napraviti. Ako netko želi pronaći podatke o meni, to će svakako uspjeti*“(7). No, bez obzira na takav stav svi sugovornici se osjećaju relativno sigurno u dijeljenju svojih podataka na internetu „*Pa ono, s jedne strane država ima moje podatke jer imam osobnu iskaznicu, svakako te neke podatke imaju. A sad baš da neke treće osobe i tvrtke trebaju imati moje podatke i ti algoritmi koji su toliko napredovali koji stvaraju sadržaj specifično za tebe, taj targeted marketing nekad ode baš u nekakve ekstreme. Skužim da algoritam bude previše točan pa me to malo uplaši i izbaci iz takta jer gubim taj osjećaj sigurnosti*“(1). Iako smatraju da ne mogu do kraja upravljati tim podacima, to ih ne sprječava u svakodnevnom surfanju i dijeljenju jer doživljavaju to kao način života. „*Nije da se ne osjećam sigurno, ali i ne osjećam se baš pretjerano sigurno. Smatram da je to dio današnjeg društva i da se to ne može izbjeći, ali mislim da još uvijek ne znamo kakve posljedice će to trajno imati na društvo*“(5). Sukladno tome, najviše ih brine na koji način se njihovi podaci koriste i što se s njima sve radi bez njihovog znanja. Također, svi sugovornici su izrazili zabrinutost u vezi internet kupovine i web shopova, gdje ostavljaju podatke svojih bankovnih kartica i računa. Na pitanje o informiranosti u vezi privatnosti na internetu i zaštite svojih podataka, točno

pola sugovornika je odgovorilo kako misli da su dovoljno informirani o toj temi, a druga polovica da nisu dovoljno.

Zlouporaba podataka

U slučaju zlouporabe podataka, ni jedan od sudionika u ovom istraživanju se nije susreo s takvom situacijom „*Osobno ne, dogodilo se u slučaju distributera telekomunikacijskih usluga mojoj kolegici. Dobila je zamjenski broj službenog telefona koji je već bio u funkciji druge osobne, to se ne bi smjelo događat*“(6). „*Pa čula sam da je na primjer, banka posudila novce s nečijeg privatnog računa, kad je osoba shvatila nazvala je banku pa su joj oni rekli da nisu imali dovoljnu količinu novca u banci i da bi oni to vratili*“(9). Po odgovorima dobivenim na ovo pitanje bi mogli zaključiti da se zlouporaba podataka ne događa baš toliko često, no s obzirom na uzorak od samo 10 sugovornika ne možemo generalizirati. Bez obzira na to, svi su sugovornici odgovorili da je moguće zlouporabiti njihove podatke bez njihovog znanja i pristanka „*Naravno. Vrlo je jednostavno i to se događa svaki dan*“(2). Isto tako se svi sugovornici slažu da je danas nemoguće ostati anoniman na internetu, osim 3 sugovornika koji rade u IT struci. Oni smatraju da je moguće ostati anoniman na određenim internetskim pretraživačima. Na pitanje o IP adresi, dobili smo slične odgovore kao na pitanje o „kolačićima“. Svi znaju što je IP adresa, ali samo nekoliko sudionika zna njenu ulogu.

Što se tiče zakonskih regulativa i institucija koje se tiču zaštite privatnosti na internetu, svi sudionici istraživanja su naveli GDPR i policiju. Dok je četvero sudionika navelo i tijela EU koja se bave tim, te njihove preporuke i naputke. Također, nitko od sudionika ne zna kome bi se trebali obratiti u slučaju zlouporabe podataka. Svatko od njih je započeo svoj odgovor sa „*Ne znam, možda…*“ po čemu možemo zaključiti da takve informacije baš i nisu osviještene.

Reklame i oglasi

Svi sugovornici su primijetili pojavu određenih reklamnih oglasa koji se čine personalizirani, odnosno upućeni direktno njima. „*Podvojenog sam mišljenja o toj personalizaciji oglasa. Nekad zna bit toliko jezivo jer ispada da tamo neki algoritam na internetu poznaje mene bolje nego ja sam sebe, a nekad zna biti korisno. Ili me bombardiraju s nečim što sam ja onako usputno otvorio, a oni su zamislili da mene to zanima. Tako da, kako kad mi smeta, ali definitivno su Instagram i Facebook puno agresivniji u tome*“(1). Neki su izrazili svoju zabrinutost i strah od takvih oglasa, dok su drugi izrazili potpuno razumijevanje „*U početku mi je to bilo čudno, nakon toga sam shvatila da je to posao kao i svaki drugi. Gdje je ljudima zapravo cilj da ti stvore svjesnost o nekom proizvodu, to je nekakva marketinška domena. S vremenom sam to naučila ignorirat uz AdBlockere. Jednostavno, to je ljudima posao kao što je nama posao napisat diplomski. Nudi jednu vrstu konformizma gdje sve što zamisliš ti se pojavi na oglasu. Nađeš stvari koje nisi ni znao da želiš dok ih ne vidiš i mislim da je to jedna od linija potrošačkog društva koja će bit teško zamjenjiva i blokirana jer ljudima koliko god da smeta pruža i uslugu*“(4). Što se tiče afera prodaje internetskih podatka marketinškim tvrtkama, svi sugovornici su čuli za njih, ali samo jedan je bio dovoljno upoznat s potpunom pričom. „*Sudjelovala sam na jednoj konferenciji gdje je bila velika priča o Google analiticsima i google marketingu, gdje jednostavno svaka stranica ima svoj oglašavački prostor koji prodaje drugima. A što se tiče afera, najveća stvar u tome je da se teško mogu naplaćivat te usluge, provodit zakonske norme i PDV. Veliki skandal je bio u IKEI u Francuskoj, kada su skupljali podatke o svojim zaposlenicima i kupcima, kartične transakcije, platežnu moć itd. I to je sigurnosni most i za IKEU i za banke jer si ti to potpisao. Ljudi kliknu bez problema „I Agree“ na internetskim stranicama u ugovorima, ništa ne čitaju, a da ga imaš uživo ugovor bi pročitao i pregledao*“(4). Kako nisu pretjerano bili upoznati s aferama, tako te afere nisu nužno utjecale na njihovo mišljenje o privatnosti korisnika na internetu. Svakako su i bez afera bili svjesni da se podacima trguje. Većini sugovornika reklame na internetu ne smetaju, osim starijim korisnicima, iako su primijetili da su se u posljednjih nekoliko godina povećale. Osim kada se radi o

Youtubeu, gdje reklame iskaču dok je video pušten i zaustavljaju ga „*Reklame su se u zadnjih godina učetverostručile. Mislim jasno, Internet je besplatan i svima dostupan pa plaćamo svojim podacima. Inače bismo plaćali samu uslugu, a ovako oni imaju svoje sponzore i hrpetinu reklama. Postale su neizbježne, bez obzira na broj AdBlockera koje imam. Youtube je postao katastrofa, oni imaju duple reklame, neizdrživo je. Ili će me maltretirati reklamama ili će me natjerati da se pretplatim na Youtube Premium*“(5).

Kraj intervjua

Za kraj, na pitanje brinu li više o privatnosti na internetu mlađi ili stariji korisnici, odgovori su bili različiti. Pola sugovornika je odgovorilo da mlađi korisnici više brinu o tome jer su upoznati s internetom i prijetnjama na njemu, dok su 4 sugovornika izjavila da stariji korisnici više brinu. Jer im je stalo do tuđeg mišljenja i oprezniji su. Te jedan sugovornik koji je rekao da „*jednako ne brinu o tome i uopće nisu svjesni toga*“(2). „Obrnuta ideja, da mladi ljudi više ne brinu o privatnosti - dokazana je, barem u očima Marka Zuckerberga, činjenicom da razmjenjuju masu osobnih podataka koje su ljudi u prošlosti mogli smatrati privatnima - slično je pogrešno shvaćena. Kad se pomno pogleda, kao što su to učinili brojni znanstvenici, može se vidjeti da je mladima doista stalo do privatnosti, samo na drugačiji način od svojih prethodnika. Doista, na mnogo načina, oni više brinu o privatnosti nego neki od svojih starijih, bolje se bave tehnologijom zaštite privatnosti i više su 'upućeni' u to kako izbjeći nadzor i manipulaciju putem Interneta. Na primjer, manje je vjerojatno da će mlade ljude zavarati lažne vijesti od onih srednjih godina i naviše.“ (Bernal, 2020:17).

Na pitanje govori li se dovoljno o privatnosti na internetu i kršenju iste, 2 sugovornika su odgovorila da ide u dobrom smjeru. Sve se više priča o tome i te teme postaju aktualnije, dok 5 sugovornika smatra da se ne govori o tome dovoljno i ne viđaju baš članke vezane za to. Tri sugovornika koja su IT struke smatraju kako se o tome govori dosta, ali društvo ne sluša. Na kraju intervjua, sugovornicima je bilo postavljeno pitanje kako bi oni više osvijestili ovu temu u društvu, na što su svi, bez iznimke, odgovorili da informatika treba biti obavezan

predmet jer je informatička pismenost ovdje najbitnija. „ *Informatička pismenost je nešto na čemu se mora poradit, informatika definitivno mora postat obvezan predmet u osnovnoj školi, ali ne na način na koji smo ju mi imali prije 10 godina. Učili smo Word, Excell i tako dalje, ali definitivno je potrebno uvesti i zaštitu podataka*“(1). Kroz svoje odgovore su podijelili i neka razmišljanja, pa tako jedan od sugovornika smatra kako je naše društvo teško osvijestiti o ovakvoj temi jer smo potpuno uronili u potrošačko društvo i konformizam. „*Nisam sigurna ni da ljudi žele bit svjesni toga jer je to toliko uzelo maha što privatno što poslovno te ljudi više ne pate od nekakve privatnosti. Ne smatraju to tolikim sigurnosnim propustom, problem u banci s karticom je veliki problem, ali ovo ne. Baš zato što nisu informirani o tome, ne znaju što je Big Data collection, misle da to nije bitno. Ali bitno je za razvijanje umjetne inteligencije i načina komunikacije, mislim da to više kod nas ide ugodno s korisnim jer neki zarađuju putem toga dok drugima to ne smeta*“(10).

RASPRAVA

Kako bi utvrdili u kojem smjeru ide briga korisnika interneta o njihovim podacima i privatnosti te zaštiti istih, provedeno je kvalitativno istraživanje na uzorku od 10 sugovornika metodom strukturiranog intervjua.

Nakon provedenog istraživanja, možemo zaključiti da geografsko mjesto, to jest mjesto stanovanja nema utjecaj na ponašanje korisnika na internetu. Kao što Castells tvrdi „prostor tokova“ zapravo strukturira i oblikuje prostor mjesta, irelevantno je gdje se korisnici nalaze dok god imaju pristup internetu.

Svi korisnici su upoznati s pojmom privatnosti te smatraju kako se taj pojam razlikuje u digitalnom i stvarnom svijetu. To jest istina, ali se isto tako digitalni, odnosno online svijet prelijeva u stvarni svijet. To je virtualni svijet, ali sve što se napravi tamo se prenosi u realni svijet. Ako se napravi nekakav online zločin, osoba koja ga je počinila odgovarat će za njega u stvarnom svijetu iako možda smatra da neće. Tu vidimo nemogućnost prepoznavanja stvarnosti i jave, te javljanje dominacije simulakruma. Drugačije norme, opća pravila i načini

komunikacije koji su utvrđeni na internetu stvaraju hiperrealnost kao što objašnjava Baudrillard i vritualnu stvarnost po Castellsu.

Većina sugovornika smatra da nisu zaštitili svoje podatke na internetu, no i dalje se osjećaju sigurno u dijeljenju svojih podataka. Takvi stavovi dokazani su i u ranijim istraživanjima. Taj paradoks možemo promatrati kroz riječi Paula Bernala, s obzirom da svi sugovornici posjeduju i svakodnevno koriste društvene mreže, na njima se samoprofiliraju, odnosno „lajkajući, sherajući i surfajući“ ostavljaju svoje digitalne tragove, odabiru željene načine komuniciranja i nesvjesno pružaju društvenim mrežama sve podatke koji su im potrebni za izradu personaliziranih oglasa. Ovdje možemo uvidjeti i prethodno spomenuti paradoks „Želimo sve“ u poglavlju „Ranija istraživanja o privatnosti i zaštiti podataka“ koji objašnjava da korisnici nisu spremi podijeliti svoje osobne podatke u svrhu praktičnosti i jednostavnosti upotrebe digitalne tehnologije, ali koristeći društvene mreže i internetske tražilice to svakako rade.

Svi sugovornici smatraju kako ne mogu upravljati svojim podacima na internetu, ali ih to ne zabrinjava previše jer je to jednostavno današnji način života, odnosno dominantna roba za razmjenu u današnjem dobu su informacije. Potpuno je očekivano takvo razmišljanje, te je već spomenuti autor Paul Bernal to opisao kao nerazumno je očekivati da će ljudi razumjeti, a kamoli djelovati kako bi se pozabavili masovnim društvenim problemima. Tu političari i regulatori trebaju biti najhrabriji. Moramo pronaći način da smanjimo njihovu moć - moć kojom raspolažu ne samo svojim utjecajem na mjerodavna tržišta, već i svojim ogromnim resursima podataka, mogućnostima prikupljanja podataka, analitičkom moći podataka i izravnim pristupom ljudima.

Pola sugovornika misli da su informirani o privatnosti i zaštiti podataka, a druga polovica da nisu. Na kraju ipak zaključujemo da je druga polovica sugovornika bila u pravu.

Kao što i ranija istraživanja pokazuju, većina smatra da će se njihova razina privatnosti smanjiti u narednih pet godina, ali ne poduzimaju nikakve mjere vezane za to. Iz toga proizlazi da nitko od sugovornika ne zna kome se treba obratiti u slučaju zlouporabe podataka, čak ni sugovornici koji su zaposleni u IT struci.

Reklame i oglasi im većinom ne smetaju, osim starijim sugovornicima, ali svi ih ignoriraju, odnosno ne otvaraju, kao što je dokazano i u istraživanju Domagoja Justamenta „Zaštita privatnosti na internetu“ (2017). Kao što je Paul Bernal (2020:70) zaključio YouTube može jednako učinkovito širiti lažne vijesti videozapisima, postavljati velik broj reklama i oglasa. Ovdje uviđamo Baudrillardovu teoriju koja tvrdi da reklame postaju oblik kontrole društva. Google, koji je vlasnik YouTubea, ima „carstvo“, koje je na mnogo načina tako veliko i moćno kao i Facebook. Oba „carstva“ imaju daleko više podataka o nama nego što je zdravo za našu privatnost i autonomiju i za budućnost naših demokracija. Manuel Castells također tvrdi da su mediji način putem kojeg se može manipulirati, odnosno formirati drugačije mišljenje i ponašanje njihovih korisnika.

Većina sugovornika smatra kako mlađi korisnici više brinu o zaštiti privatnosti i podataka, što tvrdi i Paul Bernal. Mlađi korisnici su jednostavno odrasli uz internet, zato im je i manji problem ignorirati reklame i oglase, toliko su već navikli na sve to da lako ignoriraju. Dok je starijim korisnicima internet došao u vrijeme kada su već odrasli i navikli na neke druge stvari, pa im se teže prilagoditi.

Neki sugovornici smatraju da se dovoljno govori o ovoj temi u društvu, a neki se ne slažu. Točnije, sugovornici koji rade u IT struci smatraju da se dovoljno govori o ovoj temi jer su konstantno okružen tim informacijama dok ostali sugovornici smatraju da tema nije učestala u društvu.

Svi su izjavili kako bi informatika u osnovnim školama trebala postati obvezan predmet i moderniziran. Te da bi ljudi trebali postati informatički pismeni kako bi se služili internetom bez da to ugrožava njihovu privatnost i sigurnost. To je kontradiktorno s dobivenim rezultatima istraživanja Domagoja Justamenta „Zaštita privatnosti na internetu“ (2017) gdje je dokazano da se većina korisnika interneta smatra adekvatno medijski pismenima. Postoji li problem s priznavanjem medijske (ne)pismenosti ili se tehnologija toliko brzo razvija da društvo teško prati taj napredak? Potrebno je istražiti u budućnosti.

S obzirom da je ovo istraživanje provedeno na uzorku od samo 10 sugovornika nije moguće generalizirati zaključke. Unatoč tome, dobiveni

rezultati se poklapaju sa navedenim sociološkim teorijama i prethodno napravljenim istraživanjima na ovu temu pa možemo biti poprilično sigurni da su doneseni zaključci valjani.

PREDVIĐANJA ZA BUDUĆNOST ZAŠTITE I PRIVATNOSTI PODATAKA

„Hitno je potrebno razviti novu zaštitu privatnosti, tehnike i metode koje se mogu oduprijeti analizi Velikih podataka. U tako velikom podatkovnom okruženju način zaštite privatnosti podataka posebno je važan. Zaštita privatnosti od analize Velikih podataka uglavnom se odnosi na dinamičku zaštitu privatnosti koja može odoljeti dubinskoj analizi povezanosti u okruženju velikih podataka. Poseban pristup je potreban da bi se postigla takva zaštita. Korištenjem desenzibilizacijskih tehnika kao što su anonimnost, konfuzija i dinamička kombinacija Velikih podataka bi moglo pomoći. Uz informacije i umrežavanje cijelog društva, ogromne količine podataka se prikupljaju, pohranjuju i koriste u ovom procesu“ (Zhong, S. i H., Yang, X., Shi, J., Xie, L., Wang, K., 2019:45). Stoga se može reći da je zaštita privatnosti od analize Velikih podataka temelj za daljnji razvoj u području Velikih podataka, a vrlo je važna i u perspektivnom području istraživanja. Autori stoga predlažu tri sljedeće točke za buduća istraživanja u ovom području:

• Razvoj različite privatnosti u različitim područjima primjene - zahtijeva daljnja istraživanja.

• Vrlo je važno dodatno poboljšati korisnost podataka nakon zaštite privatnosti, ili kako napraviti dobru ravnotežu između zaštite privatnosti, korisnosti i opsega primjene podataka, uz pretpostavku osiguravanja privatnosti podataka.

• Kako koristiti i integrirati postojeće i buduće metode zaštite privatnosti i konstruirati praktične alate i sustave za zaštitu privatnosti od analize Velikih podataka?

Iako većina korisnika interneta ne mari previše o svojim podacima i privatnosti, te koriste čestu uzrečicu „Nemam što skrivati“, Paul Bernal smatra da je prijedlog „ništa za skrivanje“ ustrajan, zavaravajući i manipulativan. Koristi se ne samo za opravdanje vladinog nadzora, već i za upad novinara u osobne živote slavnih, političara i javnosti. Umanjuje privatnost na drugoj razini: dobrim ljudima, prema ovoj logici, ne treba privatnost jer nemaju što skrivati, dok loši ljudi ne zaslužuju privatnost, pa kako smo svi dobri ili loši, ne treba imati privatnost. Doista, postalo je gotovo javna dužnost narušavati privatnost, kako za vlasti, tako i za medije, a polaganje prava na privatnost automatski vas čini sumnjičavim. Zagovornici privatnosti postaju prijatelji - možda „korisni idioti“ - kriminalaca i terorista, pedofila i dilera droge (2020:18). U prošlosti su se neki oblici podataka smatrali mnogo važnijima i mnogo osjetljivijima od drugih pa im je stoga pružana mnogo veća zaštita. Ovi osjetljivi podaci uključuju stvari poput političkih pogleda, seksualnosti, financija i zdravlja. U eri Velikih podataka ta zaštita postaje daleko manje učinkovita: ako možete izvući najosjetljivije podatke iz najobičnijih svakodnevnih podataka, tada bi svaka zaštita morala pokriti sve podatke, a ne samo osjetljive, a to je daleko manje praktično nego ikada u sadašnjem okruženju. Ovo je izazov kojim se zakon zapravo nije pozabavio i kojim se tehnološka industrija sasvim prirodno ne želi baviti. To je ipak izazov s kojim će se uskoro morati suočiti jer će korisnici shvatiti da se našu privatnost sustavno napada ne samo od strane korporacija, već i od strane vlasti. Izum weba započeo je proces koji ga je proširio od nečega što je bilo samo područje „štrebera“ do goleme mreže koja čini dio gotovo svakog aspekta svačijeg života. Razvoj poslovnih modela prvo Googlea, a zatim Facebooka ubrzao je proces i osigurao da su narušavanje privatnosti i prikupljanje osobnih podataka postali norma i kritični dio tog rasta i proširenja. Bit modela, odnosno usluge koje su „besplatne“ za korisnika u pozadini, zarađujući novac iskorištavanjem tih korisnika i njihovih osobnih podataka, radeći pomoću profiliranja i ciljanja, imao je mnogo utjecaja i mnoge potencijalne uporabe izvan onih koje su predviđene. Između ostalog, vlade svih vrsta iskoristile su potencijal koji bi to moglo pružiti. Rezultat je internet koji sada imamo: sveprožimajući, širi se po veličini i funkciji, neizbježan u gotovo svim društvima. Potencijal nisu iskoristile samo tvrtke i vlade. Od prevaranata i drugih kriminalaca do onih koji žele manipulirati našom politikom, primjene i

implikacije izrazito su uznemirujuće. To se dogodilo gotovo bez da smo toga svjesni i u velikoj mjeri bez poduzimanja odgovarajućih mjera bilo da to shvatimo ili se pozabavimo implikacijama. To se mora promijeniti jer ćemo ubrzo doći do točke bez povratka (2020:29).

No, nije sve tako crno. Postoje vrlo jasni znakovi da počinjemo nešto poduzimati po tom pitanju. Privatnost se pomaknula od opskurne teme za teoretičare zavjera do redovitih naslova vijesti, rasprave za političare i barem ponekad, prodajnog mjesta za tvrtke. Čak se i Facebook i Instagram i većina društvenih mreža sada plasiraju kao da privatnost shvaćaju vrlo ozbiljno, iako su na mnogo načina najveći krivci od svih u smislu narušavanja privatnosti, a posebno njezinog utjecaja. Čuvanje privatnosti u naslovima ključno je jer na njih vrši pritisak koji mogu imati značajan utjecaj na našu privatnost. Gledajući što bismo trebali učiniti u vezi s privatnošću interneta, prvo što treba naglasiti je ono što ne bismo trebali činiti jer dobar dio onoga što vlade posebno guraju nije samo neučinkovito, već izravno kontraproduktivno. Neke su politike u praksi najgore stvari koje možemo učiniti ne samo zbog privatnosti, već i zbog sigurnosti te zbog osobne i društvene slobode. Dva takva koncepta se posebno ističu: prava imena i šifriranje. Inzistiranja na korištenju pravih imena na društvenim mrežama i u virtualnom svijetu uopće ne bi trebalo biti. Iako u jednu ruku daje sigurnost ostalim korisnicima koji vas mogu prepoznati i biti sigurni da ste to vi, u drugu ruku daje istu priliku hakerima, kriminalcima i obmanama. Digitalni svijet se prenosi u stvarni svijet, ako netko zna vašu lokaciju, ime i prezime u online svijetu, zna to isto i u stvarnom. Također, enkripcija podataka, odnosno šifriranje je oslabilo kao koncept zbog upotrebe Velikih podataka. Zbog napretka tehnologije, postalo je i suviše lako pročitati šifrirane podatke te bi se stoga trebali šifrirati na drugačiji i kompliciraniji način. „Sigurnost i privatnost često se sukobljavaju, ali mora postojati kompromis s nultom sumom. Postoji način za usklađivanje privatnosti i sigurnosti: stavljanjem sigurnosnih programa pod nadzor, ograničavanjem buduće uporabe osobnih podataka i osiguravanjem da se programi provode uravnoteženo i kontrolirano“ (Solove, 2011:207). Korisnici počinju pokazivati da unatoč tome što prihvaćaju Facebook, stalo im je do privatnosti, u protivnom kršenje privatnosti ne bi učinilo glavne vijesti, a velike komercijalne organizacije ne bi učinile privatnost prodajnim mjestom.

Dobiveni su važni pravni slučajevi, od kojih su mnogi u obliku Davida i Golijata, s malim nevladinim organizacijama koje preuzimaju vlade i internetske divove. Takve situacije natjerale su sigurnosne i obavještajne službe u Velikoj Britaniji da otkriju mnogo više o njihovoj praksi nego prije, a to je potaknulo i druge države. Način na koji možemo pomoći u rastu ovih pozitivnih znakova od vitalnog je značaja, a podrška tim nevladinim organizacijama i aktivistima ključni je dio toga. Najvažnije od svega je pronaći način za promjenu paradigme. Privatnost bi trebala biti zadana vrijednost - a onima koji je žele ugroziti trebaju vrlo dobri razlozi za to te moraju dokazati te razloge, a ne čekati prigovore. U konačnici, pitanje je kakvu budućnost želimo: onu pogodnosti i kontrole, ili onu slobode i autonomije (Bernal, 2020:74).

ZAKLJUČAK

Razvoj tehnologije i potrošačkog društva doveo je do toga da je korisnicima neizbježno koristiti osobne podatke na svakodnevnoj bazi. Povezanost interneta i potrošačke kulture može se objasniti dvostrukom logikom – standardizacija i personalizacija. Internet je svima dostupan, a potrošačka kultura kroz njega vrši personalizaciju, odnosno refleksiju identiteta svakog korisnika pojedinačno. Internet je osmišljen kao mjesto slobode, povezanosti i zabave kroz virtualnu stvarnost. Svaka web stranica, svaka društvena mreža posjeduje svoje postavke privatnosti i „kolačiće“. Svaka online trgovina, odnosno web shop traži naše osobne podatke, e-mail, adresu, broj mobitela i tako dalje. Potraživanje takvih podataka je postalo toliko uvriježeno da nitko više ne pridaje pažnju tome. Kako bi pokušali utvrditi u kojem smjeru ide briga korisnika o svojim podacima i privatnosti na internetu, postoji li uopće digitalna privatnost te koliko zakoni i preporuke djeluju u svojoj svrsi, osmišljeno je kvalitativno istraživanje koje je provedeno na uzorku od 10 sugovornika. Svi su donekle upoznati s pojmovima vezanim za internetsku kulturu, ne osjećaju se sigurno na internetu, ali i dalje dijele osobne podatke i životne navike. Svjesni su da ne mogu upravljati svojim podacima na internetu i da se na njima zarađuje putem reklama i oglasa. Nadalje, svjesni su da se ne govori dovoljno o ovoj temi i ne znaju kome se treba obratiti u slučaju zlouporabe njihovih podataka. Svi

sugovornici smatraju da informatika treba biti obvezni predmet, da korisnici trebaju biti više informatički pismeni i da ih zakoni ne štite dovoljno.

Važnost privatnosti korisnika na internetu možda nije bila jasna kada se internet rasprostranio, no danas uz pregršt dostupnih informacija, trebala bi biti potpuno jasna. Tolika mogućnost zadiranja u privatnost svakog korisnika interneta i društvenih mreža ne treba biti normalna, uzevši u obzir koliko korisnici o tome znaju. Iako se priča o privatnosti korisnika na internetu povećala i dalje mnogi korisnici nisu prepoznali njenu važnost. Kako navodi Paul Bernal, to se mora promijeniti uskoro ako želimo pronaći put naprijed koji štiti stvari do kojih nam je doista stalo. Ono što je također vrijedno napomenuti je da gotovo svi oni koji žele umanjiti privatnost imaju nešto osobno u tom umanjivanju. Sigurnosne i obavještajne službe imale bi koristi ako bismo se svi odrekli privatnosti i dopustili da nam se u svako doba nametnu - ili barem vjeruju da bi im to koristilo. Slični ljudi poput McNealyja i Zuckerberga više bi voljeli da nema ograničenja u izvlačenju i korištenju osobnih podataka njihovih tvrtki, kako bi mogli zaraditi što više novca. „Umjesto uobičajenih argumenata, „nemam što skrivati“, zabluda sve ili ništa, trebamo se usredotočiti na važnija pitanja: Koje probleme određene sigurnosne mjere uzrokuju za privatnost i građanske slobode? Kako se ti problemi mogu ublažiti? Kakav bismo nadzor trebali imati nad mjerom sigurnosti? Koliko će sigurnosna mjera biti učinkovita? Možemo li zaštititi privatnost na način koji neće bitno smanjiti učinkovitost sigurnosne mjere?“ (Solove, 2011:208). Koliko god se ova tema bazirala na tehničkom i informatičkom znanju, toliko je bitna i u društvenim znanostima, poput sociologije, komunikologije, psihologije, politologije i tako dalje. Računalni stručnjaci se bave unaprjeđenjem sustava, programa i algoritama, a društvene znanosti na prvo mjesto stavljaju društvo, to jest korisnike interneta kojima je potrebno osvijestiti i ukazati na važnost privatnosti i zaštite podataka.

LITERATURA

Alexander, C. J., Pal, L. A. (2001.) Digitalna demokracija: politike i politika u umreženom svijetu, prev. Jurišić, K., Paić Jurinić, M., Osijek, Zagreb, Split: PAN LIBER.

Baudrillard, Jean (2001). Simulacija i zbilja. Zagreb, Naklada Jesenski i Turk. Hrvatsko sociološko društvo.

Baudrillard, Jean (2001). Simulakrumi i simulacija. Karlovac, Naklada DAGGK.

Berman, J. J. (2013), Principles of big data: preparing, sharing, and analyzing complex information, Elsevier, Morgan Kaufman, Amsterdam.

Bernal, P. (2020), What Do We Know and What Should We Do About Internet Privacy?, SAGE Publications Ltd.

Brautović, M. (2007.) „Zaštita privatnosti kod hrvatskih online medija“, Medijska istraživanja, sv. 13 (1): 51-67.

Castells, M. (2002/2007). „An Introduction to the Information Age” u: City: analysis of urban trends, culture, theory, policy, action. Routledge.

Castells, M. (2000). „Uspon umreženog društva, svezak 1. Informacijsko doba: Ekonomija, društvo i kultura“, Golden marketing, Zagreb.

Currie, S. (2013) „How is the internet eroding privacy rights?“, Referencepoint Press

Ivanušić, M. (2017.) „Etika i zaštita privatnosti“, diplomski rad, Sveučilišni centar Varaždin, Varaždin

Justament, D. (2017.) „Zaštita privatnosti na internetu“, diplomski rad, Sveučilište u Zagrebu, Hrvatski studiji, Zagreb.

Kocijan, K. (2014.) „Big Data: kako smo došli do velikih podataka i kamo nas oni vode“ U: Vrana, R. & Pečarić, Đ. (ur.) „Komunikacijski obrasci i informacijska znanost.“ Zagreb, Zavod za informacijske studije, str. 37-62.

Mejovšek, M. (2005.) „Metode znanstvenog istraživanja“ Jastrebarsko: Naklada Slap.

Miller, M. (2003.) „Apsolutna zaštita privatnosti PC-ja i privatnosti“, prev. D. Ivanišević, B. Zec, D. Marković, Čačak: Kompjuter biblioteka.

Nikodem, K. (2019.) „Teorije postmoderniteta“, predavanje Suvremene sociološke teorije 1, Filozofski fakultet Sveučilišta u Zagrebu.

Nikodem, K. (2019.) „Cyber kultura i društvo“, predavanje Sociologija Cyber kulture, Filozofski fakultet Sveučilišta u Zagrebu.

Nikodem, K. (2019.) „Pitanje identiteta u virtualnim svjetovima“, predavanje Sociologija Cyber kulture, Filozofski fakultet Sveučilišta u Zagrebu.

Rajko, A. (2011.) „Informacijsko upravno pravo (Pravo na pristup informacijama, zaštita osobnih i tajnih podataka)“ Zagreb, TEB - Poslovno savjetovanje.

Reeve, A. (2013.) „Managing Data in Motion: Data Integration Best Practice, Techniques and Technologies“, Morgan Kaufmann, Waltham.

Zhong, S. i H., Yang, X., Shi, J., Xie, L., Wang, K. (2019.) „Security and Privacy for Next-Generation Wireless Networks“, Springer Nature Switzerland AG.

Simon, P. (2013.) „Too Big to Ignore“, John Wiley & Sons, Inc., Hoboken, New Jersey.

Solove, J. D. (2011.) „Nothing to hide : the false tradeoff between privacy and security“, Set in Electra type by Integrated Publishing Solutions.

Waldman, A. (2018) „Privacy as Trust information privacy for an information age“, Cambridge University Press

Internetski izvori

Cambridge Analytica scandal https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (pristupljeno 15.06.2021.)

Diebold, F. X. (2000), „'Big Data' Dynamic Factor Models for Macroeconomic Measurement and Forecasting“ Discussion Read to the Eighth World Congress of the Econometric Society, Seattle, August, dostupno na: http://www.ssc.upenn.edu/~fdiebold/papers/paper40/temp-wc.PDF (pristupljeno 27.06.2021.).

Direktiva Europskog parlamenta i vijeća o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (2002.) EUR-Lex – Access to European Union law, http://eur-lex.europa.eu/legalcontent/HR/TXT/?uri=CELEX%3A32002L0058 (pristupljeno 01.07.2021.)

Djelatnost i unutarnje ustrojstvo Agencije, Agencija za zaštitu osobnih podataka, http://azop.hr/djelatnost-agencije (pristupljeno 08.07.2021.)

Edward Snowden upravo je iznio strastveni argument zašto je privatnost najvažnije pravo. https://www.businessinsider.com/edward-snowden-privacy-argument-2016-9 (pristupljeno 10.09.2021.)

Global Internet Privacy Study Reveals Consumers' Confilicting Views (2014.) Dell EMC, https://www.emc.com/about/news/press/2014/20140612-01.htm (pristupljeno 12.06.2021.)

Kako Internet stvari pomaže i mijenja našu svakodnevicu? https://ec.europa.eu/croatia/How_IoT_is_helping_and_changing_our_everyday_life_hr (pristupljeno 08.07.2021.)

Percepcija zaštite podataka i pitanja privatnosti među djecom i mladima (2012.) Agencija za zaštitu osobnih podataka, http://azop.hr/images/dokumenti/251/istraivanjepitanjeprivatnostiizatitaosobnihpodatakadjeceimladih.pdf (pristupljeno 08.07.2021.)

Povijest i razvoj interneta (2013.) Djeca medija, http://www.djecamedija.org/?p=2522 (pristupljeno 15.08.2021.)

Privatnost na Internetu (2013.) Totalweb, http://www.totalwebseo.com/hr/blog/2013/rujan/privatnost-zastita-podataka-na-internetu (pristupljeno 15.08.2021.)

Statistički podaci o informacijskom društvu – kućanstva i pojedinci. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:Statisti%C4%8Dki_podaci_o_informacijskom_dru%C5%A1tvu_%E2%80%93_ku%C4%87anstva_i_pojedinci&oldid=216793 (pristupljeno 10.09.2021.)

Što je krađa identiteta?, Agencija za zaštitu osobnih podataka, u daljnjem tekstu AZOP http://azop.hr/aktualno/detaljnije/kradaidentiteta-i-kako-se-zastititi (pristupljeno 08.07.2021.)

Veliko istraživanje: Dominacija interneta u Hrvatskoj sve veća (2017.) 24sata, http://www.24sata.hr/tech/veliko-istrazivanje-dominacija-interneta-u-hrvatskoj-sveveca-518278 (pristupljeno 16.08.2021.)

Zakon o elektroničkim komunikacijama (2017.) Zakon.hr – pročišćeni tekstovi zakona, https://www.zakon.hr/z/182/Zakon-o-elektroničkim-komunikacijama (pristupljeno 19.08.2021.)

Zakon o informacijskoj sigurnosti (2017.) Zakon.hr – pročišćeni tekstovi zakona, https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti (pristupljeno 19.08.2021.)

Zakon o zaštiti osobnih podataka (2017.) Zakon.hr – pročišćeni tekstovi zakona, https://www.zakon.hr/z/220/Zakon-o-zaštiti-osobnih-podataka (pristupljeno 19.08.2021.)

Zaštita osobnih podataka u RH, Agencija za zaštitu osobnih podataka, http://azop.hr/images/dokumenti/217/zastita_op_rh.pdf (pristupljeno 19.08.2021.)

SAŽETAK

Privatnost korisnika na internetu i zaštita njihovih podataka postaje sve važnija tema današnjice. Virtualni svijet postaje dio svakodnevnog načina života te korisnici dijele svoje privatne podatke i fotografije koje mogu biti

zlouporabljene. Postavlja se pitanje koliko je digitalna privatnost moguća i u kojoj mjeri korisnici mogu utjecati na nju? Istraživanje je provedeno na 10 sudionika iz različitih geografskih područja u Republici Hrvatskoj, različitih zanimanja i dobnih skupina. Fokus istraživanja je stavljen na zaštitu podataka, osjećaj sigurnosti u dijeljenju istih, zlouporabu i stavove o personaliziranim reklamama i oglasima. Nakon provedenog istraživanja možemo zaključiti da su korisnici zabrinuti za svoju digitalnu privatnost, ali da ne poduzimaju potrebne korake kojima bi se osigurali. Nisu svjesni opasnosti zlouporabe podataka što je danas sve češći problem te smatraju da ta tema nije dovoljno zastupljena u društvu.

Ključne riječi: internet, digitalna privatnost, zaštita podataka, zlouporaba podataka, reklame.

SUMMARY

The privacy of users on the Internet and the protection of their data is becoming an increasingly important topic today. The virtual world thus becomes an integral part of everyday life and users are sharing their private data and photos which can be misused. The question is to what extent is digital privacy possible and to what extent can users influence it? The research was conducted on 10 participants from different geographical areas in the Republic of Croatia, different occupations and age groups. The focus of the research was on data protection, a sense of security in sharing it, abuse and attitudes about personalized ads and advertisements. After conducting research we can conclude that users are concerned about their digital privacy but they do not take the necessary steps to ensure it. They are not aware of the dangers of data misuse which is an increasingly common problem today and they believe that this topic is not sufficiently represented in society.

Keywords: Internet, digital privacy, data protection, data misuse, personalized ads.