Stavovi, znanje i zabrinutost studenata o zaštiti podataka na Internetu

Nikolić, Josip

SVEUČILIŠTE U ZAGREBU
FAKULTET HRVATSKIH STUDIJA

Josip Nikolić

STAVOVI, ZNANJE I ZABRINUTOST STUDENATA O ZAŠTITI OSOBNIH PODATAKA NA INTERNETU

DIPLOMSKI RAD

Zagreb, 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET HRVATSKIH
STUDIJA

ODSJEK ZA KOMUNIKOLOGIJU

DIPLOMSKI RAD

STAVOVI, ZNANJE I ZABRINUTOST STUDENATA O ZAŠTITI OSOBNIH PODATAKA NA INTERNETU

Student: Josip Nikolić
Mentorica: doc. dr. sc. Jelena Jurišić
Sumentorica: dr. sc. Vanesa Varga

Zagreb, rujan 2021.

Sažetak

Internet je olakšao svakodnevicu svojih korisnika omogućivši nadilaženje prostorno-vremenskih barijera. Također je ponudio nove načine komunikacije, rada, zabave, informiranja i edukacije, no te pogodnosti često idu ruku pod ruku s ugrozama za osobne podatke korisnika. Sukladno razvoju interneta razvijena je i upravljačka struktura naziva *internet governance* koja se bavi razvojem i primjenom načela, normi, pravila, postupaka donošenja odluka i programa koji oblikuju evoluciju i upotrebu interneta, a čine ju nacionalne vlade, privatni sektor i civilno društvo. Upravo je ta struktura zaslužna za današnji izgled i način funckioniranja interneta. Danas se većina internetskih stranica oslanja na metode prikupljanja podataka kako bi sakupili velike količine podataka o svojim korisnicima i time stvorili korisničke profile od kojih imaju profitabilne koristi. Neke najčešće metode prikupljanja podataka su: „kolačići“, otisci prstiju na pretraživaču i internetskim stranica, *web beacon* itd. Međutim, neželjeno prikupljanje podataka može se spriječiti korištenjem metoda zaštite podataka. Neke metode zaštite podataka na internetu su: korištenje *firewall-a*, korištenje antivirusnih aplikacija, uključivanje „Do-Not-Track“ sigurnosne funkcije pretraživača, korištenje VPN mreža, brisanje „kolačića“ itd. Također, postoje i razni pravni akti koji štite pojedinčevo pravo na zaštitu privatnosti među kojima se najviše ističe Opća uredba o zaštiti podataka kao najvažnija pravna regulativa kojom se regulira zaštita podataka unutar Europske unije.

Ovaj diplomski rad bavi se pitanjima privatnosti i zaštite osobnih podataka na internetu, a za njegove potrebe provedeno je i istraživanje putem mrežne ankete o stavovima, znanjima i zabrinutosti studenata Sveučilišta u Zagrebu o sigurnosti osobnih podataka na internetu. Istraživanje je provedeno na uzorku od dvjesto studenata koji studiraju na deset najvećih sastavnica Sveučilišta u Zagrebu po broju studenata. Istraživanjem je otkriveno da se znanja, stavovi i zabrinutosti razlikuju među studentima s obzirom na fakultet koji pohađaju, razinu studija na kojoj se nalaze, prosječnu ocjenu i dnevno korištenje interneta.

Ključne riječi: *internet, osobni podaci, GDPR, medijska pismenost, informacijska pismenost*

Abstract

Internet has made everyday life easier for its users by enabling them to overcome space-time barriers. It has also offered them new ways to communicate, work, entertain, inform and educate, but these benefits often go hand in hand with threats to users' personal data. With the development of the Internet, a structure called Internet governance has been developed that develops and implements principles, norms, rules, decision-making procedures and programs that shape the evolution and use of the Internet. It consists of national governments, the private sector and civil society. It is this structure that is responsible for today's appearance of the Internet and the way the Internet functions. Today, most websites rely on data collection methods to collect large amounts of data about their users and thus create user profiles from which they benefit profitably. Some common data collection methods are: „cookies", browser and website fingerprinting, web beacons etc. However, unwanted data collection can be prevented by using data protection methods. Some common data protection methods on the Internet are: use of firewalls, use of antivirus applications, activation of "Do Not Track" security features of browsers, use of VPN networks, deletion of "cookies" etc. Also, there are various legal acts that protect the individual's right to privacy on the Internet among which the General Data Protection Regulation stands out as the most important legal act regulating data protection within the European Union.

This thesis deals with issues of privacy and protection of personal data on the Internet, and for its needs, an online survey was conducted to discover attitudes, knowledge and concerns of students at the University of Zagreb about the security of personal data on the Internet. The research was conducted on a sample of two hundred students studying at the ten largest constituents of the University of Zagreb. The research found that knowledge, attitudes and concerns differ among students with regard to the faculty they attend, their graduate level, their average grade and daily internet use.

Keywords: *Internet, personal data, GDPR, media literacy, information literacy*

Sadržaj

1. UVOD

Iako internet sa sobom nosi mnoge funkcije koje uvelike olakšavaju svakodnevne aktivnosti svih nas poput neograničenog educiranja, informiranja i zabave, on donosi i mnoge opasnosti, a tu spadaju i opasnosti za osobne podatke korisnika koji mogu biti ukradeni ili preuzeti bez odobrenja ili znanja korisnika. Danas su razvijene mnoge metode prikupljanja osobnih podataka te se ti podaci prikupljaju u razne svrhe. Iako se prikupljanje osobnih podataka najčešće spominje u kontekstu marketinških namjena, osobni podaci često su meta *cyber* napada koje vrše *cyber* kriminalci radi zloupotrebe istih, ili čak državni akteri i privatni sektor, zbog čega je važno imati na umu tko stoji iza sveprisutnog upravljanja internetom (Wheatley, Maillart i Sornette, 2016:1). Također navode da prosječni financijski gubitak zbog krađe ili preuzimanja pojedinog osobnog podatka korisnika iznosi 213 američkih dolara, što ide u korist tvrdnji da su osobni podaci sve više etiketirani kao sredstva kojima se može trgovati, odnosno da nose vrijednost koja se može novčano odrediti (ibid). Meglena Kuneva (2009, prema: Spiekermann et al., 2015:161) govori o osobnim podacima kao „nafti“ interneta i valuti digitalnog svijeta kako bi dočarala da su informacije koje se odnose na pojedince postale presudna imovina u digitalnoj ekonomiji. Sve više organizacija danas se bavi trgovanjem podacima tako da prikupljaju, objedinjuju, pakiraju i preprodaju podatke korisnika, čineći to uglavnom bez da prosječni korisnik zamijećuje da se to događa (Spiekermann et al., 2015:165).

1.1. Predmet rada

Važnost zaštite podataka raste kako količina stvorenih i pohranjenih podataka nastavlja rasti neviđenom brzinom. Činjenica da ljudi sve više vremena provode na internetu ostavljajući sve više svojih osobnih podataka na mreži znači da je sve više osobnih podataka internetskim tvrtkama na raspolaganju za prikupljanje, korištenje i dijeljenje, a to može dovesti do gubitka kontrole nad vlastitim podacima. Korisnici interneta često nisu svjesni količine i vrste podataka koja se o njima otkriva samim *surfanjem* na internetu. Osobne podatke na internetu korisnici ostavljaju, dobrovoljno ili nedobrovoljno, svojom mrežnom aktivnošću, bilo da je riječ o korištenju e-pošte, foruma, internetskih igara ili korištenjem internetskog bankarstva, mrežnih trgovina i učenja putem interneta. Uzmemo li u obzir da danas više od 60 % svjetske populacije, odnosno 4,66 milijarde ljudi (Kemp, 2021), koristi internet, što znači da jednako toliko ljudi samom svojom prisutnošću na internetu otkriva podatke o sebi koji ulaze u ogromne baze osobnih podataka raznih aktera, te da internet nema granica niti globalno propisana

ograničenja, dolazimo do zaključka da je privatnost danas gotovo nemoguće održati ukoliko se ne poduzmu sigurnosne mjere na internetu. Međutim, korisnicima interneta ne prijeti samo narušavanje privatnosti od strane internetskih tvrtki, već i od raznih napadača koji te podatke mogu zlorabiti npr. radi krađe identiteta. Neke od prijetnji koje nastaju prikupljanjem osobnih podataka korisnika su: ranjivost na prijevare, narušavanje privatnosti, neželjene marketinške komunikacije te ciljane, nametljive marketinške komunikacije koje remete ritam svakodnevnih aktivnosti (Martin i Murphy, 2016:135).

1.2. Ciljevi i metoda istraživanja

Glavni je cilj istraživanja u sklopu ovoga diplomskog rada utvrditi postoje li razlike u poznavanju internetskih politika privatnosti i načina prikupljanja podataka te razlike u zabrinutosti oko ugroženosti osobnih podataka na internetu među studentima s obzirom na fakultet koji pohađaju. Naime, želimo usporediti znanja i stupanj zabrinutosti studenata deset najvećih sastavnica Sveučilišta u Zagrebu, među kojima se nalaze fakulteti s vrlo različitim studijskim programima, te zaključiti postoji li fakultet/i čiji studenti pokazuju veće znanje i veći stupanj zabrinutosti za osobne podatke. Također, odredili smo tri sporedna cilja istraživanja koja ćemo predstaviti u poglavlju *4.1. Ciljevi i hipoteze istraživanja*.

Istraživanje izvodimo mrežnim anketnim upitnikom. S obzirom na to da je istraživanje provedeno za vrijeme pandemije bolesti COVID – 19 uzrokovane SARS-CoV-2 virusom, za istraživanje smo odabrali metodu mrežne ankete koja nam omogućuje sigurnu distribuciju i ispunjavanje upitnika. Osim razloga povezanih s pandemijom ovu smo metodu odabrali kako bismo omogućili sudionicima potpunu anonimnost i pogodnost rješavanja upitnika bilo gdje (kod kuće, u autobusu/tramvaju itd.), u bilo kojem trenutku i preko raznih uređaja (računalo, mobilni telefon, tablet).

1.3. Struktura rada

Ovaj je diplomski rad podijeljen u 13 poglavlja. Rad započinjemo teorijskim dijelom u kojem objašnjavamo i opisujemo najvažnija pitanja teme zaštite osobnih podataka na internetu nakon

kojeg slijedi istraživački dio u kojem ispitujemo znanja, zabrinutost i stavove studenata Sveučilišta u Zagrebu o tim istim pitanjima.

U drugom poglavlju rada dotičemo pojam upravljanja internetom (engl. *Internet governance*) te ga objašnjavamo kao upravljačku strukturu interneta koja se sastoji od raznih aktera; privatnog sektora, tehnoloških tvrtki, civilnog društva, nacionalnih vlada, akademske zajednice i međunarodnih organizacija. Treće poglavlje posvećeno je objašnjavanju čestih metoda prikupljanja osobnih podataka. U tom smo poglavlju posvetili tri potpoglavlja objašnjavanju najraširenijih metoda prikupljanja osobnih podataka koje internetske tvrtke koriste, a to su: „kolačići“, otisci prstiju na pretraživaču i *web beacon*. Predstavili smo i druge metode prikupljanja osobnih podataka u potpoglavlju *Ostale metode prikupljanja osobnih podataka u svrhu njihove zloupotrebe*. Četvrto poglavlje posvećeno je objašnjavanju metoda zaštite osobnih podataka od neželjenog prikupljanja. Neke od metoda koje smo u tom poglavlju objasnili su: antivirusni softveri, VPN mreže, *Ad blocker* dodaci za pretraživač, korištenje snažnih lozinki itd. Peto pogavlje rada dotiče pravne aspekte zaštite osobnih podataka na internetu, odnosno najvažnije zakone Republike Hrvatske koji osiguravaju zaštitu privatnosti i osobnih podataka. Šesto poglavlje posvećujemo predstavljanju Opće uredbe o zaštiti podataka iz razloga što je ona najvažnija pravna regulativa koja regulira pitanje zaštite osobnih podataka. Potpoglavlja ovoga su poglavlja posvećena objašnjavanju svakog pojedinačnog prava kojeg ova regulativa omogućuje. U posljednjem, sedmom, poglavlju teorijskog dijela rada objašnjavamo pojmove medijske, informacijske, informatičke i digitalne pismenosti; objašnjavamo razlike među tim pojmovima i navodimo zašto su kompetencije u sklopu tih pismenosti važne za studente. Također, u tom smo poglavlju naveli nekoliko istraživanja koja su do sada među studentima provedena na tim područjima kako bismo rezultate tih istraživanja usporedili s rezultatima našeg istraživanja.

Osmim poglavljem počinje istraživački dio rada. Što se tog dijela rada tiče, odlučili smo ispitati kako o pitanju sigurnosti osobnih podataka na internetu razmišljaju oni od kojih se zbog njihovog odrastanja u digitalnom okružju očekuje visoka razina znanja o internetu i načinima funkcioniranja interneta, a to su sadašnji studenti. U prvom potpoglavlju osmog poglavlja predstavili smo hipoteze našeg istraživanja koje smo izveli iz ciljeva istraživanja. U drugom potpoglavlju istog poglavlja objašnjavamo zašto smo za istraživanje odabrali metodu mrežnog anketnog upitnika te metodu snježne grude za uzorkovanje. Zatim slijedi potpoglavlje u kojem predstavljamo strukturu našeg anketnog upitnika, odnosno kategorije postavljenih pitanja i od kuda su pitanja preuzeta. Anketu istraživanja ispunilo je dvjesto studenata koji studiraju na

deset najvećih sastavnica Sveučilišta u Zagrebu po broju studenata. Po broju studenata najveće sastavnice Sveučilišta u Zagrebu su: Ekonomski fakultet, Pravni fakultet, Filozofski fakultet, Prirodoslovno-matematički fakultet, Fakultet elektrotehnike i računarstva, Medicinski fakultet, Učiteljski fakultet, Kineziološki fakultet, Fakultet organizacije i informatike (Varaždin) i Fakultet strojarstva i brodogradnje. Studentima je poslana anketa koja se sastoji od 19 pitanja, a koja ispituju demografska obilježja sudionika, načine njihovog korištenja interneta, znanje o zaštiti osobnih podataka i metodama koje internetske tvrtke koriste za prikupljanje osobnih podataka na internetu, njihovu razinu zabrinutosti u vezi vlastitih podataka na internetu te korake koje poduzimaju kako bi ih zaštitili.

U devetome smo poglavlju predstavili rezultate našeg istraživanja. Rezultate smo prikazali pomoću tablica i grafikona radi lakše vizualizacije dobivenih odgovora. Deveto smo poglavlje podijelili na potpoglavlje u kojem analiziramo odgovore sudionika na pitanja anketnog upitnika s obzirom na fakultet koji pohađaju i potpoglavlje u kojem analiziramo odgovore sudionika na pitanja s obzirom na trenutnu razinu studija, prosječnu ocjenu tijekom studija i dnevnu učestalost korištenja interneta.

Nakon predstavljanja rezultata, u desetom poglavlju slijedi rasprava. U desetom smo poglavlju, dakle, temeljem prethodne analize odgovora objasnili jesu li prethodno postavljene hipoteze opovrgnute ili potvrđene.

U jedanaestom smo poglavlju predstavili naše zaključke koje smo izveli na temelju rezultata dobivenih istraživanjem. U dvanaestom poglavlju predstavljamo korištenu literaturu kojom smo se vodili u teorijskom i istraživačkom dijelu rada. Posljednje poglavlje rada je prilog koji se sastoji od anketnog upitnika koji je poslan sudionicima istraživanja.

2. UPRAVLJANJE INTERNETOM I METODE PRIKUPLJANJA OSOBNIH PODATAKA

Internet kao svjetski sustav povezivanja odlikuju karakteristike otvorenosti, međupovezanosti i transnacionalnosti, stoga je i upravljanje internetom, kao skup procesa koji usmjerava evoluciju interneta, definirano sličnim karakteristikama. Upravljanje internetom, odnosno *Internet governance*, odnosi se na upravljačku strukturu interneta te podpovršinske procese i pravila koja ga oblikuju.

2. 1. Tko upravlja internetom?

Na Svjetskom summitu o informacijskom društvu (2005) upravljanje internetom definirano je kao razvoj i primjena načela, normi, pravila, postupaka donošenja odluka i programa koji oblikuju evoluciju i upotrebu interneta od strane vlada, privatnog sektora i civilnog društva (prema Kurbalija, 2014:5). Dakle, vlade, privatni sektor i civilno društvo akteri su upravljanja internetom, no za njega su važne i međuvladine organizacije za pitanje koordinacije državne politike u vezi s internetom, internetske organizacije za upravljanje i razvoj tehničkih standarda i politika u vezi s internetom te akademske zajednice koje pokrivaju istraživački aspekt tehničkog i administrativnog upravljanja internetom (RNIDS, 2021). Neke od funkcija upravljanja interneta su: administriranje internetskih resursa poput imena i brojeva, uspostava internetskih tehničkih standarda, koordinacija pristupa i međusobnog povezivanja, upravljanje kibernetičkom sigurnošću itd. (DeNardis, 2015:114). Ovakav oblik upravljanja u kojem više aktera igra značajnu ulogu u upravljanju zove se *multistakeholder* pristup, a definira ga „puno sudjelovanje svih dionika, donošenje odluka zasnovano na konsenzusu i djelovanje na otvoren, transparentan i odgovoran način“ (Stickling, 2012, prema Calandro, 2016:4). O takvom distribuiranom načinu upravljanja govori i činjenica da se pravila za internet mogu stvoriti na različite načine i na različitim razinama, sudjelovanjem niza dionika (IGF Berlin, 2019).

Jedan od najvažnijih aktera upravljanja internetom je organizacija ICAAN (engl. *Internet Corporation for Assigned Names and Numbers*). Naime, ICAAN je neprofitna organizacija koja upravlja središnjim spremištem za IP adrese i koja pomaže u koordinaciji isporuke IP adresa te koja upravlja domenskim sustavom imena (*Data Foundry,* 2016). Pod njenim se upravljanjem nalazi preko 180 milijuna naziva domena i četiri milijarde mrežnih adresa u 240 zemalja, što znači da njene funkcije održavaju osnovnu tehnološku infrastrukturu interneta (*Data Foundry,* 2016). Pod skupinu aktera koji čine tehnološku osnovu interneta

spada i IEFT (engl. *Internet Engineering Force*), međunarodna zajednica mrežnih dizajnera, operatora, dobavljača i istraživača koji se bave razvojem internetske arhitekture i koja postavlja mnoge tehničke standarde za internet (IETF, 2021). Brojne druge organizacije također imaju važnu ulogu u postavljanju standarda i tehničkih temelja interneta. Takva je organizacija i W3C (engl. *World Wide Web Consortium)* koja se fokusira na aspekte poput poboljšanja tehnologija i formata HTML koda koji se koristi na internetskim stranicama, ali i mnoge druge (IGF Berlin, 2019).

No, imenovanje i numeriranje samo je mali dio upravljanja internetom. Privatni sektor također ima velik utjecaj na oblikovanje interneta. Pravila i uvjeti korištenja internetskih stranica koje privatne tvrtke postavljaju u obliku Općih uvjeta korištenja (engl. *General Terms and Conditions of Use*) uređuju što korisnici mogu raditi na njihovim stranicama. Sukladno tome, privatne tvrtke na internetu izravno provode javnu politiku o pitanjima povezanim s privatnošću, slobodom govora, provedbom intelektualnih prava, internetskim zlostavljanjem i drugim područjima koja izravno utječu na pojedinačne građanske slobode kroz svoje Opće uvjete korištenja (DeNardis, 2015:115). Iz toga se razloga govori o pojavi dodatne uloge privatnih poslovanja kao komponente u regulatornom globalnom režimu koji se trenutno oblikuje oko novih tehnologija, prvenstveno interneta na kojem se privatne tvrtke mogu podignuti na razinu autoriteta zbog toga što drže kontrolu nad većinom internetskih infrastruktura (Bislev i Flyverbom, 2021:8). Moć privatnog sektora leži u sposobnosti kontrole, pristupa, objavljivanja i zadržavanja informacija, a činjenica da otprilike 90 - 95 % informacija razmijenjenih na internetu prolazi kroz intrenteske stranice privatnog sektora govori o utjecaju kojeg imaju na internetu i informacija koje imaju o korisnicima (Gamal Sayed Elsayed Eid, 2020:9). Pri tome, moć na internetu se definira kao skup resursa koji se odnose na stvaranje, kontrolu i komunikaciju elektroničkih i računalnih informacija (Nye, Jr., 2014:1). Ta se moć može „koristiti za stvaranje poželjnih ishoda u internetskom prostoru ili pomoću *cyber* instrumenata za postizanje poželjnih ishoda u drugim domenama izvan *cyber* prostora“ (Nye, Jr., 2014:1 – 2). Laura DeNardis (2012) tvrdi da je to dovelo do pojačane uloge privatnih tvrtki u regulaciji sadržaja i upravljanju izražavanjem, ali i u ograničenjima u izražavanju (prema Musiani, 2013). Problem te moći je to što privatni sektor nije izabran od strane naroda, nema odgovornost i obuhvaća velik dio američkih tvrtki, a svoj legitimitet povlači iz tehničke stručnosti i sposobnosti zadovoljavanja interesa civilnog društva (Gamal Sayed i Elsayed Eid, 2020:10). Uloga privatnog sektora kao važnog kreatora politike na interenetu odnosi se na ograničeni broj najvećih tehnoloških korporacija, poput Googlea,

Facebooka i Microsofta koje dobivaju ogromne ovlasti i odgovornosti, a tu moć moraju prilagoditi tako da istodobno pokazuju društvenu odgovornost i pritom dokazuju da ne razmišljaju isključivo u smislu privatnog interesa i dobiti (Bislev i Flyverbom, 2008:9). Privatne tvrtke mogu surađivati na provedbi specifičnih pravila i procesa na internetu zajedno s javnim vlastima i civilnim društvom (France Diplomacy, 2020). Dakle, u upravljanju internetom, javna i privatna regulativa često se preklapaju te se zato javlja izraz „regulirane samoregulacije" koji se odnosi na aranžman u kojem tvrtke reguliraju same sebe, dok ih država nadgleda kako bi osigurala onakvo funkcioniranje sustava kakvo se zahtijeva (IGF Berlin, 2019).

Unatoč velikom utjecaju tehnoloških i privatnih tvrtki na strukturu interneta, nacionalne vlade su akteri koji također svojim zakonima utječu na to što se smije i što se ne smije na internetu, a samim time utječu na oblik i mogućnosti interneta. Nacionalni parlamenti, uz institucije Europske unije i druge međuvladine organizacije donose zakone za određena područja upravljanja internetom. Zadaće nacionalnih vlada u upravljanju internetom prvenstveno se odnose na kontroliranje i donošenje zakona o autorskim pravima, intelektualnom vlasništvu, *cyber* sigurnosti i zaštiti podataka i druge zadaće unutar nacionalnih pravnih okvira (Nye, Jr., 2016:2). Joseph Samuel Nye Jr. (2016:3) navodi da je pružanje sigurnosti tipična funkcija vlade, a neki vjeruju da će rastuća nesigurnost (podataka i korisinika) dovesti do povećane uloge nacionalnih vlada na internetu. Isti autor također navodi da vlade žele zaštititi internet kako bi njihova društva mogla imati koristi od njega, ali istovremeno žele zaštititi svoja društva od onoga što bi moglo doći putem interneta (2016:3). Međutim, upravljanje internetom sve se više promatra pod pretpostavkom da se dobro funkcionirajući sustav može održati samo međunarodnom suradnjom, što je iznjedrilo nove oblike globalnog upravljanja (Nonnecke, 2016:2). Stoga se ne može govoriti o primarno državno upravljanom internetu, već *multistakeholder* pristupu upravljanju u kojem su nacionalne vlade samo jedan od dionika upravljanja internetom. Na istom Svjetskom summitu o informacijskom društvu na kojem je definiran pojam upravljanja internetom nastao je i Forum o upravljanju internetom (IGF) na inicajtivu Ujedinjenih naroda (dalje u teksu: Forum). Forum je godišnji, globalni forum za dijalog o pitanjima internetske politike te je mjesto za iskrene i pravovremene rasprave među dionicima na ravnopravnoj osnovi. Forum informira one koji imaju moć donošenja politika u javnom i privatnom sektoru (od predstavnika vlada do predstavnika civilnog društva) (IGF, 2021). Jedan od ciljeva Foruma je i to da se šira društvena

zajednica uključi u raspravu o upravljanju intrenetom, a ne da tu raspravu vode samo državnici (CARNET, 2021).

Kao što je spomenuto, civilno društvo također je jedan od dionika u upravljanju internetom u *multistakeholder* modelu upravljanja. Organizacije civilnog društva uključuju nevladine organizacije, udruge i zaklade okupljene radi zagovaranja interesa građana (Bežovan, 2002). Utjecaj civilnog društva na regulaciju interneta očituje se akcijama poput oblikovanja javne agende kroz kampanje, uključivanja u procese političkog odlučivanja ili olakšavanja potrage za zajedničkim vrijednostima u vezi s novim tehnologijama i aplikacijama (IGF Berlin, 2019). Većina se inicijativa civilnog društva u pogledu interneta usmjerava prema omogućavanju pristupa informacijama i znanju ili robi proizvedenoj na internetu. Primjer takve inicijative je FSF (engl. *Free Software Foundation*), zaklada za promicanje slobode korisnika računala putem promicanja takvog licenciranja računalnih softvera koji omogućuje slobodan pristup, upotrebu i izmjenu koda od strane korisnika (IGF Berlin, 2019). Važnost civilnog društva u informacijskom društvu prepoznata je još na prvom Svjetskom summitu o informacijskom društvu u Ženevi gdje je osnovan Ured za civilno društvo (engl. *Civil Society Bureau*). Osnutak Ureda za civilno društvo predstavlja prekretnicu u povijesti Ujedinjenih naroda i međunarodnih pregovora time što civilno društvo prvi put ima mehanizme koji olakšavaju dijalog s vladama (Purcell et al., 2006:8). Funkcije Ureda za civilno društvo uglavnom su organizacijske prirode, odnosno s ciljem maksimiziranja sudjelovanja civilnog društva u pitanjima informacijskog društva. Civilno društvo dobiva dodatni poticaj za sudjelovanje u upravljanju internetom osnivanjem Foruma 2006. godine. Forumom je stvoreno mjesto na kojem svi dionici *multistakeholder* upravljanja internetom mogu raspravljati o internetu, dodatno je olakšana koordinacija i rasprava pitanja javnih politika povezanih s internetom te je omogućeno ravnopravno sudjelovanje vlada, privatnog sektora i civilnog društva u raspravi (Purcell et al., 2006:13). Također navode (2006:14) navode da formuliranje odgovarajućih i legitimnih javnih politika koje se odnose na upravljanje internetom zahtijeva puno i značajno sudjelovanje nevladinih dionika. Kako bi se to ostvarilo, odnosno kako bi se evolucija interneta kretala u skladu s javnim interesom, važno je da svi dionici bolje razumiju kako funkcioniraju osnove upravljanja internetom, preciznije, upravljanje sustavom domenskih imena, dodjela IP adresa itd. (ibid). Važnost Foruma očituje se i u tome što omogućuje dionicima iz svih zemalja, uključujući zemlje u razvoju, priliku da se uključe u raspravu o upravljanju internetom te im omogućuje da stvore znanje i vještine koje će im olakšati sudjelovanje u upravljanju internetom (IGF, 2021). Forum funkcionira na način da glavni

tajnik Ujedinjenih naroda svake godine imenuje Savjetodavnu skupinu (engl. *Multistakeholder Advisory Group*) koju čine grupa stručnjaka koji predstavljaju sve skupine dionika, dakle 50 do 55 članova iz vlada, privatnog sektora, civilnog društva, akademske i tehničke zajednice, koji određuju program Foruma (IGF, 2021).

Dakle, može se reći da u određenim apektima, međunarodne organizcije poput Ujedinjenih naroda oblikuju internet i više od nacionalnih vlada, što je vidljivo na primjeru osnivanja i godišnjeg održavanja međunarodnog Foruma. Također, Opća skupština Ujedinjenih naroda bavi se pitanjima koja se odnose na upravljanje internetom u svojim rezolucijama o privatnosti u digitalno doba i međunarodnoj *cyber* sigurnosti (IGF Berlin, 2019). Osim Ujedinjenih naroda, velik broj drugih međunarodnih organizacija na regulacijama koji izravno ili neizravno utječu na internet, npr. Opća uredba o zaštiti podataka Europske unije ili trgovinska pravila Svjetske trgovinske organizacije (IGF Berlin, 2019).

Ono po čemu se upravljanje internetom razlikuje od drugih globalnih pordučja djelovanja je to što ono zahtijeva uključivanje različitih dionika koji se razlikuju u mnogim aspektima. Zbog toga se u članku 49. deklaracije Svjetskog summita o informacijskom društvu određuju uloge glavnih dionika. Naime, ovim se člankom države, odnosno nacionalne vlade, određuju kao nadležno tijelo za javne politike povezane s internetom (uključujući međunarodne aspekte), dok se privatni sektor zadužuje za razvoj interneta, kako na tehničkom, tako i na ekonomskom polju (Kurbalija, 2021:8). Civilno društvo ima važnu ulogu u smislu koordinacije pitanja javnih politika povezanih s internetom na području zajednice, dok je uloga internacionalnih organizacija razvoj internetskih tehničkih standarda i relevantne politike (Kurbalija, 2021:8).

Iz svega navedenog proizlazi da je upravljanje internetom vrlo složeno područje koje obuhvaća niz aspekata, uključujući tehnologiju, socio-ekonomiju, pravo i politiku.

Ugroženost osobnih podataka samo je jedna od opasnosti na internetu. Zbog toga i zbog velikog značaja interneta, potrebno je ekonomijama i društvima omogućiti učinkovito funkcioniranje na način da ih se zaštiti na internetu. Neke prijetnje na internetu su sljedeće: presretanje podataka, interferencija podataka, ilegalni pristup, *spyware* i *malware*, *botnet* mreže, korupcija podataka, sabotaža, DoS (engl. *denial-of-service*) napad i krađa identiteta (engl. *phishing*) (Internet Governance for Libraries, 2021:5), a njh ćemo detaljnije objasniti u sljedećem poglavlju. Potencijalni napadači mogu biti kriminalci, anarhisti, haktivisti, revolucionari, teroristi, tajne službe i obrambene i vojne jedinice, dok žrtve mogu biti pojedinci,

ali i privatne tvrtke, organizacije civilnog društva, medijski subjekti i javne institucije, vojske i dr. (Internet Governance for Libraries, 2021:5). Sigurnost na internetu jedan je od aspekata na kojem postoje i globalni i regionalni pothvati da se stavi pod univerzalnu regulativu. U području sigurnosnih aspekata upravljanja internetom međunarodne organizacije imaju najznačajniju ulogu. To se vidi po tome što Ujedinjeni narodi imaju Grupu međuvladinih stručnjaka (UN GGE) koja ima od 2004. godine radi na polju informacijske sigurnosti. Ured UN-a za droge i kriminal (UNODC) također je vrlo aktivan u borbi protiv *cyber* kriminala, a Međunarodna telekomunikacijska unija (ITU) pokrenula je nekoliko aktivnosti na području *cyber* sigurnosti kao što su Globalna agenda za kibernetičku sigurnost (GCA) i Globalni indeks kibernetičke sigurnosti (GCI) (Internet Governance for Libraries, 2021:6).

2.2 Metode prikupljanja osobnih podataka na internetu

U prethodnom poglavlju naveli smo neke od ugroza na internetu, među kojima prevladavaju opasnosti koje se tiču osobnih podataka korisnika. Iako se upravljanje internetom kreće prema sve sigurnijem internetskom okolišu uvođenjem regulativa koje osobne podatke vraćaju pod kontrolu korisnika, postoje metode prikupljanja podataka koje zaobilaze regulacije te se sakupljaju velike količine podataka o nama našom aktivnošću na internetu.

Nove tehnologije ne samo da nude obilje metoda koje organizacije mogu koristiti za prikupljajanje i pohranu informacija, već ljudi učestalo rado dijele svoje podatke. Dakle, korisnik može dobrovoljno predati osobne podatke na internetu (npr. popunjavanjem obrazaca) ili se podaci mogu prikupiti bez njihovog znanja analizom IP zaglavlja, HTTP zahtjeva, upita u tražilicama ili čak upotrebom JavaScript-a i Flash programa ugrađenih u internetske stranice (Bujlow et al., 2017:1). To omogućuje mrežnim posrednicima podataka, tražilicama, sakupljačima podataka i mnogim drugim akterima na internetu da profiliraju ljude u razne svrhe kao što su poboljšanje marketinga kroz bolju statistiku i radi sposobnosti predviđanja ponašanja potrošača, a osim instrumentalizacije podataka, oni se mogu i zlorabiti (Aïmeur i Lafond, 2013:821). Aïmeur i Lafond (2013:821) navode da osobni podaci koje takvi sakupljači podataka mogu sakupiti na internetu mogu biti identifikacijski podaci (ime, dob, spol, adresa, telefonski broj, zanimanje, bračni status itd.), obrasci kupnje (trgovine koje se redovito posjećuju, računi, imovina itd.), navigacijske navike (posjećene web stranice, učestalost posjeta, pseudonimi koji se koriste na forumima, poznanstva na mreži itd.), podaci o načinu

života (hobiji, ponašanje na putovanjima, odmori itd.), osjetljivi podaci (medicinski ili kazneni podaci), ili biološke informacije (krvna grupa, genetski kod, otisci prstiju).

Dakle, osobni podaci su postali novi izvor ekonomske vrijednosti, jer kada su ti podaci obrađeni i klasificirani, pružaju relevantne informacije tvrtkama o interesima i aktivnostima ljudi, što je izuzetno korisno za oglašavanje. Zbog toga se govori da su neke od najvećih današnjih tvrtki, poput Googlea i Facebooka, izgrađene na ekonomiji osobnih podataka (Esteve, 2017:36). No, osim u svrhu ciljanog oglašavanja, velike količine osobnih podataka na internetu prikupljaju se radi personalizacije rezultata pretraživanja, procjene financijske vjerodostojnosti, vladinog nadzora, radi krađe identiteta itd. (Bujlow et al., 2017:1).

2.2.1. „Kolačići“

Oglašavanje prilagođeno korisnicima prevladavajući je oblik oglašavanja na internetu, a temelji se na poslovnom modelu kojeg karakterizira nadzor korisnika, prodaja prikupljenih podataka tvrtkama za oglašavanje i predviđanje karakteristika, preferencija i aktivnosti korisnika, u stvarnom vremenu, što uvelike ugrožava privatnost korisnika interneta (Angwin i McGinty 2010, prema Sipior, Ward i Mendoza, 2011:1). Jedna od najraširenijih metoda internetskog praćenja i prikupljanja informacija su „kolačići“ (engl. *cookies*). „Kolačići“, zajedno s drugim metodama prikupljanja podataka poput „web-pratilica“ (engl. *web-beacon*) i otiska internetskog preglednika (engl. *browser fingerprinting*), nude trgovcima priliku da prikupe mnoštvo informacija o potrošačkim karakteristikama i preferencijama korisnika. Informacije prikupljene „kolačićima“ koriste se za poboljšanje segmentacije tržišta i ciljani marketing kako bi se potrošači dosegnuli na individualnoj osnovi (Sipior, Ward i Mendoza, 2011:2).

„Kolačići“ su zapravo datoteke koje sadrže nizove tekstualnih znakova koji kodiraju relevantne informacije o korisniku (ime i prezime, broj kreditne kartice, adresa stanovanja itd.) prilikom posjete internetskoj stranici. Oni funkcioniraju na način da se nizovi tekstualnih znakova šalju na tvrdi disk ili RAM korisnika dok korisnik posjećuje internetsku stranicu koja koristi „kolačiće“. Internetski poslužitelj dohvaća podatke korisnika iz tih „kolačića“ kada se korisnik kasnije vrati na istu internetsku stranicu (Park i Sandhu, 2000:36). U tom smislu, svrha je „kolačića“ prikupljanje podataka za upotrebu u narednim komunikacijama bez traženja istih podataka (ibid). Osim toga, uloge „kolačića“ uključuju autentifikaciju korisnika, praćenje korisnika ili ciljano oglašavanje.

Postoje razne vrste „kolačića“. „Kolačići“ prve strane su oni koje postavljaju internetske stranice koje korisnik posjećuje te ih samo te internetske stranice mogu pročitati, a svrha im je omogućiti vlasniku internetske stranice da prikupi analitičke podatke o posjetiteljima te da olakšaju posjetiteljima korisničko iskustvo npr. pamćenjem postavka jezika ili lozinke (Cahn et al., 2016:1). U širokoj su upotrebi i „kolačići“ treće strane. To su „kolačići“ koje postavlja domena koja se razlikuje od one koja je prikazana na adresnoj traci preglednika, a uglavnom ih na internetske stranice postavljaju tvrtke za posredovanje u podacima (npr. Axiom, Datalogix i Epsilon), mrežni oglašivači i aplikacije za praćenje (npr. Google Analitika) (Cahn et al., 2016:1).

S obzirom na to da je jedan od primarnih ciljeva tvrtki za posredovanje podataka i mrežnih oglašivača prikupiti što više podataka o korisnicima u svrhu prikazivanja ciljanih oglasa, korištenje „kolačića“ iznimno im je bitan dio strategije zbog velike količine informacija koje se njima otkrivaju o korisnicima. Naime, podatke sakupljene putem „kolačiće“ tvrtke mogu koristiti za izradu visoko informativnog profila pojedinog korisnika ili potrošača do kojih bi bilo vrlo teško, ako ne i nemoguće, doći iz bilo kojeg drugog izvora, a ti im profili pomažu u ciljanom oglašavanju, odnosno omogućavanju pojedinačno relevantnog iskustva kupnje (Mitchell, 2012:1). Razlog zašto internetske stranice dopuštaju postavljanje „kolačića“ treće strane (npr. nezavisnih oglašivača) je to što ih ta treća strana često u zamjenu za kolačiće podržava besplatnim sadržajem, analizom prometa itd. (Mitchell, 2012:3).

„Kolačići“ predstavljaju prijetnju privatnosti iz razloga što prate ponašanje korisnika prilikom „surfanja“ na internetu i to ponašanje ostaje zapisano u tekstualnom zapisu, zbog čega je važno imati u vidu mogućnost brisanja „kolačića“ putem internetskog preglednika. Često korisnici nisu svjesni da a je tekstualna datoteka o njihovoj internetskoj aktivnosti postavljena na njihov tvrdi disk. Tome pomaže činjenica da je zadana postavka većine internetskih preglednika dopuštenost svih „kolačića“, uključujući „kolačiće“ treće strane. No, većina internetskih preglednika u svojim postavkama dopušta mogućnost prihvaćanja i odbijanja kolačića, omogućavajući tako korisnicima da isključe postavljanje „kolačića“ na svoj tvrdi disk. Problem u tome je to što veliki broj internetskih stranica zahtijeva obavezno prihvaćanje „kolačića“ za pristup njima, zbog čega isključivanje „kolačića“ na internetskom pregledniku samo sprečava korisnika da pristupi većini internetskih stranica (Mitchell, 2012:3). Stoga je kod stranica koje zahtijevaju obavezno prihvaćanje privatnosti važno proučiti kakve opcije privatnosti ta stranica nudi te koju vrstu „kolačića“ koristi, odnosno koje će informacije ostati zapisane pri pristanku na „kolačiće“. Proučavanje opcija privatnosti umjesto slijepog

prihvaćanja svih „kolačića“ važno je zbog štetnih učinaka „kolačića“ koji mogu proizaći upravo iz komercijalne eksploatacije prikupljenih podataka koji se mogu prenositi na druge poslužitelje, a čije prikupljanje uključuje i osjetljive podatke poput seksualne ili vjerske orijentacije, financijskih i kliničkih podataka (Couto, 2013:95). S obzirom na to da su „kolačići“ tekstualni zapisi koje je lagano pročitati, podaci koje oni otkrivaju lako se mogu dohvatiti, pregledati i krivotvoriti. Postoje razne vrste napada koji se koriste u svrhu razotkrivanja „kolačića“. Tzv. „njuškanje predmemorije“ (engl. *cache sniffing*) može se dogoditi ako napadač pristupi korisnikovom pregledniku ili predmemoriji *proxy* servera, tada napadač može dobiti i sadržaj „kolačića“. „Njuškanje XSS kolačića“ događa se kada internetska aplikacija zlonamjerno prikuplja podatke od korisnika. XSS napadi (engl. *cross-site scripting,* odnosno skriptiranje na više lokacija) omogućuju otmicu računa, promjenu korisničkih postavki, lažno oglašavanje te omogućuju napadaču dohvaćanje „kolačića“ iz kojih može izvući podatke (ENISA, 2011:7). U istome izvoru (2011:7) stoji da „kolačići“ stoga prijete privatnosti korisnika jer napadaču ne samo omogućuju prikupljanje osobnih podataka, već i njihovu izmjenu.

2.2.2. Otisci prstiju na pretraživaču i internetskim stranicama

Otisci prstiju na pretraživaču (engl. *browser fingerprinting*) odnose se na skup tehnika koje su oglašivači i druge tvrtke razvili kao način praćenja i prikupljanja podataka o korisnicima, bez korištenja „kolačića“. Naime, korištenje otisaka prstiju na pretraživaču odnosi se na upotrebu skupa atributa dobivenih iz korisnikova preglednika, kao što su informacije o instaliranim fontovima ili dodacima za preglednik, u svrhu jedinstvenog prepoznavanja okruženja surfanja bez kolačića (Upathilake, Li i Matrawy, 2015:1). Iz istoga izvora (2015:1) saznajemo i definiciju otisaka prstiju na internetskim stranicama (engl. *website fingerprinting*) kao oblik analize prometa gdje napadač promatra šifrirane podatke i pokušava izvući zaključke iz određenih značajki prometa.

Praćenje otisaka prstiju na pretraživaču omogućeno je, među ostalim, korištenjem značajki preglednika kao što su Flash ili Java za dohvaćanje podataka o instaliranim fontovima, dodacima, platformi preglednika i razlučivosti zaslona (Upathilake, Li i Matrawy, 2015:2). Ova metoda funkcionira na način da osobe koja prikupljaju otiske šalju više upita putem značajki preglednika (npr. Flash ili Java) kako bi izdvojili različita svojstva sustava. Zatim kombiniraju prikupljena svojstva kako bi generirali identifikator (ili otisak prsta) za preglednik

(FaizKhademi, Zulkernine i Weldemariam, 2015:293). Praćenje otisaka prstiju na pretraživaču moguće je s jedne strane jer dnevnici pristupa internetskom mjestu na poslužitelju mogu prikupljati podatke koje šalje korisnikov preglednik, a to su obično traženi protokol i URL, IP adresa koja traži, korisnički agent preglednika itd. (Watson, 2020).

S druge strane, slanjem upita kroz već spomenute Java i Flash značajke moguće je praćenje jedinstvenih podataka o korisnikovom uređaju. Korištenjem Flash značajke predaju se sljedeće informacije: cjelokupni popis fontova, identifikacijski brojevi matične ploče i drugih *hardwarea,* IP adresa itd. (Multilogin, 2017). Takvi dodaci poput Flash-a već otkrivaju puno informacija, ali i sam popis dodataka također može biti otisak prsta. (Multilogin, 2017). Proces praćenja otisaka prstiju je neprimjetan za korisnike i ne ostavlja nikakve tragove na pretraživaču. Metoda otisaka prstiju na pretraživaču obično se koristi za internetsko praćenje korisnika, a široko je raširena jer je to tajniji način praćenja ljudi od korištenja kolačića za koje je potreban pristanak. Uglavnom se prikupljeni podaci ovom metodom praćenja koriste za oglašavanje i prilagodbu iskustva na mreži na način da pomoću otiska prsta (značajki uređaja) znaju je li korisnik posjetio već stranicu, izrađuju profile ponašanja ili stvaraju prateće oglase (Latto, 2021).

Otisci prstiju na internetskim stranicama koriste napadači čiji cilj je identificirati sadržaj (tj. internetske stranice kojima korisnik pristupa) šifriranih i anonimnih veza promatrajući obrasce protoka podataka (Panchenko et al., 2016:1). Preciznije, cilj napadača je ovom metodom saznati informacije o korisnikovim aktivnostima pregledavanja interneta prepoznavanjem obrazaca u njegovom prometu. Ova metoda omogućuje prepoznavanje internetskih stranica koje je korisnik posjetio, unatoč njihovoj upotrebi alata za privatnost kao što su VPN mreže ili sustava anonimnosti poput Tor-a. Napadač, koji može biti davatelj internetskih usluga korisnika ili netko tko njuška korisnikovu bežičnu vezu, identificira internetske stranice u šifriranoj vezi analizirajući i prepoznajući obrasce mrežnog prometa, a najnovije inačice mogu nadvladati postojeću obranu (Shan et al., 2021:1). Ovom metodom napadač koristi samo meta informacije, poput veličine paketa i smjera prometa, bez prekida kodiranja (Panchenko et al., 2016:1). Internetske stranice mogu pomoću takvog digitalnog otiska prsta doznati prijašnje posjete, stvoriti profile ponašanja ili stvoriti oglase da prate korisnika.

2.2.3. Web beacon - internetski bug

Web beacon (dalje u tekstu: *beacon*) invanzivna je metoda prikupljanja podataka poznata i pod nazivima internetski *bug*, prateći *bug*, piksel za praćenje itd. To je zapravo malena grafička sličica koja je smještena u kod internetske stranice ili komercijalne e-pošte kako bi pružatelj usluga mogao nadzirati ponašanje posjetitelja stranice ili pošiljatelja/primatelja e-pošte (*Web Beacon*, 2021). Dakle, beaconi su ugrađeni, često nevidiljivi dio internetske stranice. Kada preglednik učita internetsku stranicu, a stranica ima ugrađen beacon, preglednik upućuje zahtjev za preuzimanje slike (Zabawa, 2020:6). To je moguće jer svaki beacon na sebe ima vezan HTML kod za preuzimanje te sličice koja kada je preuzeta može prenijeti napadaču informacije poput IP adrese uređaja koje je dohvatilo sliku, kada je beacon pregledan itd.(Zabawa., 2020:6). Sama veličina sličice, koja je često veličine 1x1 piksela, omogućuje izuzetno brzo preuzimanje bez ometanja korisnika. Na temelju informacija dobivenih beaconom tvrtke predviđaju korisnikove mrežne radnje, jer oni pružaju mogućnost izrade određenih profila ponašanja korisnika kombiniranjem dobivenih informacija sa zapisnicima poslužitelja (*Web Beacon*, 2021). Beaconi također mogu otkriti i sve postojeće kolačiće koji pripadaju istom vlasniku internetske stranice (Zabawa, 2020:6)

No, beaconi ne moraju nužno biti zlonamjerni. Ako su vlasnici transparentni o tome kako koriste beacon i koje se informacije prikupljaju od korisnika, onda se beacon koristi na legalan način bez narušavanja privatnosti korisnika u svrhu razumijevanja ponašanja korisnika i praćenja uspjeha oglasnih kampanja (*What is a Web Beaco*n, 2020). U slučajevima ugradnje beacona u tijelo komercijalne e-pošte, beaconi funkcioniraju na isti način kao i na internetskim stranicama te mogu oglašivaču pružiti mjerne podatke kao što je pročitanost e-pošte ili je li korisnik kliknuo poveznicu e-pošte (Zabawa, 2020:6).

2.2.4. Ostale metode prikupljanja osobnih podataka u svrhu njihove zlouporabe

Neke od metoda prikupljanja podataka u svrhu njihove zlouporabe također su: ilegalno presretanje podaraka, interferencija podataka, *botnet* mreže, *spyware* programi itd.

Ilegalnim presretanjem podataka smatra se kada osoba bez zakonitog opravdanja tehničkim sredstvima presreće bilo koji nejavni prijenos u, iz ili unutar računalnog sustava ili ako se presreću elektromagnetske emisije iz računalnog sustava koje prenose računalne podatke (*Model Law on Computer and Computer Related Crime*, 2017:7). Ivica Kokot

(2014:313) navodi da za razliku od klasičnog prijenosa i dostave pošiljaka, upotreba informacijsko-telekomunikacijskih tehnologija uključuje brojne pružatelje usluga i mjesta na kojem se podaci mogu presresti. Podaci se smatraju u prijenosu sve dok nisu došli do krajnjeg odredišta, bilo sustava bilo primatelja ili sve dok primatelj ne ostvari pristup tim podacima, a presretanje je neovlašteno kada se presreću podaci koji se nalaze u nejavnom prijenosu. Isti autor (2014:313) navodi da se kriminalizacijom neovlaštenog presretanja zaštita širi s podataka koji se nalaze u računalnom sustavu i na podatke u prijenosu. Kazneno djelo ilegalnog presretanja podataka propisano je člankom 3. Konvencije o kibernetičkom kriminalu Vijeća Europe.

Interferencija podataka događa se kada osoba namjerno ili nepromišljeno, bez zakonitog opravdanja uništi ili izmijeni podatke, čini podatke besmislenim, beskorisnim ili neučinkovitim. Interferencijom podataka smatra se i kada osoba ometa ili prekida zakonitu upotrebu podataka ili uskraćuje pristup podacima bilo kojoj osobi koja ima pravo na njih te ako prekida ili ometa bilo koju osobu u zakonitom korištenju podataka (*Model Law on Computer and Computer Related Crime*, 2017:7). Ono po čemu se interferencija podataka razlikuje od presretanja podataka je to što presretanje podataka utječe na podatke tijekom postupka prijenosa, dok druga utječe na podatke tijekom njihove pohrane. Najčešći način izvršavanja intereferencije podataka uključuje unošenje zlonamjernih kodova, poput virusa i trojanskih konja (Bande, 2018:17). Konvencija o o kibernetičkom kriminalu zabranjuje interferenciju podataka člankom 4.

Botnet mreže također su pošasti koje ganjaju neoprezne korisnike interneta. Kako bi se objasnio pojam *botnet* mreža, važno je prvo definirati *botove*. Naime, *bot* je skraćenica riječi robot, a odnosi se na aplikaciju koja može izvesti i ponoviti određeni zadatak brže od čovjeka. Kada se velik broj *botova* proširi na nekoliko računala i međusobno se poveže putem interneta, oni tvore skupinu koja se naziva *botnet* mreža, a to je mreža *botova* (Eslahi et al., 2012:349). Problem *botneta* je to što je *bot* je dizajniran da zarazi uređaje (npr. računala ili mobilne telefone), i učini ih dijelom *botneta* bez znanja njihovih vlasnika, a to se događa pod nadzorom osobe koja se zove *botmaster*. *Bomtaster* pokušava dobiti kontrolu nad tim uređajima i provoditi svoje zlonamjerne aktivnosti na njima (Eslahi et al., 2012:349).

Sumirano, *botnet* mreže su mreže privatnih računala zaraženih zlonamjernim softverom koja se kontrolira kao grupa bez znanja vlasnika. Najčešća motivacija za stvaranje *botnet* mreža je ostvarivanje profita. *Botnet* mreže se mogu proširiti na kućne, poslovne i

obrazovne mreže, dok istovremeno pokrivaju brojne autonomne sustave kojima upravljaju različiti davatelji internetskih usluga (Stevanović i Pedersen, 2013:1). Ishodi *botnet* napada su različiti, variraju od od sporih performansi zaraženog uređaja do velikih računa za internet i ukradenih osobnih podataka (*What is a botnet attack?*, 2021). Podaci ukradeni sa zaraženog uređaja se zatim koriste u podle svrhe, poput krađe identiteta, prijevara s kreditnom karticom, slanja neželjene e-pošte, napada na internetske stranice i distribucija zlonamjernog softvera.

Sljedeća kategorija opasnosti za osobne podatke na internetu spada pod široki pojam *spyware* programa. *Spyware* se odnosi na kategoriju aplikacija dizajniranih za daljinsko praćenje i izvještavanje o korisničkim aktivnostima računala (Metz, 2004, prema Stafford i Urbaczewski, 2004:291). Autori navode (ibid) kako je prosječno 28 *spyware* programa instalirano po korisniku. U osnovi je to špijunski softver koji uspostavlja kontrolu nad korisnikovim računalom bez njegovog/njezinog pristanka i izvještava treću stranu o ponašanju korisnika na tom računalu. Pod informacije o kojima *spyware* izvještava treću stranu spadaju korisnikove aktivnosti na internetu, odnosno internetske stranice koje posjećuje i podatke koje skuplja i/ili dijeli.

Najpoznatiji *spyware* programi su: *Adware* – programi koji nadgledaju aktivnost pregledavanja korisnika na mreži i šalju ciljane oglase na radnu površinu korisnika na temelju te aktivnosti pregledavanja te koji mogu promijeniti zadane postavke internetskog preglednika, *Keystroke Loggers* - softver za nadzor dizajniran za bilježenje pritiska tipki koje je napravio korisnik, često bez dopuštenja ili znanja korisnika, *Trojanski konj* - zlonamjerni računalni program koji se lažno predstavlja kao neki drugi program s korisnim ili poželjnim funkcijama, često se predstavaljaju kao besplatni softver za preuzimanje, poput računalne igre ili *peer-to-peer* programa za razmjenu datoteka (Stafford i Urbaczewski, 2004:291).

S obzirom da pod *spyware* spadaju svi programi koji prate aktivnost korisnika bez njegova/njezinog znanja, postoji još mnogo vrsta *spywarea* koje ćemo dotaknuti u sljedećem poglavlju. Oni, naime, rade u pozadini računala bez znanja korisnika i smanjuju performanse procesora i memorije te na kraju usporavaju ukupne performanse računala. Dakle, glavna svrha *spyware* programa je prikupljanje podataka i slanje istih sakupljaču informacija.

Važno je napomenuti da se *spyware* može postaviti i uz pristanak korisnika, ali bez njegovog/njenog znanja. To se postiže uključivanjem klauzula o *spywareu* u ugovoru o licenci za krajnjeg korisnika (EULA), zbog čega je uvijek potrebno pročitati uvjete i odredbe prilikom instaliranja programa ili preuzimanja datoteka s interneta (Klang, 2003:315). Osim što se

spyware koristi za prikazivanje prilagođenih oglasa, osobni podaci koje prikupljaju *spyware* programi mogu dovesti i do krađe identiteta, a mogu i nanijeti financijsku štetu korisniku preuzimanjem podataka o kreditnim karticama korisnika, a zabrinjavajuće je to što spyware može postaviti svatko tko želi znati nešto o drugoj osobi i njegove/njezine računalne navike.

Anti-spyware programi učinkovita su zaštita od s*pyware* programa, no za zaštitu podata ipak je najbolja zaštita svijest o prijetnjama koje predstavljaju legalne i ilegalne primjene spyware tehnologije, jer će se priroda prijetnje za korisnike računala s vremenom razvijati i prilagođavati razvoju *anti-spryware* programa (Stafford i Urbaczewski, 2004:301).

3. ZAŠTITA OSOBNIH PODATAKA

Činjenica da danas samim korištenjem interneta, odnosno pukim pretraživanjem, korisnici odaju veliku količinu informacija o sebi, poduzimanje koraka za zaštitu podataka sada je potrebnije više nego ikad. Zaštita podataka nužna je prvenstveno zbog rastućeg broja metoda za prikupljanje osobnih podataka te kako bi korisnici interneta spriječili neželjene i nepredviđene posljedice takvog prikupljanja poput zlouporabe podataka, financijskih gubitaka i *cyberbullyinga*.

3.1. Metode zaštite osobnih podataka

U niz tehničkih rješenja za internetsku privatnost i internetsku zaštitu podataka spadaju korištenje vatrozida (engl. *firewall*) te antivirusnih i *antispyware* softvera, koje je potrebno redovito ažurirati radi povećanja učinkovitosti. Vatrozid je sustav koji uspostavlja politiku ograničenja pristupa između dviju mreža (Sundaram, 2017). On, dakle, može biti softverski - specifični softver pokrenut na pojedinom računalu ili mrežni - namjenski uređaj odgovoran za zaštitu jednog ili više računala, s time da obje vrste vatrozida potiču korisnika da iznese pravila pristupa za dolazne veze te obje vrste uglavnom dolaze s unaprijed definiranim sigurnosnim smjernicama (Sundaram, 2017). ograničava vanjskim stranama pristup podacima pod kriterijima koje korisnik postavlja, a nakon postavljanja tih kriterija vatrozid pregledava svaku dolazeću, ali i odlazeću, poruku, informaciju ili podatak ulazne veze i blokira one koje ne udovoljavaju postavljenim sigurnosnim kriterijima. Zbog toga što većina vatrozida nudi mogućnost konfiguracije koja zaustavlja izvlačenje podataka iz baze podataka i krađe podataka, a i zbog toga što bilježe svaki pokušaj neodobrenog pristupa uređaju i podacima na uređaju, vatrozid se u zaštiti privatnih podataka smatra prvom linijom obrane (*The Role of Firewalls in Defending Your Data*, 2020).

Antivirusni softveri otkrivaju, popravljaju, čiste i/ili uklanjaju virusom zaražene datoteke i zlonamjerne softvere (Phua, 2009:15). Zbog toga što oglašivačke tvrtke sve agresivnije prate korisnike interneta putem softvera za praćenje koji potajno špijuniraju surfanje i ponašanje korisnika, kao i konfiguraciju uređaja i druge osjetljive podatke, ali i zbog velikog broja zlonamjernih hakera koji plasiraju raznorazne *malware* programe na internetu, kvalitetni antivirusni softveri danas su dizajnirani ne samo da brane uređaj i korisnika od prijetnji već i da spriječe neželjeni odljev osjetljivih podataka (*Data Protection or Virus Protection?*, 2016). Antivirusni softver skenira sve informacije koje ulaze i izlaze iz

korisnikovog uređaja, uspoređuje ih sa svojom bazom podataka već poznatih virusa i *malwarea* kako bi pronašao podudaranja te bilježi koje datotoke napuštaju uređaj u mrežnom prometu. Podudaranja koja su slična ili identična bazi podataka izoliraju se, skeniraju i uklanjaju (*How does Antivirus Work?,* 2020).

S obzirom na to da postoji veliki broj različitih antivirusnih softvera te da je tehnološki okoliš prikupljanja podataka promjenjiv, preporučuje se osnovno razumijevanje funkcioniranja softvera koje može pomoći pri odluci koja vrsta antivirusa je najpogodnija za zašitu podataka (*How does Antivirus Work?,* 2020). Pomoću kombinacije metoda otkrivanja, antivirusni softver može otkriti sve vrste poznatih zlonamjernih softvera, uključujući ali ne ograničavajući se na *ransomware, adware, spyware*, trojanske programe itd., dok neki napredniji antivirusi također imaju dodatne, naprednije značajke za otkrivanje *cyber* prijetnji kao što su zaštita preglednika i *anti-phising* alatne trake za zaštitu od krađe identiteta putem *phishing* e-pošte i web lokacija za krađu identiteta, („How does Antivirus Work?“, 2020).

Kao što je spomenuto u prošlome poglavlju, *spyware* programi su softveri instalirani na korisnikov uređaj bez njegovog/njenog znanja ili pristanka, a koji može nadgledati korisnikove mrežne aktivnosti i pritom prikupljati osobne podatke. Zaštita od špijunskog softvera uključena je u neke antivirusne softvere, ali postoje i zasebni softveri s isključivo antispyware značajkama (*Protect Your Computer from Viruses, Hackers, & Spies*, 2015). *Antispyware* programi funkcioniraju na sličan način kao i antivirusi, bez prestanka skeniraju korisnikov uređaj tražeći *spyware* kojeg uklanjaju ako ga pronađu. Kako bi se uključile antispyware značajke antivirusnog softvera važno je proučiti dokumentaciju za upute o aktiviranju istih. Spyware programi se mogu izbjeći i preuzimanjem dokumenata samo s pouzdanih izvora, izbjegavanjem veza u skočnim prozorima ili u neželjenoj e-pošti, čitanjem uvjeta korištenja pri instaliranju aplikacija te izbjegavanjem interaktivnih igara na mreži (*Protect Your Computer from Viruses, Hackers, & Spies,* 2015).

S obzirom na to da su javno otvorene Wi-Fi mreže ozbiljna prijetnja osjetljivim i privatnim podacima zbog toga što je teško znati tko drugi koristi mrežu i nadzire njen promet, VPN (Virtual Private Network) po tom pitanju služe kao efikasno rješenje za zaštitu privatnosti internetskih korisnika. VPN je je privatna mreža koja služi kao način omogućavanja sigurne komunikacije između članova grupe korištenjem javne telekomunikacijske infrastrukture, održavanjem privatnosti korištenjem protokola za tuneliranje i sigurnosnim postupcima. (Jaha, Shatwan i Ashibani, 2008:309).

VPN mreže su uglavnom zasnovane na pretplatama, što znači da korisnik mora preuzeti program od svog davatelja usluge i prijaviti se na određeno vrijeme kako bi mogao koristiti privatnu mrežu za zaštitu, no postoje i besplatne VPN mreže (Sharma i Kaur, 2020: 2336). Prednosti korištenja VPN-a su to što te mreže omogućuju zaobilaženje restrikcija povezanih s geolokacijom te osiguravaju privatnost na internetu spajanjem na privatnu mrežu koja šifrira prijenos podataka (Sharma i Kaur, 2020:2337).

U suštini, VPN je mreža koja spajanjem na server, koji se može nalaziti bilo gdje u svijetu, stvara „tunel“ koji omogućuje siguran prijenos privatnih podataka putem javne mreže.

Čitanje politika privatnosti internetskih stranica također je efikasna metoda zaštite privatnosti. Svrha politika privatnosti internetskih stranica je informirati korisnike o praksama organizacije po pitanju rukovanja podacima kako bi korisnici smatrali organizaciju koja se obvezuje na privatnost korisnika vjerodostojnom, a samim time i potaknuti korisnike na sudjelovanje u internetskim transakcijama na toj stranici (Pollach, 2007:104). Međutim, zbog duljine i složenosti tipičnih po1itika privatnosti koju objavljuju tvrtke, korisnicima je teško protumačiti istu te zbog toga imaju i smanjenu motivaciju za čitanje i razumijevanje. Takvim obeshrabrivanjem korisnika da čitaju politike, tvrtke se odriču mogućnosti ublažavanja zabrinutosti u vezi s privatnošću i izgradnje povjerenja (Pollach, 2007:104).

Danas gotovo svaka internetska stranica koja prikuplja podatke ima politiku privatnosti kojoj korisnici mogu pristupiti kako bi pročitali praksu privatnosti organizacije. Bez čitanja politike privatnosti, primjerice, korisnici ne znaju hoće li tvrtka slati neželjenu poštu nakon što donesu odluku o davanju svoje adrese e-pošte, stoga pomoću politike privatnosti oni mogu provjeriti zaštitu privatnosti prije nego što posluju sa stranicom (McDonald i Cranor, 2008:6). Čitanje politike privatnosti važno je i zato što su neke korporacije stava da bi njihovi korisnici trebali pročitati politiku privatnosti tvrtke, a ako to ne učine, to je dokaz nedostatka brige o privatnosti, zbog čega u politike privatnosti mogu ukomponirati prikupljanje podataka s vrlo malo ograničenja (McDonald i Cranor, 2008:22).

Sljedeći korak u očuvanju internetske privatnosti tiče se odabira lozinki za korisničke račune na internetu. Naime, vjerodajnice za pristup korisnika poput korisničkog imena i lozinki napadačima su vrlo vrijedan resurs, jer one napadačima omogućuju neovlašteni pristup podacima lažnim predstavljanjem, što je iznimno opasno ako korisnik koristi istu lozinku za sve račune na internetu (Information Commissioner's Office, 2014:22). Korištenje jednostavnih lozinki također je opasno jer takve lozinke mogu predložiti obrazac koji napadač

može koristiti za pogađanje drugih lozinki, zbog čega treba izbjegavati korištenje datuma rođenja ili imena kućnog ljubimca kao lozinke za račune s osjetljivim podacima (ibid). Takve lozinke napadačima je lako „dešifrirati“ pukim nagađanjem. Također, napadač može stvoriti lažnu internetsku stranicu koja mami korisnike besplatnim sadržajem ako se registriraju s korisničkim imenom i lozinkom, stoga se, uz korištenje različitih lozinki, preporuča i redovito mijenjanje lozinki kako napadač jednim Snaga lozinke može se povećati stvaranjem duge lozinke koristeći širok raspon znakova, npr. kombinaciju znakova koja se sastoji od velikih slova, malih slova, brojeva, interpukcijskih znakova i drugih simbola. Time se smanjuje šansa da napadač nagađanjem ostvari pristup računu, a tome pomaže i izbjegavanje upotrebe riječi iz rječnika gdje je to moguće (ibid).

„Kolačići“ i otisci prstiju na pretraživaču samo su neke od metoda koje se koriste za akumulaciju golemih količina podataka o korisnicima na internetu. Akumulirani podaci uglavnom se koriste za prikazivanje personaliziranih oglasa korisnicima. Google, kao najveća svjetska internetska tražilica i prikazivač oglasa, većinu praćenja svojih korisnika vrši putem njihovih korisničkih računa (Esteve, 2017:39). Dakle, Google prikuplja osobne podatke koje korisnici dobrovoljno nude kada se prijave na Google račun ili kada stvore javno vidljivi Google profil, no glavni Googleov izvor osobnih podataka su podaci iz „upita pretraživanja" koje pojedinci unose kada pretražuju sadržaj koji pruža Google (tu spada i YouTube) i koji omogućava Googleu da automatski prati ponašanje korisnika (ibid). Praćenje im olakšava i korištenje kolačića, čime dobivaju informacije i s drugih internetskih stranica. No, Google je samo jedna od mnogih internetskih tvrtki koje prate korisnike u svrhu stvaranja vrlo preciznih profila o svojim korisnicima koji im daju podlogu za personalizirano oglašavanje. S obzirom na invanzivnost ovih procesa koje izaziva ogorčenje korisnika, tvrtke koje primjenjuju personalizaciju postaju sve transparentnije u vezi svojih postupaka te su počele pružati aktivniju ulogu korisnicima u procesu personalizacije. Korisnici sada mogu odlučiti žele li uopće biti meta personaliziranih oglasa ili ih aktivno žele izbjeći (Strycharz et al., 2019:2). Pa tako korisnici Googlea mogu pregledati i prilagoditi predviđene interese, kao i potpuno isključiti personalizirane usluge, a tu opciju je preuzela i većina drugih pretraživača, što označava kontrolu obrade podataka koju korisnicima pružaju same oglašivačke platforme (ibid). Međutim, personalizacija oglasa je prema zadanim postavkama većine internetskih usluga uključena, stoga ju je potrebno manualno isključiti u postavkama pretraživača ili internetske stranice, ukoliko korisnik smatra personalizaciju nepoželjnom.

Također, postoji i „Do-Not-Track“ (dalje u tekstu: DNT) sigurnosna postavka. Naime, riječ je o jednostavnom i univerzalnom mehanizmu za isključivanje internetskog praćenja korisnika (Mayer i Narayanan, 2010:2). Kada korisnik odluči uključiti DNT postavku, dostupnu na svim pretraživačima, preglednik šalje poseban signal internetskim mjestima, analitičkim tvrtkama, oglašivačkim mrežama, dobavljačima priključaka i ostalim internetskim uslugama s kojima se korisnik susreće tijekom pregledavanja kako bi zaustavio praćenje njegove/njene aktivnosti (*What is Do Not Track and How Does it Work?*, 2021). DNT postavka je također prema zadanim postavkama isključena te zahtijeva od korisnika da fizički izmijeni postavke preglednika kako bi se postavka uključila.

Onemogućavanje oglasa putem *ad blocker* dodataka za preglednik također je jedan od načina suprotstavljanja problemima privatnosti na internetu i popularan način filtriranja internetskih zahtjeva koji ne poslužuju glavni sadržaj internetske stranice (Gervais et al., 2017:1). Naime, ti su dodaci dostupni na svim preglednicima, a svrha im je uklanjanje neželjenog oglašivačkog sadržaja, ali i sprječavanje curenja osjetljivih korisničkih podataka prema poslužiteljima trećih strana (Gervais et al., 2017:1).

Najpopularnija *ad blocking* rješenja su proširenja preglednika, poput *Ghostery* i *AdblockPlus* dodataka. Oni funkcioniraju na osnovi složenih konfiguracija filtriranja URL-ova koristeći jedan ili više popisa koji opisuju sadržaj koji treba dopustiti i koji blokirati („crne liste“) te ih redovito ažuriraju (Gervais et al., 2017:2). Slijedom toga, posjećeno internetsko mjesto ne prima oglašivački prihod od korisnika koji koristi *ad blocker*, niti njegove osobne podatke. Iz tog razloga neke platforme zabranjuju upotrebu dodataka za blokiranje oglasa. Kod tih stranica važno je pročitati politike privatnosti pri pristupu njima. Prema Richardu Tynanu (Streitz i Tynan, 2016:78), *ad blocker* dodaci automatizirani su način kojim korisnici drže kontrolu nad time s kim komuniciraju, ali i način minimiziranja količine podataka koje tvrtke prikupljaju na mrežnim uzorcima ponašanja korisnika.

Dakle, na internetu je prijetnja dugoročnog pohranjivanja i otkrivanja osobnih i privatnih podataka sveprisutna. Zbog toga je potrebno poduzeti čim više koraka navedenih u ovome poglavlju, pritom imajući na umu važnost poznavanja s kime se vodi interakcija na internetu, ne isticanja vlastitog profila, opreznog preuzimanja datoteka, prepoznavanja *junk* e-pošte i držanja anonimnosti gdje je to moguće, kako bi se izbjegle neželjene posljedice i očuvala privatnost na internetu.

3.2. Pravni okvir za zaštitu osobnih podataka na internetu

Zaštita osobnih podataka u Republici Hrvatskoj (dalje u tekstu: RH) omogućena je mnogim pravnim dokumentima. Najvažniji među njima su: Zakon o zaštiti osobnih podataka, Zakon o elektroničkim komunikacijama, Zakon o informacijskoj sigurnosti te Zakon o provedbi Opće uredbe o zaštiti osobnih podataka.

3.2.1. Zakon o zaštiti osobnih podataka

Zaštita osobnih podataka u Republici Hrvatskoj (dalje u tekstu: RH) omogućena je mnogim pravnim dokumentima. Prvi dokument u RH koji je regulirao zaštitu osobnih podataka je Zakon o zaštiti osobnih podataka. Zakon je to kojeg je 2003. godine donio Hrvatski sabor, a čiji se cilj navodi u njegovom prvom članku, a to je zaštita osobnih podataka pojedinaca i nadzora nad prikupljanjem, obradom i korištenjem osobnih podataka u RH (NN 103/2003). Ovaj je zakon prestao važiti 25. svibnja 2018. godine nakon što je na snagu stupila nova uredba o zaštiti osobnih podataka na razini Europske unije naziva Opća uredba o zaštiti osobnih podataka. No, on je važan zbog toga što je u članku 7. prvi puta obvezao voditelje obrade podataka da prikupljaju i obrađuju osobne podatke samo uz privolu ispitanika i za svrhu za koju je ispitanik pristao na obradu, u slučajevima određenim zakonom ili ako je ispitanik sam objavio te podatke. Također, članak 9. istoga zakona određuje da prije prikupljanja bilo kojih osobnih podataka, voditelj obrade podataka dužan je informirati ispitanika čiji se podaci prikupljaju o vlastitom identitetu, o svrsi obrade, o mogućim posljedicama uskraćivanja davaja podataka, o korisnicima ili kategorijama korisnika osobnih podataka te da li se radi o dobrovoljnom ili obveznom davanju podataka. Sljedeća važna stavka ovoga zakona nalazi se u članku 13. gdje se određuje da se osobni podataci smiju iznositi iz RH u svrhu daljnje obrade samo ako država ili međunarodna organizacija u koju se osobni podaci iznose ima odgovarajuće uređenu zaštitu osobnih podataka, odnosno ako ta druga država ili organizacija može osigurati zaštitu ispitanikovih podataka. Ono što je kasnije u Općoj uredbi o zaštiti osobnih podataka nazvano ispitanikovim pravom na ispravak osobnih podataka u Zakonu o zaštiti osobnih podataka definirano je u članku 20. koji obvezuje voditelje obrade podataka da dopune, izmijene ili obrišu osobne podatke ako su podaci nepotpuni, netočni ili neažurni. Također, važna promjena u kontekstu zaštite osobnih podataka uvedena ovim zakonom je navedena u članku 27., a to je osnivanje Agencije za zaštitu osobnih podataka koja nadzire provođenje zaštite osobnih podataka. Članak 32. navodi da ona ukazuje na uočene zloupotrebe

prikupljanja osobnih podataka, sastavlja listu država i međunarodnih organizacija koje imaju odgovarajuće uređenu zaštitu osobnih podataka, rješava povrede prava te vodi središnji registar. S obzirom na to da Zakon o zaštiti osobnih podataka više nije važeći, danas Agencija za zaštitu osobnih podataka djeluje u skladu s odredbama Opće uredbe o zaštiti osobnih podataka (NN 103/2003).

3.2.2. Zakon o elektoničkim komunikacijama

Zakon o elektroničkim komunikacijama donesen je 2008. godine, a njime se uređuju prava i obaveze pružatelja usluga elektoničkih komunikacija i korisnika tih usluga. Članak 1. ovog zakona navodi da on pruža zaštitu podataka i sigurnost elektroničkih komunikacija te obavljanje inspekcijskog i stručnog nadzora i kontrole u elektroničkim komunikacijama (NN 73/2008). Što se tiče zaštite osobnih podataka na elektroničkim komunikacijskim mrežama, u članku 5. navodi se da Hrvatska agencija za poštu i elektroničke komunikacije kao regulatorno tijelo koje se bavi provedbom odredbi ovoga zakona zadužena je za osiguravanje visoke razine zaštite osobnih podataka i privatnosti. Nadalje, članak 100. ovoga zakona propisuje da je korištenje elektroničkih komunikacijskih mreža za pohranu podataka ili za pristup podacima korisnika usluga dopušteno samo u slučaju kada je taj pretplatnik ili korisnik usluga dobio jasnu i potpunu obavijest u skladu s posebnim propisima o zaštiti osobnih podataka, i to osobito o svrhama obrade podataka. Istim člankom zabranjuje se slušanje, prisluškivanje, pohranjivanje te svaki oblik presretanja ili nadzora elektroničkih komunikacija, dok se člankom 43. operatori javnih komunikacijskih usluga obvezuju na pružanje zaštite od zlouporaba i prijevara te na upoznavanje korisnika usluga sa zaštitom podataka i privatnosti. No, u članku 109. navode se slučajevi kada se pružatelje usluga obvezuje na zadržavanje podataka o elektorničkim komunikacijama, npr. radi provedbe istrage ili zaštite nacionalne sigurnost. Posljednji članak ovoga zakona važan za zaštitu privatnosti i osobnih podataka korisnika je članak 110. koji operaterima zabranjuje zadržavanje podataka koji otkrivaju sadržaj komunikacije (NN 73/2008).

3.2.3.Zakon o informacijskoj sigurnosti

Zakon o informacijskoj sigurnosti donesen je 2007. godine, a u njegovom članku 1. definira se pojam informacijske sigurnosti, mjere i standardi informacijske sigurnosti, nadležna tijela

zadužena za provedbu i nadzor mjera i standarda informacijske sigurnosti itd. (NN 79/2007). Članak 2. ovoga zakona navodi da je informacijska sigurnost „stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda“. U članku 5. navodi se da mjere i standardi informacijske sigurnosti obuhvaćaju nadzor pristupa i postupanja s klasificiranim podacima, postupanje prilikom neovlaštenog otkrivanja i gubitka klasificiranih podataka, planiranje mjera prilikom izvanrednih situacija itd. Navode se i područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti u članku 8., a to su: sigurnosna provjera, fizička sigurnost, sigurnost podataka, sigurnost informacijskog sustava te sigurnost poslovne suradnje. (NN 79/2007).

U kontekstu teme ovoga rada, važan je članak 11. ovoga zakona koji omogućuje sigurnost podataka, pod čime se misli na opće zaštitne mjere za prevenciju, otkrivanje i otklanjanje štete od gubitka ili neovlaštenog otkrivanja klasificiranih i neklasificiranih podataka u informacijskim sustavima. Ovi se pojmovi primjenjuju na sve informacijske sustave, odnosno sve komunikacijske, računalne ili druge elektroničke sustav u kojima se podaci obrađuju, pohranjuju ili prenose, tako da budu dostupni i upotrebljivi za ovlaštene korisnike (NN 79/2007).

3.2.4. Zakon o provedbi Opće uredbe o zaštiti podataka

Zakonom o provedbi Opće uredbe o zaštiti podataka dostigla se nova razina zaštite osobnih podataka u skladu s tom regulativom i kontrola do nedavno neobuzdane obrade velikih količina podataka. Članak 1. navodi da osim u slučajevima obrade podataka svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, obrada osobnih podataka stavljena je pod nadzor pojedinaca na koje se ti podaci odnose (NN 42/2018). Ovim se zakonom u njegovom članku 4. definiraju nadležna tijela zadužena za osiguravanje primjene odredaba Opće uredbe o zaštiti podataka, pa je tako određena Agencija za zaštitu osobnih podataka kao središnje tijelo odgovorno za praćenje primjene uredbe. Također, člankom se 6. ovim se zakonom Agencija za zaštitu osobnih podataka ovlašćuje za pokretanje i sudjelovanje u kaznenim postupcima u slučajevima povrede odredaba uredbe, donošenje kriterija za određivanje visine naknade administrativnih troškova, za vođenje odgovarajućih postupaka protiv odgovornih osoba zbog povrede odredbi uredbe te za druge zadaće (NN 42/2018).

Osim toga, člankom 19. se uređuje obrada podataka u posebnim slučajevima. Naime, obrada je osobnih podataka djeteta u slučajevima kada se djetetu izravno nude usluge informacijskog društva, npr. mrežne igre, vijesti ili obrazovne internetske stranice i bilo koje internetske stranice koje nude drugu robu ili usluge korisnicima, zakonita ako dijete ima najmanje 16 godina. Također, člankom 20. zabranjuje se obrada genetskih podataka radi izračuna izgleda bolesti i drugih zdravstvenih aspekata. Članci 21. i 26. zabranjuju obradu biometrijskih podataka te se određuje da se obrada osobnih podataka putem videonadzora može provoditi samo u svrhu koja je nužna i opravdana za zaštitu osoba i imovine (NN 42/2018).

Dakle, Zakon o provedbi Opće uredbe o zaštiti podataka osigurava provedbu, primjenu i kontrolu pridržavanja odredbama koje donosi ta regulativa te donosi ograničenja i zabrane u posebnim slučajevima koje ona ne dotiče.

3.2.5. Ustav Republike Hrvatske

Ustav Republike Hrvatske je pravni dokument s najvećom pravnom snagom u Republici Hrvatskoj. Pitanje zaštite osobnih podataka u Ustavu Republike Hrvatske dotiče se u članku 37. Navedeni članak jamči sigurnost i tajnost osobnih podataka te osigurava da se osobni podaci pojedinaca ne smiju prikupljati, obrađivati i koristiti bez privole ispitanika, osim ako je riječ o uvjetima određenim zakonima (NN 41/2001). Isti članak Ustava navodi da je zabranjena uporaba osobnih podataka suprotna svrsi zbog koje su prikupljeni.

3.3. Opća uredba o zaštiti podataka

U kontekstu zaštite osobnih podataka na internetu, Opća uredba o zaštiti podataka (GDPR) zakonska je regulativa s najširim utjecajem na zaštitu privatnosti pojedinaca u digitalnom dobu, jer ona omogućuje građanima država koje su članice Europske unije povratak kontrole nad vlastitim osobnim podacima. Uredba je to koja je na snazi od 25. svibnja 2018., a čiji temelj čini pristup da je privatnost jedno od fundamentalnih ljudskih prava (Goddard, 2017:713). Kako bi zaštitili podatke i privatnost osoba, Europski je parlament, na prijedlog Europske komisije, ovom uredbom osigurao potpune informacije pojedincima te da sve organizacije preuzmu dokazivu odgovornost pri korištenju osobnih podataka (Goddard, 2017:713). Prema GDPR informeru (2021), cilj Europske komisije bio je korisnicima dati više nadzora nad

načinom na koji se njihovi podaci (zlo)upotrebljavaju, a to obvezuje organizacije da usvoje unutarnje mjere koje udovoljavaju načelima zaštite podataka (Tankard, 2016:6).

Jedan od osnovnih principa ove uredbe čini ideja da je obrada podataka poštena samo ako je transparentna, a to znači da mora postojati otvorenost organizacija prilikom obrade podataka koja se očituje kroz učinkovitu komunikaciju s pojedincima (Goddard, 2017:714). Opća uredba o zaštiti osobnih podataka obuhvaća organizacije koje proizlaze iz Europske unije, ali i one koje se nalaze izvan Unije, a koje rukuju podacima iz Europske unije (GDPRinformer, 2021). Opća uredba o zaštiti osobnih podataka ojačavanjem prava pojedinaca na privatnost štiti njihove osobne podatke, odnosno one podatke iz kojih se s velikom vjerojatnošću može otkriti identitet pojedinca, što znači da se uredba ne odnosi na anonimizirane podatke (GDPRinformer, 2021). Od kada je Opća uredba o zaštiti osobnih podataka na snazi, nositelji osobnih podataka moraju dati pristanak za obradu njihovih podataka, koji mora biti informiran i dobrovoljan, imaju maju pravo pristupa informacijama koje se odnose na njih te se mogu protiviti obradi njihovih podataka ako za to postoje legitimni razlozi (Tankard, 2016:5). Ove pogodnosti omogućene su sljedećim pravima u sklopu Opće uredbe o zaštiti podataka: pravo na zaborav, pravo na pristup osobnim podacima, pravo na ispravak osobnih podataka, pravo na ograničenje obrade osobnih podataka, pravo na prigovor i pravo na prenosivost podataka.

3.3.1 Pravo na zaborav

Iako je za ljudska bića svojstvena i u potpunosti prihvatljiva karakteristika zaboravljanja, bilo zbog prevelike količine informacija ili zbog ograničenog kognitivnog kapaciteta, isto se ne može očekivati i od računala za koje bi ta pojava bila smatrana *bugom* ili greškom sustava, stoga su računalne tehnologije dizajnirane da ne zaboravljaju i da djeluju kao produžetci naše memorije (Ghezzi et al., 2014:11 – 13).

Razvojem mreže kao arhivirajuće tehnologije i sve širim susatvnim korištenjem iste za raznovrsne aktivnosti, razvijen je sustav koji bezgranično „pamti“. Pod to „pamćenje“ spadaju i namjerno i nenamjerno ostavljene informacije na mreži koje tamo ostaju zapečaćene u obliku digitalnih podataka čak i ako ih korisnik pokuša odstraniti s mreže. Osjetljivi podaci na mreži, poput podataka o stečaju, o maloljetničkoj kaznenoj evidenciji ili o kreditnoj povijesti podrazumijeva da pojedinci do pojave GDPR regulative nisu imali pravo na institucionalni i socijalni zaborav (Ghezzi et al., 2014:11), što je problematično iz razloga što ti podaci

potencijalno mogu slijediti korisnika u svim sferama života i naštetiti njegovom prosperitetu dolaskom tih informacija u posjed potencijalnog poslodavca, šire javnosti ili osobe koja nam želi nauditi. No, kao što je spomenuto, to „pamćenje“ podrazumijeva i informacije koje korisnici svjesno ostavljaju na intrernetu. Zbog rasta popularnosti društvenih mreža gotovo je nemoguće zadržati osobne informacije u uskom krugu bliskih poznanika, pa tako „jednostavna pretraga imena pojedinca putem *Googlea* ili *Yahooa* često će otkriti gdje osoba živi, gdje je zaposlena, gdje su išli u školu, je li osoba u braku, tko je njihov supružnik i imaju li djecu“ (Cook, 2015:122-123). Zbog toga je ugrožena korisnikova privatnost na način da više nemamo izbora držati određene podatke privatnima, niti imamo slobodu da ne govorimo, pri čemu oduzeta nam sloboda da ne govorimo podrazumijeva pravo da se podaci ne otkrivaju bez pristanka ili na način koji je suprotan nečijem interesu (Cook, 2015:123).

Kako bi se privatnost i diseminacija osobnih podataka držala pod kontrolom korisnika, u sklopu GDPR regulative razvijeno je pravo na zaborav, odnosno pravo na brisanje. Ovo se pravo definira člankom 17. Opće uredbe o zaštiti podataka. Pravo na zaborav omogućuje pojedincima da zatraže od voditelja obrade podataka odstranjivanje podataka kada njihovo zadržavanje više nije bitno za ispunjenje svrhe radi koje su prikupljeni, a moguće ga je ostvariti pod sljedećim uvjetima:

> osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili na drugi način obrađeni; b) ispitanik povuče privolu na kojoj se obrada temelji i ako ne postoji druga pravna osnova za obradu; c) ispitanik uloži prigovor na obradu svojih osobnih podataka te voditelj obrade nema jače legitimne razloge za obradu.; d) osobni podaci nezakonito su obrađeni; e) osobni podaci moraju se brisati radi poštovanja pravne obveze iz prava Unije ili prava države članice kojem podliježe voditelj obrade; f) osobni podaci prikupljeni su u vezi s ponudom usluga informacijskog društva (Opća uredba o zaštiti podataka, 2016, čl. 17).

Ono što ovo pravo omogućuje nije brisanje i ponovno ispisivanje povijesti, odnosno potpuno uklanjanje neugodnih tragova iz povijesti koje je pojedinac ostavio za sobom krečući se kroz život, već osiguranje da nečija sadašnjost ne bude pretrpana njegovom/njenom prošlošću (Ghezzi et al., 2014:83). Pravo na zaborav smanjuje šansu za osudom, a omogućuje kretanje u budućnost bez osvrtanja na greške u prošlosti, jer iako ono ne omogućuje brisanje podataka u pravom smislu te riječi, omogućuje prestanak povrata podataka iz prošlosti (Ghezzi et al., 2014:83). Ostvarivanjem ovoga prava osobni podaci za koje smo iskoristili pravo na zaborav uklanjaju se iz rezultata pretraživanja na svim pretraživačima i postaju nedostupni slučajnim namjernicima (*Pravo na zaborav: što sve obuhvaća?*, 2018). Shodno tome, ovo pravo podrazumijeva pravo na pokajanje i promjenu mišljenja u vezi s prethodno otkrivenim

podacima ili za koje je dana suglasnost za obradu, već spomenuto pravo da prošlost ne utječe na sadašnjost i budućnost, pravo na brisanje podataka koje više nije legitimno čuvati te pravo odbijanja dekontekstualizacije podataka (koja se često događa preuzimanjem podataka s internetskih tražilica) (Ghezzi et al., 2014:97). Pravo na zaborav smatra se elementom informacijskog samoodređenja, odnosno prava pojedinca da odredi koji će podaci o njemu biti otkriveni, kome i u koju svrhu (de Terwangne, 2012; Rouvroy & Poullet, 2009; Hornung & Schnabel, 2009; Leonard & Poullet, 1992; Schwartz, 1989, prema Ghezzi et al., 2014:86). Ovim se pravom, dakle, ostvaruje „povrat" osobnih podataka, bilo da je riječ o fotografiji koju bismo htjeli zaboraviti, informaciji o pojedinčevoj problematičnoj prošlosti ili neki drugi osobni podatak koji ispitanik želi zadržati za sebe, iz bezdana interneta i stavljanje istih pod kontrolu pojedinca na kojeg se ti podaci odnose.

3.3.2. Pravo na pristup osobnim podacima

Pravo na pristup osobnim podacima definira se prema članku 15. Opće uredbe o zaštiti podataka kao pravo koje omogućuje ispitaniku mogućnost da dobije od voditelja obrade „potvrdu obrađuju li se osobni podaci koji se odnose na njega te ako se takvi osobni podaci obrađuju, pristup osobnim podacima" (Opća uredba o zaštiti podataka, 2016, čl. 15). Osim toga, ovo pravo ispitaniku omogućuje da dobije informacije o svrsi obrade, kategorijama osobnih podataka o kojima je riječ, primateljima ili kategorijama primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, predviđenom razdoblju u kojem će osobni podaci biti pohranjeni, ali i sve ostale podatke koje je voditelj obrade prikupio (ibid). Također, ovo pravo omogućuje ispitaniku da ukoliko se osobni podaci prenose u treću zemlju (ili međunarodnu organizaciju), osoba na koju se podaci odnose mora biti obaviještena o svim odgovarajućim zaštitnim mjerama koje se mogu poduzeti kako bi zaštitio podatke (ibid). Navedeni podaci ispitaniku se moraju dostaviti bez naknade, no postoje slučajevi kada se ispitaniku može uskratiti pristup tim podacima, npr. u slučaju da su zahtjevi prečesti ili očito zlonamjerni (GDPR informer, 2018).

3.3.3. Pravo na ispravak osobnih podataka

Jedan od osnovnih ciljeva GDPR-a je osigurati točnost osobnih podataka koje prikupljaju i obrađuju organizacije, stoga je sljedeće pravo koje omogućuje Opća uredba o zaštiti podataka pravo na ispravak osobnih podataka. Ono se definira člankom 16. Opće uredbe o zaštiti

podataka (2016), a omogućuje pojedincu da bez nepotrebnog odgađanja ishodi od voditelja obrade ispravak netočnih osobnih podataka koji se na njega odnose ili dopunu osobnih podataka ako podaci nisu točni, potpuni i ažurni. Ovo je pravo važno iz razloga što netočni podaci koje voditelj obrade posjeduje mogu negativno utjecati na život pojedinca. Agencija za zaštitu osobnih podataka (2021) na svojoj web stranici navodi sljedeći primjer kako netočni podaci mogu negativno utjecati na pojedinca: „ugovarate policu životnog osiguranja i doznajete da osiguravajuća kuća raspolaže s netočnim podatkom da ste srčani bolesnik, što povećava iznos premije životnog osiguranja. Imate pravo tražiti osiguravajuću kuću ispravak tog netočnog podatka“. No, negativan učinak netočnih podataka može se primijeniti i na internetu, gdje potencijalni budući poslodavac putem netočnih informacija koje je dobio o pojedincu pretraživanjem na internetu može donijeti neutemeljenu odluku o zaposlenju pojedinca.

Dakle, važno je biti svjestan ovoga prava i onoga što omogućuje prilikom donošenja značajnih odluka kako bi ishod situacije bio pod kontrolom osobe na koju se osobni podaci odnose.

3.3.4. Pravo na ograničenje obrade osobnih podataka

Pravo na ograničavanje obrade osobnih podataka se definira 18. člankom Opće uredbe o zaštiti osobnih podataka (2016), a odnosi se na ispitanikovu mogućnost da zatraži od voditelja obrade ograničenje obrade ako ispitanik osporava točnost osobnih podataka koje voditelj posjeduje, ako je obrada nezakonita, ako se ispitanik protivi brisanju osobnih podataka te umjesto toga traži ograničenje njihove uporabe. Osim u ovim slučajevima, ispitanik može zatražiti ograničenje obrade podataka ako se podaci moraju čuvati radi ostvarivanja ili obrane ispitanikovih pravnih zahtjeva, a voditelj obrade više ne treba podatke za potrebe obrade. Ograničenje obrade u ovom kontekstu znači da će podaci biti obrađivani samo uz pristanak nositelja podataka ili radi uspostavljanja, izvršavanja ili obrane pravnih zahtjeva, radi zaštite prava druge fizičke ili pravne osobe ili iz razloga važnog javnog interesa (Opća uredba o zaštiti osobnih podataka, čl. 18., 2016). Pod pojmom obrade u ovom se kontekstu) misli na širok spektar operacija koji uključuje prikupljanje, strukturiranje, širenje i brisanje podataka (*The Right to Restrict Processing,* 2021). Pravo na ograničenje obrade osobnih podataka često se navodi kao alternativa traženju brisanja osobnih podataka, jer ono umjesto uklanjanja osobnih

podataka ograničava načine na koje organizacije mogu koristiti osobne podatke. No, uglavnom je zatraženo ograničenje samo privremeno (*The Right to Restrict Processing*, 2021).

3.3.5. Pravo na prigovor

Pravo na prigovor definira se člankom 21. Opće uredbe o zaštiti podataka. Ono omogućuje ispitaniku da u bilo kojem trenutku uloži prigovor na obradu podataka koji se odnose na njega. Ukoliko je prigovor valjan te voditelj obrade ne dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze interese, prava i slobode ispitanika, obrada osobnih podataka se obustavlja (Opća uredba o zaštiti podataka, čl. 21., 2016). Iz istog članka proizlazi da će se prigovor uvažiti te će obrada podataka biti obustavljena ako se osobni podaci obrađuju za potrebe izravnog marketinga, a ispitanik se protivi takvoj obradi. Također, moguće je uložiti prigovor kada organizacija koristi osobne podatke ispitanika za zadaću koja se provodi u javnom interesu, za vršenje službene ovlasti, za njihove legitimne interese te za za znanstvena ili povijesna istraživanja ili u statističke svrhe (*The right to object to the use of your data*, 2021). U slučaju izravnog marketinga, nema izuzeća ili osnova za odbijanjem prigovora, no to ne znači da je organizacija prisiljena izbrisati podatke o ispitaniku, već da je prisiljena osigurati da ispitanik više ne bude primatelj izravnog marketinga (*Right to object*, 2021). Također, uspješno ostvarivanje prava na prigovor zahtijeva motivaciju za prigovor.

3.3.6. Pravo na prenosivost podataka

Pravo na prenosivost podataka definira se člankom 20. Opće uredbe o zaštiti osobnih podataka (2016) kao ispitanikovo pravo na primanje osobnih podataka koji se odnose na njega, a koje je pružio voditelju obrade u strukturiranom, uobičajenom i strojno čitljivom formatu te mogućnost prijenosa tih podataka drugom voditelju obrade bez ometanje voditelja obrade kojem su dani osobni podaci. Prijenos će biti moguć ako se obrada podataka provodi automatiziranim putem i temelji se na privoli ili ugovoru, npr. pri promjeni teleoperatera moguće je zatražiti od teleoperatera čije usluge pojedinac više ne koristi vlastite osobne podatke u digitalnom obliku i prijenos istih drugom operateru (Agencija za zaštitu osobnih podataka, 2021).

Također, važna je primjenjivost ovog prava na internetu pri promjeni s jednog pružatelja usluge na drugi, jer ono omogućuje pojedincu da po svojoj želji odaberu one usluge

koje im se sviđaju bez previše napora. Primjerice, ako se pojedinac želi prebaciti s jednog pružatelja usluge e-pošte (npr. Googleov *Gmail*) na drugi (npr. Microsoftov *Outlook*), ovo pravo omogućuje mu uštedu vremena i sigurnost time što omogućuje prijenos svih osobnih podataka s jedne usluge na drugu (GDPRinformer, 2018). Kako bi se pravo ostvarilo, podnositelj zahtjeva mora poslati tvrtki koja posjeduje i obrađuje podatke pismeni zahtjev za prijenosom, nakon čega tvrtka ima rok od mjesec dana da besplatno izvrši prijenos podataka drugoj tvrtki koju podnositelj zahtjeva odabere (GDPRinformer, 2018).

3.4. Medijska, informacijska i digitalna pismenost studenata

Mediji kao glavni kanali informiranja, komuniciranja, obrazovanja i zabave zauzimaju sve veću ulogu u životima. Potencijalno negativni utjecaji medija mogu se izbjeći razumijevanjem medija, a za to je potrebno biti medijski pismen. Postoji mnogo definicija medijske pismenosti. Sajjad Malik (2008: 2) definira ju kao „informirano, kritičko razumijevanje prevladavajućih masovnih medija, i uključuje ispitivanje tehnika, tehnologija i institucija uključenih u medijsku proizvodnju; sposobnost kritičke analize medijskih poruka; i prepoznavanje uloge koju publika igra u proizvodnji značenja iz te poruke“. Važnost tih kompetencija ističu i Labaš i Marinčić (2018:11), a pri tome naglašavaju vrednovanje konzumiranih informacija kao važan aspekt medijske pismenosti, jer ono korisnicima omogućuje prosudbu i vrednovanje uloge medija u njihovim životima. Dakle, iz definicija medijske pismenosti proizlazi da biti medijski pismen ne znači samo imati tehničke kompetencije pristupa medijskim sadržajima i razumijevanje istih, već je važna i kritička evaluacija sadržaja i razumijevanja kako mediji svojim sadržajem utječu na nas.

Studentima razumijevanje medija koje medijska pismenost omogućuje, odnosno razumijevanje načina na koji mediji funkcioniraju i kako mediji utječu na njih, pomaže da postanu kritični i svjesni donositelji odluka i aktivni sudionici u društvu. Zbog toga što se osnaživanjem pristupa informacija potiče analitičnost i poboljšavaju komunikacijske vještine, medijska pismenost nije važna samo za studente koji svoju karijeru vide u medijskoj industriji, već za sve one koji aktivno koriste medije. Osim toga, medijska im pismenost pomaže i u stvaranju vlastitog medijskog sadržaja te u razvoju vještine izražavanja vlastitog mišljenja (Peran i Raguž, 2016:380).

U prošlosti se medijska pismenost prvenstveno odnosila na audiovizualne medije, a danas obuhvaća i nove medije. U današnjem medijskom ozračju u kojem svi sadržaji, pa tako

i sadržaji tradicionalnih medija, gravitiraju prema digitalnim tehnologijama i internetu, važno je razgraničiti pojmove informacijske i medijske pismenosti. Informacijska pismenost također je važan skup kompetencija za studente, a podrazumijeva sljedeće: 1) prepoznavanje vlastite informacijske potrebe; 2) lociranje i procjenu kvalitete informacija; 3) pohranjivanje i preuzimanje informacija; 4) učinkovito i etično korištenje informacija; 5) primjenu informacije za stvaranje i prenošenje znanja (Catts i Lau, 2008).

Dakle, informacijska i medijska pismenost pojmovi su koji se u mnogočemu preklapaju. Informacijska pismenost danas podrazumijeva potrebu da se dopre do svijeta medija (kako bi se pristupilo potrebnim informacijama) i da se više pažnje posveti kritičkim analitičkim vještinama medijske pismenosti, dok medijska pismenost u današnjem digialnom dobu podrazumijeva korištenje vještina informacijske pismenosti za pretraživanje, procjenu i organiziranje informacija (Lee i So, 2013:138). No, najveća razlika između ova dva koncepta je u informacijskim objektima na koje se usredotočuju. Dok se medijska pismenost usredotočuje na poruke masovnih medija, informacijska se pismenost usredotočuje na informacije općenito (Lee i So, 2013:139). Iz toga možemo zaključiti da se medijska pismenost javlja kao potkategorija informacijske pismenosti, jer svaka je medijska poruka ujedno i informacija koja nosi određeno značenje i niz podataka, neovisno o tome je li riječ o objektivno izvještenoj činjenici ili vijesti koja se klasificira kao *fake news*.

Za studente, ali i učenike srednjih, pa čak i osnovnih škola, informacijska je pismenost nužna, prvenstveno zato što „[z]a razliku od učenja u tradicionalnom okruženju koje je podrazumijevalo recepciju informacija iz vanjskih, analognih, statičnih i linearno organiziranih informacija, učenje u digitalnom okruženju mora biti stalan i aktivan proces konstrukcije znanja pomoću novih, fleksibilnih, nelinearnih, dinamičkih i interaktivnih izvora informacija“, navodi Sonja Špiranec (2008) (prema Jokić et al, 2014: 65). Važno je spomenuti i pojam informatičke pismenosti koji se često poistovjećuje s pojmom informacijske pismenosti, no ti se pojmovi odnose na različite skupove kompetencija. Informatička pismenost uključuje kompetencije koje se odnose se na sposobnost razumijevanja i korištenja računala, računalnih tehnologija i programa. Studenti kompetencije informatičke pismenosti moraju savladati iz razloga što je informatička pismenost preduvjet i jedan od sastavnih dijelova informacijske pismenosti. Kako bi netko bio informatički pismen mora imati znanja o sljedećim komponentama informatičke pismenosti: o tehnološkoj svijesti, tehničkom rječniku, komponentama računala, konceptima podataka i programa, korištenju računala, radu na

datotekama, dokumentima i slikama, radu s multimedijom, procjeni resursa i komunikaciji s drugima (Son et al., 2011:27).

Prema istraživanju Suzane Peran i Anđelke Raguž (2016:392), o medijskoj pismenosti koje je obuhvatilo studente komunikologije Fakulteta hrvatskih studija i Katoličkoga bogoslovnog fakulteta Sveučilišta u Zagrebu, studenti medije koriste redovito, najviše za informiranje, pa zatim zabavu i komunikaciju s obitelji i prijateljima te su uglavnom svjesni važnosti medijske pismenosti. No, isto istraživanje navodi da studenti nemaju povjerenja u medije. Iako je ovo istraživanje obuhvatilo samo studente kojima su mediji bliski budućem profesionalnom opredjeljenju, ono ukazuje na promjenu u razmišljanju o medijima i sve kritičniji odnos prema njima, što nagoviješta rast i razvoj medijske pismenosti u obrazovnom sustavu, a i njene važnosti u svijesti studenata. Istraživanje Ivana Beroša (2020:24) o razini medijske pismenosti studenata pedagogije pokazuje da većina studenata djeluje na srednjoj, a ne visokoj razini medijske pismenosti. Ispitanicima ovog istraživanja nedostaje znanja o zakonskim preduvjetima korištenja medija, a u istraživanju su pokazali i ograničenu sposobnost iskorištavanja mogućnosti medija.

Dakle, iz dosadašnjih istraživanja medijske pismenosti studenata možemo zaključiti da iako postoji određeno znanje i kritičan stav prema medijima, važno je medijsko obrazovanje još više uključiti u obrazovni sustav kako bi se potaknulo još aktivnije sudjelovanje studenata u javnom diskursu i produkciji medijskih sadržaja, jer se povećava i efikasnost demokratskog sustava pomoću njihove ojačane svijesti o političkoj participaciji, a to će im pomoći i u proširenju njihova znanja o zakonskoj pozadini djelovanja masovnih medija.

Što se informacijske pismenosti studenata tiče, analiza raznih istraživanja o informacijskoj pismenosti studenata koju su proveli Jadranka Lasić-Lazić, Sonja Špiranec i Mihaela Banek Zorica (2012:136 – 139) pokazuje da studenti iako pokazuju veliku sklonost prema korištenju interneta u obrazovne svrhe, a u rješavanje nekoga istraživačkog problema i zadatka kreću od Googlea, radi se o „površnim interakcijama koje su usmjerene na kvantitetu podataka umjesto na njihovo kvalitetno tumačenje i kritičko razmatranje koji su pretpostavka za dubinsko, smisleno i istinsko učenje“. Točnije, studenti koriste internetsko pretraživanje za skupljanje čim većih količina podataka bez kritičkog promišljanja o njima (Lasić-Lazić et al., 2012:136). Osim toga, dostupnost svih informacija na internetu dopušta im brzo mijenjanje posjećenih internetskih stranica, nigdje se ne zadržavaju dugo i ne ulaze dublje u sam sadržaj stranica, a s time je povezana i sklonost preslikavanju/prepisivanju sadržaja s interneta bez

promišljanja (ibid). Dakle, većinu kompetencija koje informacijska pismenost obuhvaća studenti su savladali, poput shvaćanja vlastite informacijske potrebe, pristupa i preuzimanja informacija te korištenja informacija radi proširenja znanja, no studenti podbacuju u procjeni kvalitete informacija, etičnom preuzimanju i kritičkom promišljanju, a to su važne sastavnice informacijske pismenosti. Stoga se može zaključiti da se, kao što je slučaj i s medijskom pismenošću, radi o srednjoj razini informacijske pismenosti.

Međutim, u kontekstu zaštite osobnih podataka na internetu, skup kompetencija koji osigurava najsigurnije korištenje interneta spada pod digitalnu pismenost. Digitalna pismenost dio je medijske pismenosti, a posebno se odnosi na medije na internetu, pametne telefone, videoigre i druge netradicionalne izvore informiranja (*What is Digital Literacy*, 2021). Preciznije, digitalna pismenost podrazumijeva „sposobnost sigurnog i primjerenog pristupa, upravljanja, razumijevanja, integriranja, komuniciranja, procjene i stvaranja informacija putem digitalnih tehnologija [...]“ (Law, Woo i Wong, 2018:6). Neke vještine koje su ključne kako bi se pojedinac mogao smatrati digitalno pismenim su: rad sa softverskim alatima za obradu teksta, tablica i fotografija, korištenje elektroničke pošte i internetskih pretraživača, internetskih preglednika, aplikacija pomoću kojih se stvaraju prezentacije i pristup komunikacijskim kanalima na internetu kao i druge vještine pomoću kojih pristupamo digitalnom sadržaju ili stvaramo vlastiti (*Što je digitalna pismenost?*, 2021). Osim toga, pod digitalnu pismenost spadaju i kompetencije zaštite vlastitog zdravlja, računala i vlastitih osobnih podataka prilikom korištenja interneta, kao i razumijevanje i kritička evaluacija konzumiranog digitalnog sadržaja. Dakle, digitalno pismena osoba osim dobrog snalaženja u digitalnim prostorima zna poduzeti sigurnosne i zaštitne mjere na internetu, a upravo je taj sigurnosni aspekt digitalne pismenosti tema našeg istraživanja za diplopmski rad.

4. ISTRAŽIVANJE STAVOVA, ZNANJA I ZABRINUTOSTI STUDENATA O ZAŠTITI OSOBNIH PODATAKA NA INTERNETU

Kao što je predstavljeno u prethodnim poglavljima rada, zaštita osobnih podataka u današnjem svijetu u kojem dominiraju digitalne tehnologije važan je aspekt digitalne i medijske pismenosti i ključan preduvjet privatnosti. U ovome dijelu diplomskoga rada dajemo pregled istraživanja kojim smo ispitali stavove, znanja i zabrinutosti studenata Sveučilišta u Zagrebu o zaštiti osobnih podataka na internetu.

4.1. Ciljevi i hipoteze istraživanja

U poglavlju *1.2. Ciljevi i metoda istraživanja* predstavili smo glavni cilj istraživanja, a to je utvrditi postoje li razlike u poznavanju internetskih politika privatnosti i načina prikupljanja podataka te razlike u zabrinutosti oko ugroženosti osobnih podataka na internetu među sudionicima s obzirom na fakultet koji pohađaju. Također, odredili smo tri sporedna cilja istraživanja. Prvi sporedni cilj je istražiti razlikuje li se znanje i zabrinutost studenata o zaštiti osobnih podataka na internetu s obzirom na akademski uspjeh. Zatim, želimo istražiti na koje se sve načine studenti nastoje zaštiti kako bi zaštitili svoje osobne podatke na internetu. Posljednji sporedni cilj nam je istražiti postoji li povezanost između duljine dnevnog korištenja interneta i manje razine zabrinutosti u vezi zaštite osobnih podataka na internetu. Ovim istraživanjem želimo napraviti doprinos razumijevanju i razvoju pismenosti internetske sigurnosti među studentima Sveučilišta u Zagrebu te doći do zaključka koje kategorije studenata trebaju poraditi na znanju po pitanju zaštite osobnih podataka na internetu kako bi znali držati svoju privatnost pod vlastitom kontrolom.

Kako bismo ostvarili ciljeve istraživanja, iz glavnog i triju sporednih ciljeva, izvučene su četiri hipoteze za istraživanje. Prva je hipoteza glavna, dok su preostale tri sporedne.

H1: Studenti Fakulteta elektrotehnike i računarstva, Pravnog fakulteta, Filozofskog fakulteta te Fakulteta organizacije i informatike imaju više znanja o politikama privatnosti i načinima zaštite osobnih podataka te su više zabrinuti zbog ugroženosti osobnih podataka na internetu od studenata ostalih fakulteta Sveučilišta u Zagrebu. Također, više znanja imaju te više zabrinutosti pokazuju studenti na diplomskoj razini studija u odnosu na studente na preddiplomskoj razini studija.

H2: Studenti s boljim akademskih uspjehom, odnosno većom prosječnom ocjenom, imaju više znanja o politikama privatnosti i načinima zaštite osobnih podataka te su više zabrinuti oko ugroženosti osobnih podataka na internetu.

H3: Većina studenata se na internetu nastoji zaštititi tako da; koristi VPN mreže kako bi zaštitili svoje podatke na internetu, proučavaju uvjete privatnosti internetskih stranica i ne odgovaraju na neželjenu elektroničku poštu.

H4: Studenti koji koriste internet dulje tijekom dana, u odnosu na one koje koriste kraće, su manje zabrinuti u vezi zaštite osobnih podataka na internetu.

4.2. Metoda istraživanja

Već spomenuta metoda mrežnog anketnog upitnika korištena je u ovome istraživanju. Kao razloge korištenja ove metode naveli smo sigurnu distribuciju i ispunjavanje upitnika u vremenu pandemije bolesti COVID – 19, mogućnost potpune anonimnosti sudionika te pogodnost riješavanja ankete u bilo kojem trenutku putem mobilnog telefona, računala ili tableta.

Mrežna anketa je istraživanje u kojem se podaci prikupljaju bez prisutnosti anketara, ali i bez kontrole statističara nad vjerojatnostima izbora sudionika, a provodi se putem interneta (Dumičić i Žmuk, 2009). Također, mrežne ankete pružaju mogućnost automatske provjere i pohrane odgovora pomoću tehnologije baze podataka i korisničkog sučelja HTML (Harlow, 2010: 97). Još neke prednosti mrežne ankete su brzina rješavanja, fleksibilnost, intreaktivnost, besplatna izrada i distribucija te činjenica da mrežne ankete ne zahtijevaju prisustvo anketara zbog čega se izbjegava učinak anketara, odnosno tendencija sudionika da daju odgovore za koje pretpostavljaju da ispitivač očekuje (Duffy et al., 2005:2). U korist istraživačima ide i činjenica da su u novije vrijeme mrežne ankete postale jednostavnije za upotrebu te se sada mogu smatrati učinkovitom i preciznom metodom prikupljanja podataka (Harlow, 2010:104). Preciznot prikupljanja podataka rezultat je mogućnosti prijenosa odgovora izravno u bazu podataka, čime se uklanjaju pogreške u transkripciji (Harlow, 2010:98). Dumičić i Žmuk (2009:124) navode da su mrežne ankete orijentirane prema sudionicima time što većina većina pitanja ima već ponuđene odgovore pa sudionik mora samo jednim klikom miša (ili dodirom ekrana na pametnom telefonu ili tabletu) odabrati svoj odgovor.

Međutim, odabir metode mrežne ankete nosi sa sobom i mnoge izazove. Zbog anonimnosti koju naša anketeta pruža, neizbježan je problem neiskrenosti i brzopletosti sudionika koji se žele na brzinu riješiti ankete, a taj problem otežava i činjenica da se iskrenost sudionika ovakvim neizravnim kontaktom vrlo teško može provjeriti (Dumičić i Žmuk, 2009:128). Taj smo problem pokušali riješiti pitanjima koja nisu dvosmislena i koja ne dozvoljavaju sudioniku pružanje kontradiktornih odgovora te strukturom pitanja koja dozvoljava brzo odgovaranje i rješavanje ankete. U obzir uzimamo činjenicu da nemaju svi studenti jednak pristup internetu, ali i činjenicu da zbog toga što je rješavanje ankete dobrovoljno, ispitanici nemaju obavezu rješavanja te mogu odbiti rješavanje ankete. Također, iako odsutnost anketara nosi prednosti, nosi i nedostatke. Odsutnost anketara onemogućava izravnu i trenutačnu komunikaciju sa sudionicima, a to znači da u slučaju da ispitaniku neko pitanje nije u potpunosti jasno, ne postoji mogućnost da sudionik pita anketara za pojašnjenje. Zbog toga postoji mogućnost nasumičnog odgovaranja na pitanja koja sudionik ne shvaća u potpunosti.

4.3. Uzorak i uzorkovanje

Uzorak istraživanja čini 200 studenata preddiplomskih i diplomskih studija Sveučilišta u Zagrebu. Radi se o neprobabilističkom uzorku koji se sastoji od 20 studenata po svakoj od deset najvećih sastavnica Sveučilišta u Zagrebu po broju studenata. Najbrojnije sastavnice Sveučilišta u Zagrebu su sljedeći fakulteti: Ekonomski fakultet, Pravni fakultet, Filozofski fakultet, Prirodoslovno-matematički fakultet, Fakultet elektrotehnike i računarstva, Medicinski fakultet, Učiteljski fakultet, Kineziološki fakultet, Fakultet organizacije i informatike i Fakultet strojarstva i brodogradnje. Navedeni uzorak odabran je zbog heterogenosti studijskih programa koju dobivamo odabirom deset najvećih fakulteta Sveučilišta u Zagrebu po broju studenata. Naime, ovakvim uzorkom dobili smo studente s raznolikih područja znanosti, uključujući prirodne znanosti, tehničke znanosti, biomedicinu i zdravstvo, biotehničke znanosti, društvene te humanističke znanosti.

Za uzorkovanje smo koristili metodu snježne grude (engl. *snowball sampling*). Uzorkovanje putem metode snježne grude počinje utvrđivanjem određenog broja članova ciljane populacije koji zadovoljavaju postavljene kriterije za ulazak u uzorak. Nakon njihovog ulaska u uzorak, preko njih se dolazi do ostalih članova tako da oni istraživanje upućuju na svoje poznanike i prijatelje koji zadovoljavaju postavljene kriterije (Baćak, 2006:195). Dakle,

lociranje i komunikacija s jednim studentom fakulteta koji spada pod deset najvećih fakulteta Sveučilišta u Zagrebu, olakšava nam pristup drugim studentima tog istog fakulteta i pomaže nam da dođemo do broja od 20 studenata po odabranim fakultetima na način da taj student, koji postaje izvorištem istraživanja, proslijeđuje istraživanje drugim studentima tog fakulteta. Još jedan razlog korištenja metode snježne grude za uzorkovanje je to što takav način pogoduje metodi mrežnog anketnog upitnika koji ne zahtijeva interakciju licem u lice sa sudionicima, već može biti poslan putem interneta, a to je ključno zbog toga što je istraživanje provedeno za vrijeme već spomenute pandemije.

Za naš uzorak prvo su odabrani pojedini studenti koji studiraju na navedenim fakultetima. Njima je poslan anketni upitnik putem *Facebook Messenger* aplikacije. Nakon što su rješili upitnik, oni su putem iste aplikacije proslijeđivali anketni upitnik svojim fakultetskim kolegama koji su zatim ispunjavali isti upitnik te ga proslijedili na isti način svojim fakultetskim prijateljima. Uzorak smo kontrolirali tako da smo od poznanika kojima je prvotno poslan upitnik tražili da nas obavijeste o broju prijatelja kojima su poslali upitnik i o vremenu kada su poslali upitnik kako bismo na vrijeme onemogućili prihvaćanje odgovora dolaskom do brojke od 20 studenata po fakultetu. Time smo dobili uzorak snježne grude, a važna karakteristika ovog uzorka je to što odabir svakog novog sudionika nije slučajan, nego je određen karakteristikama i preferencijama sudionika koji provodi upućivanje na sljedeće sudionike (Baćak, 2006:195).

Međutim, nije u svim dijelovima istraživanja korišten uzorak od 200 studenata, već smo u dijelu u kojem prikazujemo rezultate s obzirom na razinu studija, ocjene i dnevnu učestalost korištenja interneta uzeli odgovore studenata koji su pokazali veće razumijevanje o temi istraživanja. Dakle, kako ne bismo ponovno uspoređivali odgovore svih sudionika i kako bismo stvorili ispravnu sliku i usporedbu znanja među različitim kategorijama sudionika, a ne miješali neznanja i znanja, uzeli smo odgovore polovice sudionika s onih fakulteta koji su prethodnom usporedbom pokazali veće znanje o internetskim politikama privatnosti i zaštiti osobnih podataka na internetu i time izveli zaključke o tome koje kategorije imaju veća znanja, a koja manja, a da su svejedno i isključivo znanja.

4.4. Instrument

Instrument istraživanja je mrežni anketni upitnik (Prilog 1.) koji se sastoji od 19 pitanja podijeljenih u pet skupina. Anketni upitnik, koji smo izradili putem *Google Forms* alata, namijenjen je studentima Sveučilišta u Zagrebu. Upitnik je pismenog i otvorenog tipa, što znači da anketi može pristupiti bilo tko s pristupom internetu i poveznici koja proslijeđuje na upitnik. Kako bismo sudionicima olakšali rješavanje ankete, a samim time dobili i veću stopu odgovora, pitanja naše ankete sastavljena su tako da se od sudionika traži odabir unaprijed ponuđenih odgovora na pitanja ili vrlo kratko nadopunjavanje odgovora. Prvom skupinom pitanja, koja se sastoji od šest pitanja, željeli smo ispitati demografske karakteristike studenata. Ispitali smo njihovu dob, spol, fakultet koji pohađaju, njihovu trenutnu razinu studija i prosječnu ocjenu tijekom studija te njihovu procijenjenu učestalost korištenja interneta. Ove smo karakteristike ispitali kako bismo istražili povezanost između određenih demografskih karakteristika studenata i znanja i zabrinutosti povezanih s ugroženosti osobnih podataka na internetu. Dobne skupine u pitanju o dobi sudionika preuzete su iz istraživanja Enis Horvat i Krešimira Šolića (2020) naziva *Ispitivanje znanja i ponašanja studenata o pitanjima zaštite privatnosti na internetu metodom socijalnog inženjeringa*, dok smo prosječno svakodnevno korištenje intreneta sudionika ispitali skalom preuzetom iz studije *Problematic Internet Use of Adolescents: Role of Daily Hassles and Social Isolation* (Zorbaz et al., 2020).

Sljedećom skupinom pitanja postavljenih u obliku četiri tvrdnje željeli smo utvrditi sudionikovu procjenu poznavanja prirode internetskih politika privatnosti i načina funkcioniranja internetskih tvrtki te zna li načine kako osigurati svoje podatke. Za kreiranje tvrdnji iz ove skupine pitanja poslužilo nam je poglavlje *Results* iz *Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale*" (Trepte et al., 2015). Odgovorima na ove tvrdnje stvorili smo predodžbu o svijesti studenata o nesigurnosti podataka na internetu. Trećom smo skupinom pitanja ispitali koje metode sudionici koriste kako bi spriječili nekontroliranu diseminaciju svojih podataka i njihovu upoznatost s GDPR regulativom. Ova kategorija pitanja sastoji se od pitanja oblikovanih u obliku tvrdnji i pitanja s mogućim jednim ili više odgovora. Osmo pitanje oblikovano je u obliku tvrdnji u kojima sudionik na skali od pet stupnjeva mora označiti procijenjenu učestalost korištenja određenih metoda zaštite. Većina tvrdnji iz osmoga pitanja preuzeta je iz *Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data,* (Boerman,

Kruikemeier et al., 2018.), dok smo neke dodali kako bi obuhvatili većinu mogućih metoda zaštite osobnih podataka na internetu.

Pitanja od devetog do dvanaestog su pitanja s mogućim višestrukim odgovorima, a njima dodatno istražujemo motivaciju za korištenje metoda zaštite podataka i svijest o „tragovima“ koje ostavljaju svojom aktivnošću na internetu te njihovu upoznatost i korištenje prava koja im GDPR regulativa omogućuju. Ova skupina kombinira pitanja preuzetih iz *Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation. Procedia Computer Science* (Presthus et al., 2018), pitanja koja smo mi konstruirali te pitanja iz *Are We Really Informed on the Rights GDPR Guarantees?* (Sideri, Gritzalis, 2020).

Sljedeća skupina pitanja oblikovana je na način da sudionik odabire samo jedan odgovor. Ova skupina pitanja sastoji se od šest pitanja koja ispituju sudionikovo znanje o internetskim „kolačićima“ i korištenje dodatnih metoda zažtite podataka poput isključivanja personalizacije oglasa, neodgovaranja na neželjenu e-poštu i dr.. Iz istraživanja koju su proveli Presthus et al. (2018.) preuzeto je šesnaesto pitanje, dok je četrnaesto preuzeto iz *Protective Behavior Against Personalized Ads: Motivation to Turn Personalization Off* (Strycharz et al., 2019).

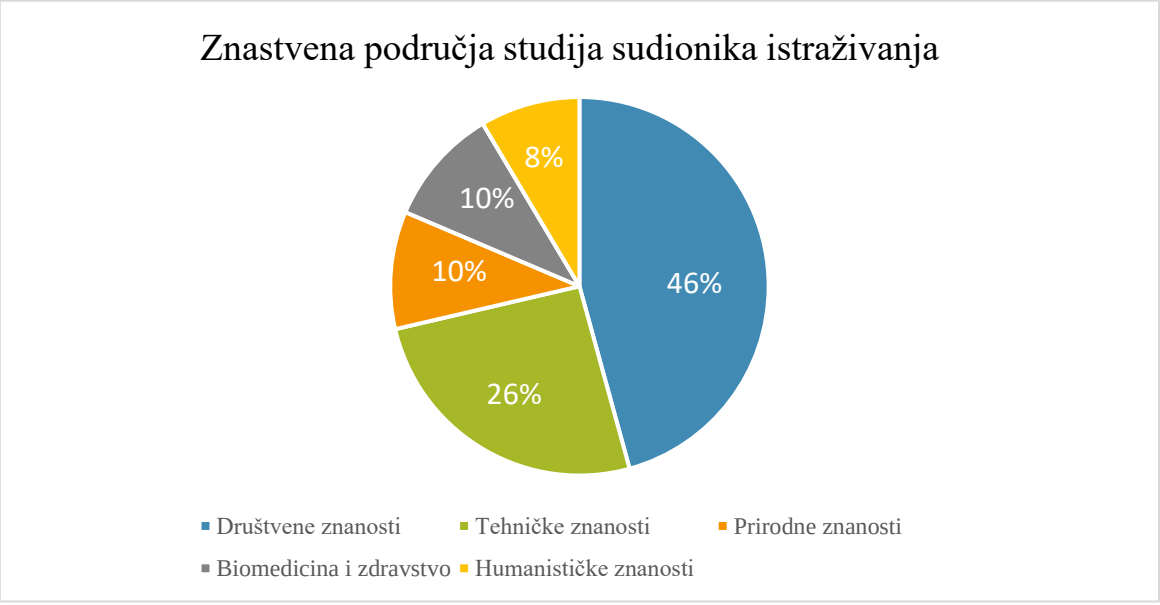
Posljednja skupina pitanja sastoji se od četrnaest tvrdnji. Sudionici u ovoj skupini pitanja na skali od pet stupnjeva označuju u kojoj se mjeri tvrdnja odnosi na njih. Ovom skupinom pitanja željeli smo saznati stupanj zabrinutosti studenata u vezi privatnosti i ugroženosti vlastitih podataka na internetu, stupanj povjerenja koji sudionici imaju u internetske tvrtke te generalno pozitivan ili negativan stav, odnosno beznađe spram nekontroliranog prikupljanja osobnih podataka od strane internetskih tvrtki. Tvrndje iz ovog pitanja preuzete su i prilagođene potrebama našeg istraživanja iz: *Investigating the Relationship Between Internet Privacy Concerns and Online Purchase Behavior* (Brown, 2004), *Internet users' information privacy concerns* (Malhotra et al., 2004), *Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data,* (Boerman et al., 2018), *Consumer Attitudes Toward Data Privacy Survey* (2018) i *Most consumers worry about online privacy but many are unsure how to protect it* (Whitney, 2020).

4.5. Rezultati istraživanja

U sljedećim ćemo poglavljima predstaviti odgovore sudionika istraživanja na sva pitanja iz mrežnog upitnika te usporediti ih s obzirom na fakultet koji sudionici pohađaju te s obzirom na njihovu trenutnu razinu studija, prosječnu ocjenu i dnevnu učestalost korištenja interneta. Prvo ćemo predstaviti socio-demografska obilježja sudionika u našem uzorku i njihove navike korištenja interneta, nakon čega ćemo uspoređivati odgovore sudionika na pitanja iz upitnika s obzirom na fakultet koji pohađaju, a zatim s obzirom na trenutnu razinu studija, dnevnu učestalost korištenja interneta i prosječnu ocjenu tijekom studija.

4.5.1. Socio-demografska obilježja studenata i navike korištenja interneta

U ovome dijelu rada prikazujemo rezultate istraživanja. U anketi je sudjelovalo 200 studenata. Preciznije, 20 studenata po svakoj od deset najvećih sastavnica Sveučilišta u Zagrebu po broju studenata, različitih godina i razina studija. Anketu je ispunilo 69 studenata i 131 studentica, pri čemu je prosječna dob sudionika u istraživanju 21,33 godina. U uzorku se nalaze studenti koji studiraju na studijima koje svrstavamo u pet različitih znanstvenih područja; društvene, prirodne, humanističke i tehničke znanosti te biomedicina i zdravstvo. Najviše sudionika (Grafikon 1.) pripada studiju društvenih znanosti, njih 45.5% (N=91), dok su humanističke znanosti znanstveno područje kojem pripada najmanji broj sudionika, njih 8,5% (N=17).



Grafikon 1. Znanstvena područja studija (Izvor: istraživanje autora) (N=200)

Kada je riječ o razini studija na kojoj se sudionici trenutno nalaze, rezultati pokazuju da se više sudionika trenutno nalazi na preddiplomskoj razini studija, njih 63,5% (N=127), dok se 36,5% sudionika (N=73) trenutno nalazi na diplomskoj razini studija. Zatim smo ispitali koju su ocjenu ispitanici najčešće dobivali na ispitima tijekom studija.

	FSB	FER	FOI	PMF	FFZG	EFZG	PFZG	MEF	UFZG	KIF	N
odličan (5)	1	3	0	1	1	2	1	5	5	3	**22**
vrlo dobar (4)	8	5	5	4	12	6	4	8	15	11	**78**
dobar (3)	10	12	13	15	7	11	14	7	0	6	**95**
dovoljan (2)	1	0	2	0	0	1	1	0	0	0	**5**
nedovoljan (1)	0	0	0	0	0	0	0	0	0	0	**0**
PROSJEK	3,45	3,55	3,15	3,30	3,70	3,45	3,25	3,90	4,25	3,85	**3,58**

Tablica 1. Najčešće ocjene tijekom studija (Izvor: istraživanje autora) (N=200)

Prosječna ocjena sudionika tijekom studija je 3,58. Rezultati (Tablica 1.) pokazuju kako studenti Učiteljskog fakulteta imaju najveći prosjek ocjena (4,25), a studenti Fakulteta organizacije i informatike najmanji (3,15).

	FSB	FER	FOI	PMF	FFZG	EFZG	PFZG	MEF	UFZG	KIF	N
manje od sat vremena dnevno	0	0	0	0	0	0	1	0	0	0	**1**
od 1 do 3 sata dnevno	4	1	1	2	1	0	2	1	0	4	**16**
od 3 do 5 sati dnevno	7	6	3	4	9	6	8	5	9	9	**66**
Od 5 do 7 sati dnevno	7	7	3	8	6	9	8	12	5	5	**70**
više od 7 sati dnevno	2	6	13	6	4	5	1	2	6	2	**47**

Tablica 2. Dnevna učestalost korištenja interneta sudionika (Izvor: istraživanje autora) (N=200)

Nadalje, kada je riječ o procijeni vlastitog korištenja interneta većina ga koristi od pet do sedam sati dnevno (N=70) (Tablica 2.). Više od od sedam sati dnevno na internetu provodi veći broj studenata s FOI-a (N=13). S druge strane, najmanje vremena na internetu provode studenti FSB-a, PFZG-a i KIF-a.

4.5.2. Znanja, stavovi i zabrinutost studenata s obzirom na fakultet

Sljedeći dio istraživanja prikazuje samoprocjenu studenata o poznavanju internetskih politika privatnosti i načina funkcioniranja internetskih tvrtki te načina zaštite vlastitih podataka.

Tvrdnja	***Akronim fakulteta***	***Nimalo se ne slažem***	***Ne slažem se***	***Niti se slažem ni ne slažem***	***Slažem se***	***Potpuno se slažem***
Razumijem što su internetske politike privatnosti i kako one utječu na privatnost mojih osobnih podataka.	**FSB**	1	0	6	7	6
	FER	0	2	4	12	2
	FOI	0	1	3	10	6
	PMF	0	5	5	7	3
	FFZG	1	1	6	8	4
	EFZG	1	0	9	9	1
	PFZG	0	2	6	5	7
	MEF	0	4	7	7	2
	UFZG	1	1	4	13	1
	KIF	0	6	7	2	5
	N	**4**	**22**	**57**	**80**	**37**
	%	**2%**	**11%**	**28.5%**	**40%**	**18.5%**
	Zbroj i postotak neslaganja/slaganja	**26 (13%)**		**57 (28.5%)**	**117 (58.5%)**	
Upoznat/a sam sa zakonima i pravnim aspektima zaštite osobnih podataka.	**FSB**	2	3	5	8	2
	FER	2	5	7	6	0
	FOI	0	4	4	8	4
	PMF	3	10	3	2	2
	FFZG	3	7	2	8	0
	EFZG	2	6	10	0	0
	PFZG	0	0	4	6	10

	MEF	2	9	6	3	0
	UFZG	5	5	4	5	1
	KIF	3	8	2	5	2
	N	**22**	**57**	**47**	**51**	**22**
	%	**11%**	**29%**	**23%**	**26%**	**11%**
	Zbroj i postotak neslaganja/slaganja	**79 (40%)**		**47 (23%)**	**73 (37%)**	

Tablica 3. Znanja o zaštiti osobnih podataka (Izvor: istraživanje autora) (N=200)

Tvrdnja	***Akronim fakulteta***	***Nimalo se ne slažem***	***Ne slažem se***	***Niti se slažem ni ne slažem***	***Slažem se***	***Potpuno se slažem***
Upućen/a sam u strategije koje vlasti i internetske tvrtke kao što su društveni mediji (npr. Facebook, Twitter), tražilice (npr. Google, Yahoo, Bing), pružatelji internetskog bankarstva itd. koriste za nadzor, prikupljanje, obradu i brisanje osobnih podatake.	**FSB**	0	4	8	1	7
	FER	0	4	5	7	4
	FOI	0	0	2	13	5
	PMF	3	5	4	5	3
	FFZG	5	2	5	4	4
	EFZG	1	6	5	6	1
	PFZG	0	3	3	8	6
	MEF	2	8	3	6	1
	UFZG	2	4	9	4	0
	KIF	1	7	4	5	3
	N	**14**	**43**	**41**	**66**	**34**
	%	**7%**	**22%**	**21%**	**33%**	**17%**
	Zbroj i postotak neslaganja/slaganja	**57 (29%)**		**41 (21%)**	**100 (50%)**	

Tablica 4. Znanja o zaštiti osobnih podataka (Izvor: istraživanje autora) (N=200)

Upoznat/a sam sa strategijama kontrole moje privatnosti na internetu kao što su redovito brisanje „kolačića“, korištenje firewall-a i sl.	**FSB**	1	1	4	8	6
	FER	0	1	3	11	5
	FOI	0	0	1	11	8
	PMF	1	6	2	5	6
	FFZG	1	4	7	5	3
	EFZG	1	7	3	7	2
	PFZG	0	2	3	8	7
	MEF	4	7	3	4	2
	UFZG	4	5	2	5	4
	KIF	2	7	6	4	1
	N	**14**	**40**	**34**	**68**	**44**
	%	**7%**	**20%**	**17%**	**34%**	**22%**
	Zbroj i postotak neslaganja/slaganja	**N=54 (27%)**		**34 (17%)**	**112 (56%)**	

Tablica 5. Znanja o zaštiti osobnih podataka (Izvor: istraživanje autora) (N=200)

Kada je riječ o prvoj tvrdnji (Tablica 3.), 58,5% sudionika (N=117) tvrdi kako se razumije u internetske politike privatnosti i njihov utjecaj na privatnost osobnih podataka, dok 13% sudionika (N=26) tvrdi kako se ne razumije. S tom se tvrdnjom najviše slažu sudionici s FOI-a (N=16) i FER-a te sudionici s UFZG-a (N=14), dok se najviše ne slažu s prvom tvrdnjom sudionici s KIF-a (N=6) i MEF-a (N=4). Kada je riječ o drugoj tvrdnji koja se odnosi na upoznatost sa zakonima i pravnim aspektima zaštite osobnih podataka, rezultati (Tablica 3.) pokazuju kako je 37% sudionika (N=73) upoznato s istima, dok njih 40% (N=79) nije upoznato. S tom se s tvrdnjom najviše slažu sudionici s PFZG-a (N=16) i FOI-a (N=12) te FSB-a (N=10) i FFZG-a (N=8), dok se najviše ne slažu oni s PMF-a (N=13), s MEF-a (N=12) i KIF-a (N=11). Nadalje, 50% (N=100) se slaže s tvrdnjom kako su upućeni u strategije koje vlasti i internetske tvrtke koriste za nadzor, prikupljanje, obradu i brisanje osobnih podatake (Tablica 4.). Najviše su slaganja s tom tvrdnjom, izrazili sudionici s FOI-a (N=18), slijede ih oni s PFZG-a (N=14), a u većini se s tom tvrdnjom slažu još i sudionici s FER-a (N=11), dok su najviše neslaganja s tom tvrdnjom izrazili sudionici s MEF-a (N=10) te s KIF-a i PMF-a (N=8). Nadalje, 56% (N=112) sudionika se slaže s tvrdnjom kako su upoznati sa strategijama kontrole vlastite privatnosti na internetu (Tablica 5.). Kod ove tvrdnje ponovno najveći broj slaganja vidimo kod sudionika s FOI-a (N=19), FER-a (N=16), PFZG-a (N=15) i FSB-a

(N=14), dok se u najvećoj mjeri s tom tvrdnjom ne slažu sudionici s MEF-a (N=11), KIF-a i UFZG-a (N=9) te sudionici s EFZG-a (N=8).

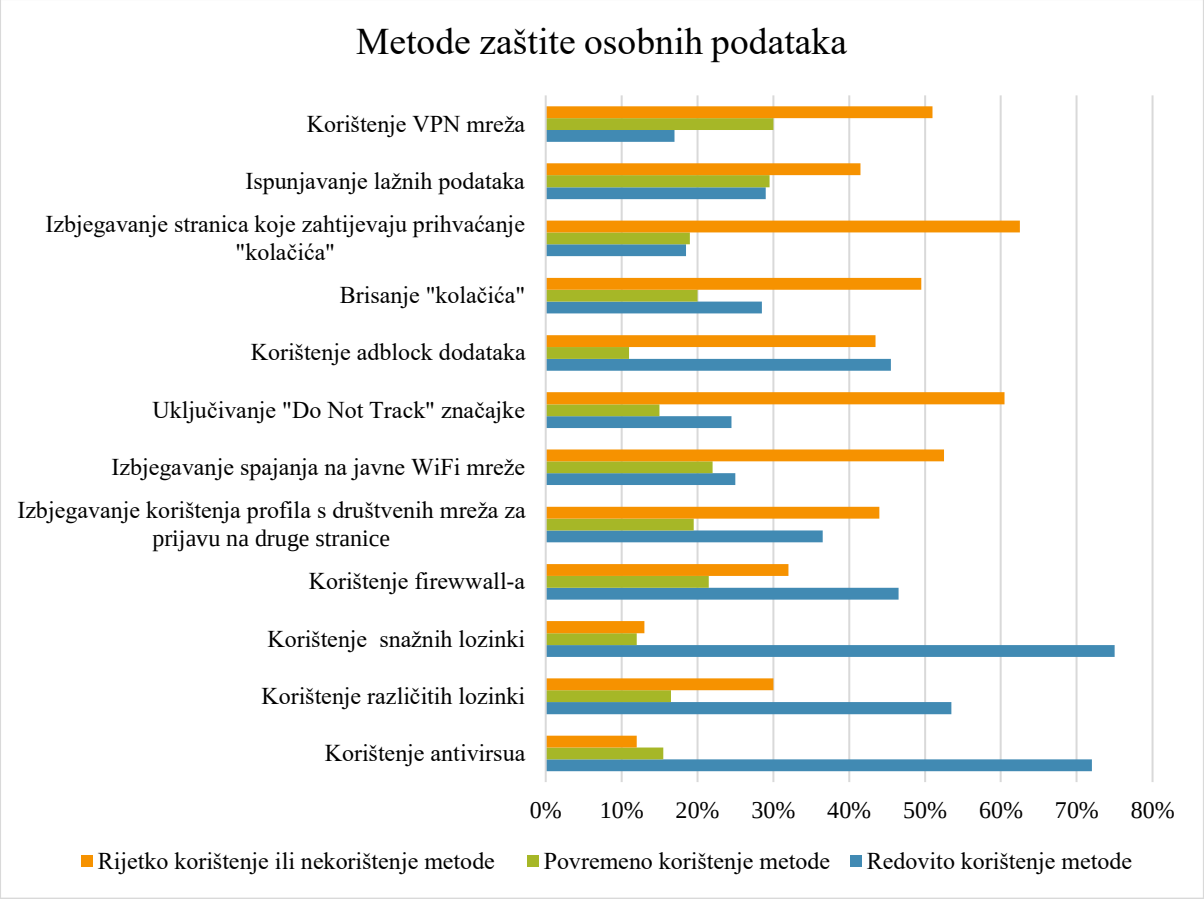
Iz odgovora na tvrdnje iz ovoga dijela upitnika izračunali smo prosječan postotak slaganja s tvrdnjama kako bi zaključili koji sudionici samoprocjenjuju najveće znanje po pitanju internetskih politika privatnosti i zaštite osobnih podataka.

	Razumijem što su internetske politike privatnosti i kako one utječu na privatnost mojih osobnih podataka.	Upoznat/a sam sa zakonima i pravnim aspektimazaštite osobnih podataka.	Upućen/a sam u strategije koje vlasti i internetske tvrtke kaošto su društveni mediji, pružatelji internetskog bankarstva itd. koristeza nadzor, prikupljanje, obradu ibrisanje osobnih podatake.	Upoznat/a sam sa strategijama kontrole moje privatnosti na internetu kao što suredovito brisanje „kolačića“, korištenje firewall-a i sl.	Prosječan postotak slaganja s tvrdnjama (%)
FOI	16 (80%)	12 (60%)	18 (90%)	19 (95%)	**81.25%**
FER	14 (70%)	6 (30%)	11 (55%)	16 (80%)	**58.75%**
FSB	13 (65%)	10 (50%)	8 (40%)	14 (70%)	**56.25%**
FFZG	12 (60%)	8 (40%)	8 (40%)	8 (40%)	**45.00%**
EFZG	10 (50%)	0	7 (35%)	9 (45%)	**32.5%**
PFZG	12 (60%)	16 (80%)	14 (70%)	15 (75%)	**71.25%**
UFZG	14 (70%)	6 (30%)	4 (20%)	9 (45%)	**41.25%**
PMF	10 (50%)	4 (20%)	8 (40%)	11 (55%)	**41.25%**
KIF	7 (35%)	7 (35%)	8 (40%)	5 (25%)	**33.75%**
MEF	9 (45%)	3 (15%)	7 (35%)	6 (30%)	**31.25%**

Tablica 6. Slaganja s tvrdnjama kojima sudionici procjenjuju svoja znanja po pitanjima internetskih politika privatnosti i zaštite osobnih podataka (Izvor: istraživanje autora) (N=200)

Rezultati (Tablica 6.) pokazuju da su većinom su kroz prosječno najveći postotak slaganja s tvrdnjama iz ove kategorije pitanja anketnog upitnika najveće znanje samoprocijenili sudionici s FOI-a (81.25%). Slijede ih sudionici s PFZG-a (71.25%), zatim sudionici s FER-a (58.75%), FSB-a (56.25%) i FFZG-a (45%).

Sljedećom smo skupinom pitanja ispitali koje metode zaštite osobnih podataka sudionici koriste kako bi očuvali svoju privatnost.



Grafikon 2. Učestalost korištenja metoda zaštite podataka (Izvor: istraživanje autora) (N=200)

Većina studenata, njih 75% (N=150) (Grafikon 2.) često ili vrlo često koristi sljedeće metode: korištenje snažnih lozinki, tj. lozinki koje kombiniraju velika i mala slova, znakove i brojeve. Nadalje, 72% sudionika (N=14) koristi antivirusnie aplikacije, 54% sudionika (N=107) koristi različite lozinke za različite račune na internetu te 47% sudionika (N=93) koristi *firewall*-a. Većina studenata 63% (N=125) rijetko ili nikada ne koristi metodu izbjegavanja stranica koje zahtijevaju obavezno prihvaćanje kolačića za pristup njima i to uključivanje „Do Not Track“ sigurnosne značajke preglednika – 61% sudionika (N=121), izbjegavanje spajanja na javne WiFi mreže – 53% sudionika (N=105) te korištenje VPN mreža – 51% sudionika (N=102).

Nadalje, usporedili smo učestalost primjene navedenih metoda među sudionicima s obzirom na fakultet koji pohađaju.

(1) – nikada, (2) – rijetko, (3) – ponekad, (4) – često, (5) – vrlo često

		(1)	*(2)*	*(3)*	*(4)*	*(5)*			*(1)*	*(2)*	*(3)*	*(4)*	*(5)*
Korištenje antivirusnih aplikacija	**FSB**	1	2	1	5	11	Korištenje različitih lozinki za različite račune na internetu	**FSB**	3	5	3	5	4
	FER	3	1	4	5	7		**FER**	5	1	2	7	5
	FOI	1	3	2	5	9		**FOI**	0	3	1	5	11
	PMF	2	2	5	4	7		**PMF**	1	5	3	5	6
	FFZG	1	2	0	10	7		**FFZG**	2	8	1	4	5
	EFZG	0	0	6	1	13		**EFZG**	3	4	5	0	8
	PFZG	1	0	2	8	9		**PFZG**	5	1	5	6	3
	MEF	0	1	3	6	10		**MEF**	1	2	4	3	10
	UFZG	1	0	4	6	9		**UFZG**	0	5	4	1	10
	KIF	2	1	4	9	3		**KIF**	0	6	5	5	4
	N	**12**	**12**	**31**	**59**	**85**		**N**	**20**	**40**	**33**	**41**	**66**
	%	**6%**	**6%**	**16%**	**30%**	**43%**		**%**	**10%**	**20%**	**17%**	**20%**	**33%**
	Zbroj i postotak neslaganja/slaganja	**24 (12%)**		**31(16%)**	**144 (72%)**			**Zbroj i postotak neslaganja/slaganja**	**60 (30%)**		**30(17%)**	**107 (53%)**	
Korištenje firewalla	**FSB**	3	2	2	7	6	Korištenje snažnih lozinki	**FSB**	0	2	4	4	10
	FER	1	1	5	5	8		**FER**	0	2	1	8	9
	FOI	3	1	5	4	7		**FOI**	0	1	3	4	12
	PMF	4	5	5	1	5		**PMF**	0	2	5	2	11
	FFZG	3	3	6	3	5		**FFZG**	0	3	1	6	10
	EFZG	2	7	2	3	6		**EFZG**	0	3	3	7	7
	PFZG	3	4	5	5	3		**PFZG**	1	4	2	6	7
	MEF	3	3	5	3	6		**MEF**	0	0	0	7	13
	UFZG	6	4	2	4	4		**UFZG**	0	5	1	3	11
	KIF	2	4	6	5	3		**KIF**	1	2	4	6	7
	N	**30**	**34**	**43**	**40**	**53**		**N**	**2**	**24**	**24**	**53**	**97**
	%	**15%**	**17%**	**43(22%)**	**20%**	**27%**		**%**	**1%**	**12%**	**12%**	**27%**	**49%**
	Zbroj i postotak neslaganja/slaganja	**64 (32%)**		**22%**	**93 (47%)**			**Zbroj i postotak neslaganja/slaganja**	**26 (13%)**		**12%**	**150 (75%)**	

Tablica 7. Korištenje pojedinih metoda zaštite podataka (Izvor: istraživanje autora) (N=200)

Kada je riječ o korištenju pojedinih metoda zaštite podataka, rezultati (Tablica 7.) pokazuju da sudionici s FFZG-a i PFZG-a (N=17) u najvećoj mjeri redovito koriste antiviruse u svrhu zaštite podataka, slijede ih sudionici s FSB-a i MEF-a (N=16), dok ih najrjeđe koriste sudionici s PMF-a, FER-a i FOI-a (N=4), no i dalje je to manji broj sudionika koji ne koristi antivirusne aplikacije.

Tablica 7. pokazuje i da korištenje različitih lozinki za različite internetske stranice kao metodu koju redovito koriste je označilo najviše sudionika s FOI-a (N=16), slijede oni s MEF-a (N=13), dok tu metodu rijetko koriste ili nikad ne koriste većinom sudionici s FFZG-a (N=10) i FSB-a (N=8). Ista tablica pokazuje i da su svi s MEF-a označili da redovito koriste snažne lozinke, slijede sudionici s FER-a (N=17) te FOI-a (N=16) i FFZG-a (N=16), dok najrjeđe to čine oni s UFZG-a (N=5) i PFZG-a (N=5). Što se korištenja *firewall*-a u svrhu zaštite podataka tiče, većinom ih redovito koriste sudionici s FER-a i FSB-a (N=13), slijede ih sudionici s FOI-a (N=11), dok sudionici s UFZG-a (N=10) te PMF-a i EFZG-a (N=9) većinom rijetko ili nikad ne koriste *firewall.*

(1) – nikada, (2) – rijetko, (3) – ponekad, (4) – često, (5) – vrlo često

		(1)	*(2)*	*(3)*	*(4)*	*(5)*
Izbjegavanje korištenja Facebook, Twitter ili Google računa za prijavu na druge internetske stranice	**FSB**	3	2	2	7	6
	FER	6	4	6	1	3
	FOI	3	1	5	4	7
	PMF	4	9	2	3	2
	FFZG	5	4	3	3	5
	EFZG	3	7	1	4	5
	PFZG	3	8	4	3	2
	MEF	4	7	3	4	2
	UFZG	4	5	7	2	2
	KIF	2	4	6	5	3
	N	**37**	**51**	**39**	**36**	**37**
	%	**18%**	**26%**	**20%**	**18%**	**18%**
	Zbroj i postotak neslaganja/slaganja	**88 (44%)**		**39(20%)**	**73 (37%)**	
Izbjegavanje spajanja na javne WiFi mreže,	**FSB**	6	4	2	4	3
	FER	5	3	5	2	5
	FOI	4	5	8	2	1
	PMF	5	8	2	4	1
	FFZG	2	8	5	2	3
	EFZG	3	7	2	3	5
	PFZG	3	6	6	4	1
	MEF	9	5	4	1	1
	UFZG	5	7	6	2	0
	KIF	3	7	4	2	4
	N	**45**	**60**	**44**	**26**	**24**
	%	**23%**	**30%**	**22%**	**13%**	**12%**
	Zbroj i postotak neslaganja/slaganja	**105 (53%)**		**44(22%)**	**50 (25%)**	

		(1)	*(2)*	*(3)*	*(4)*	*(5)*
Korištenje VPN mreža	**FSB**	6	6	4	4	0
	FER	5	5	5	4	1
	FOI	5	4	10	1	0
	PMF	8	5	5	2	0
	FFZG	6	4	5	4	1
	EFZG	10	4	4	1	1
	PFZG	5	3	7	2	3
	MEF	5	6	3	6	0
	UFZG	6	2	13	0	0
	KIF	6	6	4	4	0
	N	**62**	**40**	**60**	**28**	**6**
	%	**31%**	**20%**	**30%**	**14%**	**3%**
	Zbroj i postotak neslaganja/slaganja	**102 (51%)**		**60(30%)**	**34 (17%)**	
Uključivanje „Ne prati“ sigurnosne funkcije pretraživača	**FSB**	10	5	1	2	2
	FER	4	5	4	3	4
	FOI	2	5	7	1	5
	PMF	10	5	2	1	2
	FFZG	9	2	0	5	4
	EFZG	12	2	3	1	2
	PFZG	8	5	4	0	3
	MEF	10	3	2	1	4
	UFZG	6	5	5	1	3
	KIF	9	4	2	4	4
	N	**80**	**41**	**34**	**19**	**30**
	%	**40%**	**21%**	**17%**	**9%**	**15%**
	Zbroj i postotak neslaganja/slaganja	**121 (61%)**		**34(17%)**	**49 (25%)**	

Tablica 8. Učestalost korištenja pojedinih metoda zaštite podataka (Izvor: istraživanje autora) (N=200)

Rezultati (Tablica 8.) pokazuju da je izbjegavanje korištenja Facebook, Twitter ili Google računa za prijavu na druge internetske stranice metoda zaštite osobnih podataka koju većinom koriste sudionici s FSB-a (N=13) i FOI-a (N=11), dok ju većinom rijetko koriste ili nikad ne koriste sudionici s PMF-a (N=13) te sudionici s PFZG-a i MEF-a (N=11). Nadalje, izbjegavanje spajanja na javne WiFi mreže je metoda koju većinom redovito koriste sudionici s EFZG-a (N=8) te FER-a i FSB-a (N=7), dok ju većinom rijetko koriste ili nikad ne koriste sudionici s MEF-a (N=14) i PMF-a (N=13). Rezultati pokazuju kako je uključivanje „Do Not Track“ sigurnosne značajke preglednika metoda koju sudionici rijetko koriste, no često ili vrlo često ju koristi devetero sudionika s FFZG-a, što je najveći broj studenata jednog fakulteta koji koristi tu metodu, a slijede ih studenti KIF-a (N=8), dok većinom rijetko koriste ili nikad tu metodu ne koriste sudionici s PMF-a i FSB-a (N=15). Rezultati pokazuju i da korištenje VPN mreža također nije popularna metoda zaštite među sudionicima, većinom ju redovito koriste studenti MEF-a (N=6), a najrjeđe ju koriste sudionici s EFZG-a (N=14) i PMF-a (N=13).

(1) – nikada, (2) – rijetko, (3) – ponekad, (4) – često, (5) – vrlo često

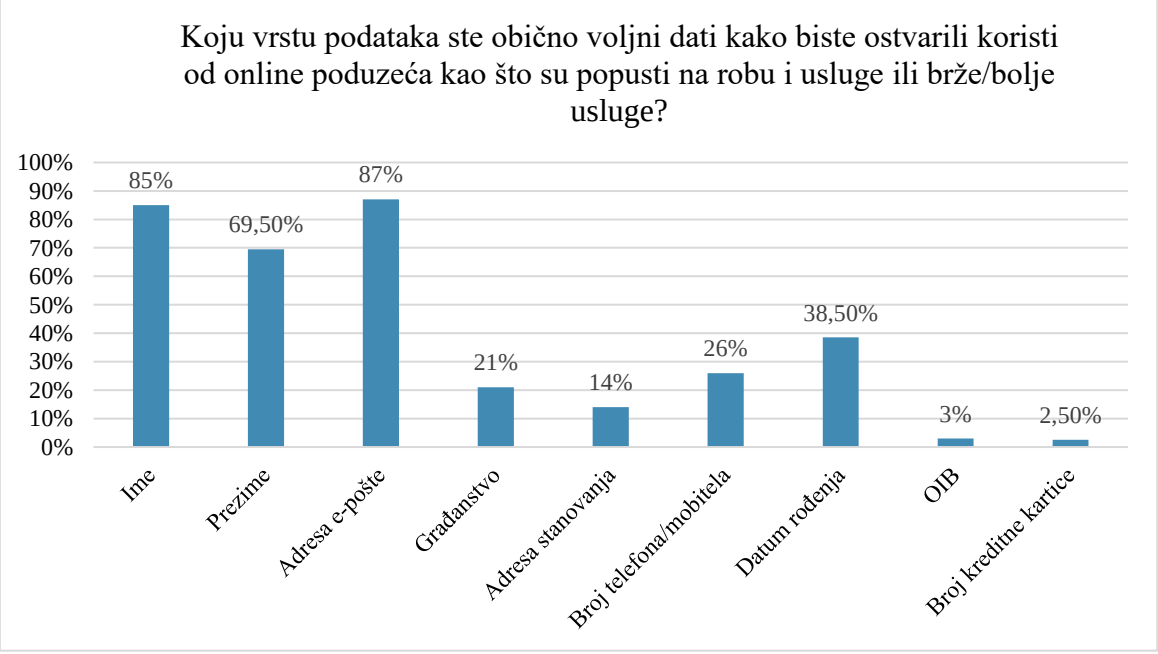
		(1)	*(2)*	*(3)*	*(4)*	*(5)*
Korištenje dodataka za pretraživače koji blokiraju oglase	**FSB**	5	3	2	1	9
	FER	0	2	0	6	12
	FOI	2	0	2	3	13
	PMF	6	6	3	0	5
	FFZG	5	3	3	3	6
	EFZG	9	1	3	2	5
	PFZG	6	5	2	2	5
	MEF	7	4	1	2	6
	UFZG	7	5	2	3	3
	KIF	8	3	4	4	1
	N	**55**	**32**	**22**	**26**	**65**
	%	**27.5%**	**16%**	**11%**	**13%**	**32.5%**
	Zbroj i postotak neslaganja/slaganja	**87 (43.5%)**		**22(11%)**	**91 (45.5%)**	
Brisanje „kolačića“	**FSB**	6	5	3	1	5
	FER	4	6	4	5	1
	FOI	2	5	7	3	3
	PMF	7	3	5	3	2
	FFZG	6	3	3	4	4
	EFZG	8	3	4	3	1
	PFZG	4	6	3	4	3
	MEF	8	0	4	7	1
	UFZG	7	3	3	4	3
	KIF	12	1	4	2	1
	N	**64**	**35**	**40**	**36**	**21**
	%	**33%**	**18%**	**20%**	**18%**	**11%**
	Zbroj i postotak neslaganja/slaganja	**99 (51%)**		**40(20%)**	**57 (29%)**	

		(1)	*(2)*	*(3)*	*(4)*	*(5)*
Izbjegavanje stranica koje zahtijevaju obavezno prihvaćanje „kolačića“ za pristup njima	**FSB**	7	8	3	1	1
	FER	6	6	7	0	1
	FOI	5	5	3	5	2
	PMF	7	7	3	2	1
	FFZG	7	6	2	2	3
	EFZG	4	6	6	1	3
	PFZG	8	6	1	4	1
	MEF	9	5	4	1	1
	UFZG	6	4	7	1	2
	KIF	8	5	2	4	1
	N	**67**	**58**	**38**	**21**	**16**
	%	**33.5%**	**29%**	**19%**	**10.5%**	**8%**
	Zbroj i postotak neslaganja/slaganja	**125 (62.5%)**		**38(19%)**	**37 (18.5%)**	
Ispunjavanje lažnih podataka o sebi kada su isti zatraženi	**FSB**	6	4	4	6	0
	FER	6	1	6	6	1
	FOI	3	3	6	4	4
	PMF	0	4	11	4	2
	FFZG	2	5	6	2	5
	EFZG	7	3	6	1	3
	PFZG	4	3	5	7	1
	MEF	1	9	3	2	5
	UFZG	7	5	7	0	1
	KIF	9	1	5	2	3
	N	**45**	**38**	**59**	**33**	**25**
	%	**22.5%**	**19%**	**29.5%**	**16.5%**	**12.5%**
	Zbroj i postotak neslaganja/slaganja	**83 (41.5%)**		**59 (29.5%)**	**58 (29%)**	

Tablica 9. Učestalost korištenja pojedinih metoda zaštite podataka (Izvor: istraživanje autora) (N=200)

Rezultati (Tablica 9.) pokazuju kako većinom redovito koriste dodatke za blokiranje oglasa sudionici s FER-a (N=18), slijede ih oni s FOI-a (N=16), dok većinom rijetko ili nikad ne koriste iste sudionici s PMF-a i UFZG-a (N=12), slijede ih sudionici s KIF-a (N=11). Rezultati pokazuju i da redovito brišu „kolačiće“ putem preglednika većinom sudionici s FFZG-a (N=8) te MEF-a s istim brojem, slijede ih oni s FOI-a, FER-a i FSB-a (N=6), dok većinom rijetko brišu ili nikad ne brišu „kolačiće“ sudionici s KIF-a (N=13), slijede ih oni s FSB-a i EFZG-a (N=11). Iz iste tablice saznajemo da je izbjegavanje pristupa internetskim stranicama s obaveznim prihvaćanjem „kolačića“ najmanje popularna metoda zaštite podataka među sudionicima; od 37 sudionika koji ju redovito koriste najviše je onih s FOI-a (N=7), dok ju većinom rijetko koriste ili nikad ne koriste oni s FSB-a (N=15) te PMF-a, PFZG-a i MEF-a (N=14). Također, rezultati pokazuju da je ispunjavanje lažnih podataka kada je ispunjavanje osobnih podataka zatražena na internetu metoda koju redovito većinom koriste sudionici s FOI-a i PFZG-a (N=8), dok ju rijetko koriste ili nikad ne koriste većinom sudionici s UFZG-a (N=12) te MEF-a, FSB-a i KIF-a (N=10).

Zanimalo nas je i koju vrstu podataka su sudionici uglavnom voljni dati kako bi ostvarili koristi od internetskih tvrtki poput popusta na robu ili bolje usluge kako bismo saznali koje osobne podatke sudionici vrednuju više od drugih, odnosno s kojim su podacima sudionici spremni trgovati.



Grafikon 3. Spremnost davanja osobnih podataka internetskim trtkama (Izvor: istraživanje autora) (N=200)

Većina je sudionika spremna internetskim poduzećima dati svoje ime (N=170), svoju adresu e-pošte (N=174) i svoje prezime (N=139) kako bi ostvarili koristi od istih, dok većinom nisu voljni dati svoj OIB (N=6), broj kreditne kartice (N=5) i adresu stanovanja (N=28). Velik je broj sudionika voljan dati i svoj datum rođenja (N=77), broj telefona ili mobilnog telefona (N=52) te informacije o svojem građanstvu (N=42).

Zanimalo nas je i razlikuje li se spremnost na davanje osobnih podataka internetskim tvrtkama radi ostvarivanja koristi od njih među sudionicima s obzirom na fakultet koji pohađaju.

	Ime	*Prezime*	*Adresa e-pošte*	*Građanstvo*	*Adresa stanovanja*	*Broj telefona /mob.*	*Datum rođenja*	*OIB*	*Broj kreditne kartice*	***N***
FSB	19	18	18	6	4	10	7	1	0	**83**
FER	15	11	16	7	2	3	12	1	0	**67**
FOI	15	11	17	4	1	4	6	0	1	**59**
PMF	17	16	18	4	4	7	10	1	1	**78**
FFZG	17	14	17	4	3	4	10	1	0	**70**
EFZG	16	14	16	5	3	3	7	0	2	**66**
PFZG	14	7	19	1	1	2	6	0	0	**50**
MEF	19	12	16	1	1	5	3	1	0	**58**
UFZG	19	18	19	2	3	5	7	0	0	**73**
KIF	19	18	18	8	6	9	9	1	1	**89**
N	**170**	**139**	**174**	**42**	**28**	**52**	**77**	**6**	**5**	

Tablica 10. Spremnost davanja osobnih podataka internetskim tvrtkama s obzirom na fakultet (Izvor: istraživanje autora (N=200)

Rezultati (Tablica 10.) pokazuju kako su internetskim tvrtkama najveći broj osobnih podataka spremni dati sudionici s KIF-a (N=89), FSB-a (N=83) i PMF-a (N=78), dok su najmanji broj osobnih podataka spremni dati sudionici s PFZG-a (N=50), MEF-a (N=58) i FOI-a (N=59).

Zanimala nas je i upućenost sudionika u pravne aspekte zaštite osobnih podataka. Upućenost u pravne aspekte zaštite osobnih podataka među sudionicima ispitali smo pitanjima u kojima su sudionici morali označiti s kojim su pravima upoznati, te koja su prava do sada koristili, a koja im omogućuje Opća uredba o zaštiti osobnih podataka.

	P. na pristup osobnim podacima	*P. na ispravak osobnih podataka*	*P. na brisanje osobnih podataka*	*P. na ograničenje obrade osobnih podataka*	*P. na prigovor*	*P. na pre-nosivost Podataka*	*Nijedno*	*N*
FSB	11	5	8	6	6	3	9	**39**
FER	14	3	5	6	2	1	5	**31**
FOI	14	11	13	11	9	6	3	**64**
PMF	11	2	5	8	3	3	7	**32**
FFZG	12	4	4	5	4	3	4	**32**
EFZG	14	2	6	9	3	2	3	**36**
PFZG	19	13	16	18	13	12	1	**91**
MEF	12	5	5	13	3	5	2	**43**
UFZG	17	5	3	11	7	3	2	**46**
KIF	9	2	3	7	4	1	8	**26**
N	**133**	**52**	**68**	**94**	**54**	**39**	**44**	

Tablica 11. Upoznatost s pravima omogućenim Općom uredbom o zaštiti podataka (Izvor: istraživanje autora) (N=200)

Rezultati iz Tablice 11. prikazuju kako su s najvećim brojem prava omogućenim Općom uredbom o zaštiti podataka upoznati sudionici s PFZG-a (N=91), FOI-a (N=64) i UFZG-a (N=46), dok su s najmanjim brojem prava upoznati oni s KIF-a (N=26), FER-a (N=31) te PMF-a i FFZG-a (N=32). Pravo pristupa osobnim podacima jedino je pravo s kojim je većina upoznata (N=133), dok je s ostalih pet prava manjina upoznata. Oznaku da nisu upoznati s nijednim navedenim pravom označilo je 44 sudionika. S pravom na ograničenje obrade osobnih podataka upoznato je njih 94, dok su s ostalim pravima upoznati u manjini. S pravom na ispravak osobnih podataka upoznato je njih 52, s pravom na brisanje osobnih podataka njih 68, s pravom na prigovor njih 54, a s pravom na prenosivost podataka 39 sudionika.

Zatim smo ispitali jesu li ikada u prošlosti koristili neka od navedenih prava, koja su prava koristili te usporedili rezultate s obzirom na fakultet koji pohađaju.

	P. na pristup osobnim podacima	*P. na ispravak osobnih podataka*	*P. na brisanje osobnih podataka*	*P. na ograniče-nje obrade osobnih podataka*	*P. na prigovor*	*P. na pre-nosivost Podataka*	*Nijedno*	*N*
FSB	4	1	4	1	1	1	13	**12**
FER	8	1	5	4	0	1	10	**19**
FOI	10	3	8	7	3	3	9	**34**
PMF	5	1	3	2	0	1	13	**12**
FFZG	6	1	1	0	1	0	12	**9**
EFZG	3	0	0	2	1	0	16	**6**
PFZG	7	5	6	6	1	2	9	**27**
MEF	6	2	5	4	1	3	7	**21**
UFZG	8	1	2	3	3	0	10	**17**
KIF	3	0	1	1	0	0	14	**5**
N	**60**	**15**	**35**	**30**	**11**	**11**	**113**	

Tablica 12. Korištena prava Opće uredbe o zaštiti podataka (Izvor: istraživanje autora) (N=200)

Rezultati (Tablica 12.) prikazuju da su navedena prava najviše koristili sudionici s FOI-a (N=34), PFZG-a (N=27), MEF-a (N=21), dok su najmanje svoja prava koristili sudionici s KIF-a (N=5), EFZG-a (N=6 FFZG-a (N=9) te PMF-a i FSB-a (N=12). Većina do sada nije koristila nijedno od navedenih prava (N=113). Među sudionicima je do sada najčešće korišteno pravo pristupa osobnim podacima, kojeg je do sada koristilo njih 60, dok su sva ostala prava korištena u manjini; korištenje prava na ograničenje obrade označilo je njih 30, pravo na prenosivost podataka njih 11, isti broj pravo na prigovor, pravo na ograničenje obrade njih 30, pravo na brisanje osobnih podataka njih 35, a pravo na ispravak osobnih podataka 15 sudionika.

Zatim smo ispitali znanja sudionika o internetskim „kolačićima“ i njihovo korištenje dodatnih metoda zaštite podataka poput isključivanja personalizacije oglasa, neodgovaranja na neželjenu e-poštu i dr.

Znate li značenje „kolačića“ na internetskim stranicama?			
	Da	**Ne**	**Nisam siguran/na**
1. FOI	18	0	2
2. PFZG	17	1	2
3. FER	16	0	4
4. FSB	13	3	4
5. EFZG	10	1	9
6. FFZG	10	3	7
7. PMF	10	4	6
8. UFZG	9	1	10
9. MEF	8	8	3
10. KIF	7	6	7
N	***118***	***27***	***54***

Tablica 13. Znanja o internetskim „kolačićima“ (Izvor: istraživanje autora) (N=199)

Rezultati (Tablica 13). pokazuju da većina sudinika (N=118) razumije značenje „kolačića“ na internetu, dok 27 sudionika ne razumije, a 54 ih nije sigurno. Većina je sudionika s FOI-a (N=18), PFZG-a (N=17), FER-a (N=16) te FSB-a (N=13) upoznata sa značenjem „kolačića“, dok su s njima najmanje upoznati sudionici s KIF-a (N=7), MEF-a (N=8) i UFZG-a (N=9).

Znate li postaviti internetski pretraživač tako da ne prima „kolačiće“ bez prethodnog upita?			
	Da	**Ne**	**Nisam siguan/na**
1. FER	16	4	0
2. FOI	14	6	0
3. FFZG	10	9	1
4. FSB	10	10	0
5. PFZG	9	8	3
6. MEF	7	9	3
7. UFZG	6	8	6
= PMF	6	8	6
8. EFZG	4	8	8
9. KIF	2	14	4
N	***84***	***84***	***31***

Tablica 14. Znanja o postavljanju internetskog pretraživača tako da ne prima „kolačiće“ bez prethodnog upita (Izvor: istraživanje autora) (N=199)

Unatoč tome što većina sudionika zna značenje „kolačića“ na internetu, jednak broj (N=84) zna i ne zna postaviti internetski pretraživač tako da ih ne prima bez prethodnog upita. Većinom sudionici s FER-a (N=16), FOI-a (N=14), FFZG-a (N=10) te FSB-a (N=10) znaju postaviti internetski pretraživač da ne prima „kolačiće“ bez upita, dok većinom oni s KIF-a (N=14), EFZG-a (N=8) te UFZG-a i PMF-a (N=8) najmanje znaju.

Sudionike smo ispitali i jesu li u prošlosti mijenjali postavke „kolačića“ na svojem internetskom pretraživaču.

Jeste li do sada promijenili postavke „kolačića“ na Vašem web pregledniku?			
	Da	**Ne**	**Nisam siguran/na**
1. FOI	11	8	1
2. PMF	9	9	2
3. PFZG	9	10	1
4. FER	9	11	0
= FSB	9	11	0
5. UFZG	8	7	5
6. FFZG	8	10	2
7. EFZG	5	10	5
8. MEF	5	11	3
9. KIF	2	15	3
N	***88***	***89***	***22***

Tablica 15. Ponašanja po pitanju mijenjanja postavki „kolačića“ na internetskom pregledniku (Izvor: istraživanje autora) (N=199)

U rezultatima (Tablica 15.) pronalazimo odgovore sudionika na pitanje „Jeste li do sada promijenili postavke „kolačića“ na Vašem web pregledniku?“ Unatoč tome što je samo 84 sudionika odgovorilo da zna postaviti svoj pretraživač tako da ne prima „kolačiće“, 88 sudionika odgovorilo je da su mijenjali postavke „kolačića“ na pregledniku, što znači da su ih mijenjali na način koji i dalje prima „kolačiće“. Većinom su samo sudionici s FOI-a

(N=11) nekada u prošlosti mijenjali postavke „kolačića“ na vlastitom internetskom pregledniku, dok većinom oni s KIF-a (N=15), MEF-a (N=11), FSB-a (N=11) i FER-a (N=11) to nisu nikada u prošlosti napravili.

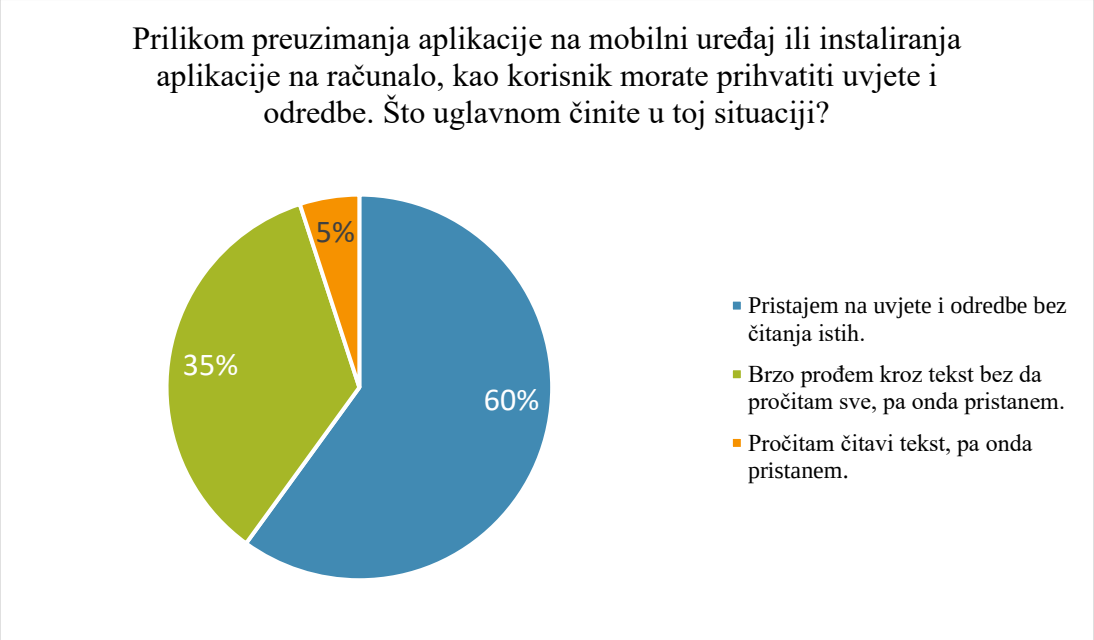
Slične rezultate pronalazimo među sudionicima i na pitanje „Jeste li ikada u prošlosti isključili personalizaciju oglasa na Vašem web pretraživaču?“.

Jeste li ikada u prošlosti isključili personalizaciju oglasa na Vašem web pretraživaču?			
	Da	**Ne**	**Nisam siguran/na**
1. FER	13	5	2
2. FOI	12	3	5
3. FFZG	12	4	4
4. FSB	10	10	0
5. PFZG	9	9	2
6. PMF	9	10	1
7. MEF	6	11	2
8. UFZG	5	9	6
9. EFZG	5	10	5
10. KIF	4	12	3
N	***85***	***83***	***30***

Tablica 16. Ponašanja sudionika po pitanju isključivanja personalizacije oglasa (Izvor: istraživanje autora) (N=198)

Rezultati (Tablica 16.) pokazuju da je većina studenata (N=85) nekada u prošlosti isključila personalizaciju oglasa. Većinom su nekada u prošlosti isključili personalizaciju oglasa sudionici s FER-a (N=13), FOI-a (N=12), EFZG-a (N=12) te FSB-a (N=10), dok većinom to u prošlosti nisu napravili sudionici s KIF-a (N=12), MEF-a (N=11), EFZG-a (N=10) te FSB-a (N=10). Dakle, podjednak broj studenata je nekada u prošlosti mijenjao postavke kolačića putem preglednika i isključio personalizaciju kao i broj studenata koji to nikada do sada nisu napravili. Potvrdno na prethodna četiri pitanja najviše su odgovarali sudionici s FOI-a (N=56), FER-a (N=54), PFZG-a (N=44) te FSB-a (N=42), dok najviše negativnih odgovora iznose sudionici KIF-a (N=47), MEF-a (N=39), PMF-a (N=31) i EFZG-a (N=29).

Zanimalo nas je i što sudionici čine kada su suočeni s neželjenom elektroničkom poštom te uvjetima i odredbama prilikom preuzimanja aplikacija.



Grafikon 4. Ponašanja sudionika kada su suočeni s Uvjetima i odredbama (Izvor: istraživanje autora) (N=199)

Na pitanje odgovaraju li na neželjenu elektroničku poštu samo su dva sudionika (oboje s KIF-a) odgovorila „ponekad“, dok su svi ostali odgovorili „ne“.

Zatim smo ispitali što studenti čine prilikom preuzimanja aplikacije na mobilni uređaj ili instaliranja aplikacije na računalo kada se od korisnika traži prihvaćanje uvjeta i odredbi. Rezultati (Grafikon 4.) pokazuju da njih 60% (N=120) uopće ne pročita, niti brzo prođe kroz tekst uvjeta i odredbi prije pristanka na iste. Brzo prođe kroz tekst uvjeta i odredbi 35% sudionika (N=69), dok 5% sudionika (N=10) pročita čitavi tekst uvjeta i odredbi prije pristanka.

Zatim smo usporedili razlikuje li se navika čitanja uvjeta i odredbi među sudionicima s obzirom na fakultet koji pohađaju.

	Pristajem na uvjete i odredbe bez čitanja istih	*Brzo prođem kroz tekst, pa onda pristanem*	*Pročitam čitavi tekst, pa onda pristanm*
FSB	13	7	0
FER	14	6	0
FOI	9	8	3
PMF	12	7	1
FFZG	14	4	2
EFZG	12	6	2
PFZG	13	6	1
MEF	13	6	0
UFZG	8	11	1
KIF	12	8	0
N	**120**	**69**	**10**

Tablica 17. Ponašanja sudionika kada su suočeni s uvjetima i odredbama pri preuzimanju i instaliranju aplikacija (Izvor: istraživanje autora) (N=199)

Prema rezultatima (Tablica 17.), sudionici s FOI-a najviše čitaju uvjete i odredbe, troje u potpunosti, dok ih osmero brzo prođe kroz tekst prije pristanka. Velik broj sudionika s UFZG-a (N=11) također brzo prođe kroz tekst prije pristanka, dok kod svih ostalih fakulteta većinom prevladavaju oni sudionici koji uopće ne pročitaju tekst uvjeta i odredbi.

Sljedećom smo kategorijom pitanja, oblikovanih u tvrdnje s kojima sudionici izražavaju svoje slaganje, ispitali stupanj zabrinutosti studenata u vezi privatnosti i ugroženosti vlastitih podataka na internetu, stupanj povjerenja koji sudionici imaju u internetske tvrtke te njihov stav spram zaštite osobnih podataka.

Prvom smo tvrdnjom ispitali razinu zabrinutosti sudionika zbog ugroženosti osobnih podataka na internetu.

Zabrinut/a sam zbog ugroženosti svojih osobnih podataka na internetu.					
	Slažem se	**Potpuno se slažem**	**Niti se slažem niti ne slažem**	**Ne slažem se**	**Nimalo se ne slažem**
FFZG	6	4	4	5	1
PFZG	5	4	6	3	2
FER	8	1	3	4	4
PMF	4	4	7	3	2
FOI	5	3	4	6	2
KIF	5	2	6	6	0
EFZG	4	2	9	5	0
UFZG	4	2	3	9	2
FSB	2	3	7	2	5
MEF	1	3	5	6	1
N	***44***	***28***	***54***	***49***	***19***
%	***22%***	***14%***	***28%***	***25%***	***10%***
Zbroj i postotak neslaganja/slaganja	***72 (37%)***		***54 (28%)***	***68 (35%)***	

Tablica 18. Zabrinutost za vlastite osobne podatke (Izvor: istraživanje autora) (N=194)

Rezultati (Tablica 18.) pokazuju da 35% sudionika (N=68) nije ili uopće nije zabrinuta zbog ugroženosti, dok je njih 37% (N=72) zabrinuto, ili je u potpunosti zabrinuto zbog te

ugroženosti, a njih 27,83% (N=54) se niti slažu, niti ne slažu s tvrdnjom. Sudionici s FFZG-a u najvećoj su mjeri iskazali zabrinutost slaganjem ili potpunim slaganjem s tvrdnjom (N=10). Slijede ih sudionici s FER-a i PFZG-a (N=9) te oni s FOI-a i FER-a (N=8), a najmanje slaganja izrazili su sudionici s MEF-a (N=4). Najviše neslaganja s tvrdnjom označili su sudionici s UFZG-a (N=11), FER-a i FOI-a (N=8) te FSB-a i MEF-a (N=7).

Sljedećom smo tvrdnjom ispitali povjerenje sudionika u internetske stranice.

Smatram da će internetske tvrtke čuvati povjerljivim ono što o meni saznaju iz mojih aktivnosti na njihovoj internetskoj stranici.					
	Nimalo se ne slažem	**Ne slažem se**	**Niti se slažem niti ne slažem**	**Slažem se**	**Potpuno se slažem**
FSB	2	7	6	3	1
FER	5	7	5	3	0
FOI	4	7	3	6	0
PMF	3	9	5	2	1
FFZG	5	3	9	3	0
EFZG	5	2	8	3	2
PFZG	3	5	6	5	0
MEF	2	4	4	5	1
UFZG	1	5	6	6	2
KIF	0	10	3	5	1
N	**30**	**59**	**55**	**41**	**8**
%	**16%**	**30%**	**28%**	**21%**	**4%**
Zbroj i postotak neslaganja/slaganja	**89 (46%)**		**55 (28%)**	**49 (25%)**	

Tablica 19. Povjerenje u internetske tvrtke (Izvor: istraživanje autora) (N=193)

Rezultati (Tablica 19.) pokazuju da je povjerenje u internetske stranice po pitanju zaštite osobnih podataka nisko, jer je 46% sudionika (N=89) označilo jedan od stupnjeva neslaganja s tvrdnjom, dok je 25% sudionika (N=49) označilo jedan od stupnjeva slaganja. Najviše oznaka neslaganja s tom su tvrdnjom označili sudionici s PMF-a (N=12), FER-a i FOI-a (N=11) te KIF-a (N=10), dok su najviše slaganja označili oni s UFZG-a (N=8) te MEF-a, FOI-a i KIF-a (N=6).

Stavove sudionika o prikupljanju osobnih podataka ispitali smo tvrdnjom „Smatram kako nije dobro to što trgovci na internetu mogu saznati osobne podatke o internetskim kupcima bez njihovog pristanka“.

Smatram kako nije dobro to što trgovci na internetu mogu saznati osobne podatke o internetskim kupcima bez njihovog pristanka.					
	Nimalo se ne slažem	**Ne slažem se**	**Niti se slažem niti ne slažem**	**Slažem se**	**Potpuno se slažem**
FSB	0	2	5	4	9
FER	1	0	3	4	12
FOI	1	1	4	2	12
PMF	0	1	2	3	14
FFZG	0	0	0	7	13
EFZG	0	0	4	7	9
PFZG	0	2	3	4	11
MEF	0	0	3	1	12
UFZG	0	0	5	5	10
KIF	0	4	5	4	6
N	**2**	**10**	**34**	**41**	**108**
%	**1%**	**5%**	**17%**	**21%**	**55%**
Zbroj i postotak neslaganja/slaganja	**12 (6%)**		**34 (17%)**	**149 (76%)**	

Tablica 20. Stavovi o prikupljanju osobnih podataka (Izvor: istraživanje autora) (N=195)

Rezultati (Tablica 20.) pokazuju da je s ovom tvrdnjom 76% sudionika (N=149) izrazilo jedan od stupnjeva slaganja, dok ih je 6% (N=12) izrazilo neslaganje. Kod ove tvrdnje nismo naišli na velike razlike u obrascima odgovaranja s obzirom na to koji fakultet sudionici pohađaju, ali smo uočili da su jedino sudionici s FSB-a, za razliku od ostalih, izrazili vrlo malo slaganja s tvrdnjom (N=4), s podosta neslaganja (N=9).

Stavove o prikupljanju osobnih podataka ispitali smo i tvrdnjom „Smeta me kada internetske tvrtke traže moje osobne podatke“.

Smeta me kada internetske tvrtke traže moje osobne podatke.					
	Nimalo se ne slažem	**Ne slažem se**	**Niti se slažem niti ne slažem**	**Slažem se**	**Potpuno se slažem**
FSB	1	1	8	5	5
FER	0	1	4	9	6
FOI	0	4	2	4	10
PMF	0	3	1	6	10
FFZG	0	1	2	8	9
EFZG	0	0	5	4	11
PFZG	0	0	5	5	10
MEF	0	0	4	8	4
UFZG	0	0	2	7	11
KIF	0	6	4	4	5
N	**1**	**16**	**37**	**60**	**81**
%	**1%**	**8%**	**19%**	**31%**	**41%**
Zbroj i postotak neslaganja/slaganja	**17 (9%)**		**37 (19%)**	**141 (72%)**	

Tablica 21. Stavovi o prikupljanju osobnih podataka (Izvor: istraživanje autora) (N=195)

Rezultati iz Tablice 21. pokazuju da je s ovom tvrdnjom 72% sudionika (N=141) označilo jedan od stupnjeva slaganja, a 9% sudionika (N=17), a 19% sudionika (N=37) označilo je oznaku „niti se slažem niti ne slažem“. Vrlo su male varijacije u odgovorima s obzirom na to koji fakultet studenti pohađaju. Jedino sudionici s FSB-a i KIF-a nisu u većini označili oznake

slaganja u usporedbi sa sudionicima s drugih fakulteta, već ih je 9 označilo jedan od stupnjeva slaganja.

Povjerenje sudionika po pitanju zaštite osobnih podataka ispitali smo i tvrdnjom „Vjerujem da su moji osobni podatci sigurni na internetskim stranicama“.

Vjerujem da su moji osobni podatci sigurni na internetskim stranicama					
	Nimalo se ne slažem	**Ne slažem se**	**Niti se slažem niti ne slažem**	**Slažem se**	**Potpuno se slažem**
FSB	3	4	9	3	0
FER	3	6	11	0	0
FOI	2	5	6	7	0
PMF	3	7	7	3	0
FFZG	5	8	6	1	0
EFZG	3	5	11	0	0
PFZG	3	6	9	2	0
MEF	4	5	4	3	0
UFZG	3	4	12	1	0
KIF	2	10	3	0	1
N	**31**	**60**	**78**	**20**	**1**
%	**16%**	**32%**	**41%**	**10%**	**1%**
Zbroj i postotak neslaganja/slaganja	**91 (48%)**		**78 (41%)**	**21 (11%)**	

Tablica 22. Povjerenje u internetske stranice (Izvor: istraživanje autora) (N=190)

Rezultati iz Tablice 22. ponovno pokazuju da je povjerenje u internetske stranice po pitanju zaštite osobnih podataka nisko, jer je 48% sudionika (N=91) označilo jedan od stupnjeva neslaganja s tvrdnjom, dok je 11% sudionika (N=21) označilo jedan od stupnjeva slaganja. Najviše oznaka neslaganja s tom su tvrdnjom označili sudionici s FFZG-a (N=13), KIF-a (N=12) te PMF-a (N=10), dok su najviše slaganja označili sudionici s FOI-a (N=7).

Sudionike smo ispitali i razmisle li dobro prije nego što predaju osobne podatke na internetu.

Kada me internetske tvrtke pitaju za osobne podatke, dobro razmislim prije nego što ih dam					
	Nimalo se ne slažem	**Ne slažem se**	**Niti se slažem niti ne slažem**	**Slažem se**	**Potpuno se slažem**
FSB	0	5	5	5	5
FER	0	3	5	7	5
FOI	0	2	3	2	13
PMF	0	3	3	5	9
FFZG	0	2	4	3	11
EFZG	1	1	1	7	10
PFZG	0	1	0	8	11
MEF	0	0	1	8	7
UFZG	0	4	3	6	7
KIF	0	5	2	4	8
N	**1**	**27**	**27**	**55**	**86**
%	**1%**	**13%**	**14%**	**28%**	**44%**
Zbroj i postotak neslaganja/slaganja	**28 (14%)**		**27 (14%)**	**141 (72%)**	

Tablica 23. Promišljanja prije davanja osobnih podataka na internetu (izvor: istraživanje autora) (N=196)

Iz Tablice 23. iščitavamo da kod ove tvrdnje također prevladavaju odgovori slaganja s tvrdnjom, 72% sudionika se slaže s tvrdnjom (N=141), dok se 14% sudionika (N=28) ne slaže s njom, a 14% (N=27) se niti slaže niti ne slaže. Odgovori slaganja kod ove tvrdnje jedino kod sudionika s FSB-a nisu u većini, dok kod sudionika svih drugih fakulteta jesu, s malenim brojem neslaganja u odnosu na odgovore slaganja. Najviše slaganja s tom tvrdnjom izrazili su sudionici s PFZG-a (N=19), sudionici s EFZG-a (N=17) te FOI-a i EFZG-a (N=15).

Zanimala nas je i razina zabrinutosti koju sudionici pokazuju spram svojih osobnih podataka na internetu.

Zabrinut/a sam da internetske tvrtke prikupljaju previše osobnih podataka o meni					
	Nimalo se ne slažem	**Ne slažem se**	**Niti se slažem niti ne slažem**	**Slažem se**	**Potpuno se slažem**
FSB	0	1	6	6	7
FER	0	5	5	8	2
FOI	1	2	3	5	9
PMF	0	3	3	6	8
FFZG	0	4	3	6	7
EFZG	0	2	8	2	8
PFZG	0	1	5	7	7
MEF	1	0	4	7	4
UFZG	0	4	6	8	2
KIF	1	6	4	4	4
N	**3**	**28**	**47**	**59**	**58**
%	**2%**	**14%**	**24%**	**30%**	**30%**
Zbroj i postotak neslaganja/slaganja	**31 (16%)**		**47 (24%)**	**117 (60%)**	

Tablica 24. Zabrinutost po pitanju osobnih podataka na internetu (Izvor: istraživanje autora) (N=195)

Rezultati iz Tablice 24. pokazuju da je na tvrdnju zabrinutosti po pitanju osobnih podataka na internetu s jednim od stupnjeva slaganja odgovorilo 60% sudionika (N=117), 16% (N=31) s jednim od stupnjeva neslaganja, a 24% (N=47) s „niti se slažem niti ne slažem“. Sudionici s FOI-a, PFZG-a i PMF-a najviše su odgovorili sa slaganjem (N=14), slijede ih sudionici s FFZG-a i FSB-a (N=13), dok su najviše neslaganja izrazili sudionici KIF-a (N=6) i FER-a (N=5).

Ispitali smo i stavove sudionika spram perosnaliziranih oglasa koji se pojavljuju na internetu.

Smatram personalizirane oglase koji mi se pojavljuju na internetu napasnima					
	Nimalo se ne slažem	**Ne slažem se**	**Niti se slažem niti ne slažem**	**Slažem se**	**Potpuno se slažem**
FSB	0	3	5	4	8
FER	1	8	2	4	5
FOI	1	4	1	6	8
PMF	1	2	2	8	7
FFZG	1	0	2	7	10
EFZG	0	3	4	4	9
PFZG	0	0	6	5	9
MEF	2	1	3	6	4
UFZG	0	5	2	4	9
KIF	0	7	4	5	3
N	**6**	**33**	**31**	**53**	**72**
%	**3%**	**17%**	**16%**	**27%**	**37%**
Zbroj i postotak neslaganja/slaganja	**39 (20%)**		**31 (16%)**	**125 (64%)**	

Tablica 25. Stavovi o personaliziranim oglasima na internetu (Izvor: istraživanje autora) (N=195)

Rezultati iz Tablice 25. pokazuju da su oni koji ih smatraju napasnima u većini, 64% (N=125), dok se njih 20% (N=39) ne slaže ili u potpunosti ne slaže s tvrdnjom, a 16% sudionika (N=31) se niti slaže niti ne slaže. Najviše su slaganja s tvrdnjom označili sudionici s FFZG-a (N=17), PMF-a (N=15), PFZG-a i FOI-a (N=14) te sudionici s EFZG-a i UFZG-a (N=13), dok su najviše neslaganja izrazili oni s FER-a (N=9) i KIF-a (N=7).

Sljedeća tvrdnja s kojom smo ispitali stavove sudionika po pitanju zaštite osobnih podataka je „Smatram problematičnim činjenicu da tvrtke koriste moje internetsku aktivnost za sakupljanje podataka o meni kako bi mi prikazivale odgovarajuće oglase“.

Smatram problematičnim činjenicu da tvrtke koriste moje internetsku aktivnost za sakupljanje podataka o meni kako bi mi prikazivale odgovarajuće oglase					
	Nimalo se ne slažem	**Ne slažem se**	**Niti se slažem niti ne slažem**	**Slažem se**	**Potpuno se slažem**
FSB	0	3	4	8	5
FER	3	4	3	4	6
FOI	1	4	3	5	7
PMF	1	0	4	7	8
FFZG	1	0	4	4	11
EFZG	0	4	2	5	9
PFZG	0	2	2	7	9
MEF	2	1	2	6	5
UFZG	0	1	4	6	9
KIF	0	5	7	3	4
N	**8**	**24**	**35**	**55**	**73**
%	**4%**	**12%**	**18%**	**28%**	**37%**
Zbroj i postotak slaganja/neslaganja	**32 (16%)**		**35 (18%)**	**128 (66%)**	

Tablica 26. Stavovi o prikupljanju osobnih podataka radi personalizacije oglasa (Izvor: istraživanje autora) (N=195)

Tablica 26. pokazuje da je s ovom tvrdnjom ponovno većina sudionika, 66% (N=128) označilo jedan od stupnjeva slaganja, najviše slaganja izrazili su sudionici s PFZG-a (N=16) te UFZG-a (N=15) i FFZG-a (N=15), dok ih je 16% (N=32) izrazilo neslaganje, od kojih najviše studenti FER-a (N=7) i FOI-a (N=5), a 18% (N=35) ih je označilo „niti se slažem niti ne slažem“.

Zanimalo nas je i slaganje sudionika s tvrdnjom „Oprostio/la bih tvrtki optuženoj zbog kršenja sigurnosti osobnih podataka ako me odmah obavijesti o prekršaju i onome što čini da me zaštiti“.

Oprostio/la bih tvrtki optuženoj zbog kršenja sigurnosti osobnih podataka ako me odmah obavijesti o prekršaju i onome što čini da me zaštiti					
	Nimalo se ne slažem	**Ne slažem se**	**Niti se slažem niti ne slažem**	**Slažem se**	**Potpuno se slažem**
FSB	5	1	6	5	2
FER	7	1	8	4	0
FOI	2	3	9	3	3
PMF	2	4	4	6	4
FFZG	5	5	6	3	1
EFZG	5	7	3	4	1
PFZG	2	5	7	5	1
MEF	1	2	8	3	2
UFZG	2	6	8	3	1
KIF	3	4	7	4	1
N	**34**	**38**	**66**	**40**	**16**
%	**17%**	**20%**	**34%**	**21%**	**8%**
Zbroj i postotak slaganja/neslaganja	**72 (37%)**		**66 (34%)**	**56 (29%)**	

Tablica 27. Stavovi o prikupljanju osobnih podataka radi personalizacije oglasa (Izvor: istraživanje autora) (N=194)

Iz rezultata iz Tablice 27. saznajemo da su sudionici na ovu tvrdnju u većini odgovarali s jednim od stupnjeva neslaganja, 37% (N=72), 29% (N=56) sa slaganjem, a 34% (N=66) s „niti se slažem niti ne slažem“. Najviše slaganja izrazili su sudionici s PMF-a (N=10), FSB-a (N=7) i FOI-a (N=6), dok su sudionici sa svih ostalih fakulteta odgovarali u većini s neslaganjem, a najviše neslaganja izrazili su sudionici s EFZG-a (N=12), FFZG-a (N=10) te FER-a i UFZG-a (N=8).

Posljednjim dvjema (zaključnim) tvrdnjama zaključili smo pokazuju li studenti veću sklonost zaštiti osobnih podataka ili personalizaciji usluga na internetu te smatraju li da je nemoguće zaštititi privatnost u današnjem digitalnom dobu.

Smatram da prednosti personaliziranih usluga na internetu koje proizlaze iz sakupljanja mojih osobnih podataka nadilaze važnost zaštite osobnih podataka.					
	Nimalo se ne slažem	**Ne slažem se**	**Niti se slažem niti ne slažem**	**Slažem se**	**Potpuno se slažem**
FSB	8	35	4	3	2
FER	4	6	8	2	0
FOI	4	8	4	3	0
PMF	5	9	2	2	2
FFZG	10	2	4	1	3
EFZG	4	6	6	2	2
PFZG	4	8	6	0	2
MEF	4	5	2	1	4
UFZG	6	2	4	5	3
KIF	1	3	5	8	2
N	**50**	**52**	**45**	**27**	**20**
%	**26%**	**27%**	**23%**	**14%**	**10%**
Zbroj i postotak slaganja/neslaganja	**102 (53%)**		**45 (23%)**	**47 (24%)**	

Tablica 28. Stavovi o važnosti personaliziranih usluga na internetu (Izvor: istraživanje autora) (N=194)

Rezultati (Tablica 28.) pokazuju da iako se većina sudionika, njih 53% (N=102) ne slaže s tvrdnjom, sudionici KIF-a jedini su u većini (N=10) označili jedan od stupnjeva slaganja s tvrdnjom (8 slaganja i 2 potpuna slaganja), a u usporedbi s drugima, i sudionici s MEF-a označili su više oznaka slaganja (N=8). Sudionici s ostalih fakulteta u velikoj su većini označili jedan od stupnjeva neslaganja, a među njima prednjače sudionici PMF-a (N=14), studenti FOI-a i PFZG-a (N=12), te studenti FSB-a (N=11).

Istraživanje smo zaključili ispitivanjem slaganja sudionika s tvrdnjom „Smatram da je nemoguće zaštititi moju privatnost na internetu“.

Smatram da je nemoguće zaštititi moju privatnost na internetu					
	Nimalo se ne slažem	**Ne slažem se**	**Niti se slažem niti ne slažem**	**Slažem se**	**Potpuno se slažem**
FSB	1	1	4	4	9
FER	1	4	7	7	1
FOI	0	1	3	10	6
PMF	1	0	4	9	6
FFZG	0	3	3	9	5
EFZG	0	1	5	9	5
PFZG	1	3	3	8	5
MEF	1	4	4	3	4
UFZG	2	2	9	3	4
KIF	0	3	6	5	5
N	**7**	**22**	**48**	**67**	**50**
%	**4%**	**11%**	**25%**	**34%**	**26%**
Zbroj i postotak slaganja/neslaganja	**29 (15%)**		**48 (25%)**	**117 (60%)**	

Tablica 29. Stavovi sudionika o tome je li moguće zaštiti privatnost na internetu (Izvor: istraživanje autora) (N=194)

Rezultati (Tablica 29.) pokazuju da se najviše sudionika slaže s tvrdnjom da je nemoguće zaštititi privatnost na internetu, njih 60% (N=117), a najviše slaganja pronalazimo kod sudionika s FOI-a (N=16), sudionika s PMF-a (N=15) te FFZG-a i EFZG-a (N=14). Sudionici sa svih ostalih fakulteta koji su izrazili neslaganje s tvrdnjom su u manjini. No, iako i dalje malen, najveći broj neslaganja s tvrdnjom pronalazimo kod sudionika s FER-a i MEF-a (N=5), dok kod sudionika svih ostalih fakulteta ne pronalazimo zamjetne razlike u broju neslaganja.

4.5.3. Znanje i zabrinutost za zaštitu osobnih podataka s obzirom na ostale parametre

Nakon bilježenja dobivenih rezultata uzeli smo rezultate sudionika s onih fakulteta koji su pokazali najveće znanje, svijest i zabrinutost po pitanju internetskih politika privatnosti, načina zaštite privatnosti i osobnih podataka, i usporedili smo odgovore studenata preddiplomskih studija s odgovorima studenata diplomskih studija kako bismo zaključili utječe li razina studija na navedene parametre.

Dakle, u ovome ćemo dijelu rezultata usporediti odgovore onih sudionika koji su pokazali znanja, veća ili manja, ali svejedno i isključivo znanja, pri čemu isključujemo odgovore onih studenata koji su u prošlom dijelu rezultata pokazali nisku ili vrlo nisku razinu znanja, kako bi razlikovali koje kategorije studenata imaju veća znanja, a koja manja, a da se svejedno mogu smatrati znanjima. Studenti čije smo razine studija usporedili pripadaju sljedećim fakultetima: FOI, FER, FSB, FFZG i PFZG. Kod istih studenata ispitali smo i utječe

li akademski uspjeh te dnevna učestalost korištenja interneta na znanje i zabrinutost u vezi osobnih podataka na internetu.

S obzirom na razinu studija, akademski uspjeh i dnevno korištenje interneta, prvo smo usporedili samoprocjene sudionika u vezi razumijevanja internetskih politika privatnosti i njihova utjecaja na privatnost.

		Nimalo se ne slažem	Ne slažem se	Niti se slažem niti ne slažem	Slažem se	Potpuno se slažem	*N*	*% slaganja*
Razumijem što su internetske politike privatnosti i kako one utječu na privatnost mojih osobnih podataka.	**PREDD.**	2 (3%)	4 (6%)	19 (28%)	27 (40%)	15 (22%)	67	**62%**
	DIPL.	0	2 (7%)	6 (20%)	12 (40%)	10 (33%)	30	**73%**
	Odličan (5)	0	0	1	5	0	6	*83%*
	Vrlo dobar (4)	2 (6%)	1 (3%)	14 (41%)	11 (32%)	6 (18%)	34	**50%**
	Dobar (3)	0	5 (9%)	12 (22%)	19 (34%)	19 (34%)	55	**68%**
	Dovoljan (2)	0	0	0	2	1	3	*100%*
	Od 1h do 3h	0	0	4	4	1	9	**56%**
	Od 3h do 5h	0	1(3%)	9 (28%)	14 (44%)	8 (25%)	32	**69%**
	Od 5h do 7h	2 (7%)	3(10%)	9 (31%)	10 (34%)	5 (17%)	29	**51%**
	Više od 7h	0	1 (4%)	4 (16%)	10 (40%)	10 (40%)	25	**80%**

Tablica 30. Razumijevanje internetskih politika privatnosti s obzirom na razinu studija, akademski uspjeh i dnevno korištenje interneta (Izvor: istraživanje autora) (N=98)

Rezultati iz Tablice 30. pokazuju da što se razumijevanja internetskih politika privatnosti i njihova utjecaja na privatnost podataka tiče sudionici s diplomskog studija za sebe smatraju da imaju veće razumijevanje (73% slaganja s tvrdnjom) u usporedbi s procjenama sudionika s preddiplomskog studija (62% slaganja s tvrdnjom). S obzirom na akademski uspjeh, sudionici s najčešće dobivenom ocjenom dobar (68% slaganja s tvrdnjom) za sebe smatraju kako imaju veće razumijevanje u odnosu na procjene sudionika s najčešće dobivenom ocjenom vrlo dobar koji su pokazali manji postotak slaganja s tvrdnjom (50% slaganja s tvrdnjom). U uzorku se nalazi devetero sudionika kojima je najčešće dobivena ocjena tijekom studija odličan te se oni također u većini slažu s tvrdnjom (83% slaganja). U uzorku se nalazi i troje sudionika kojima je najčešće dobivena ocjena tijekom studija dovoljan te su svih troje označili slaganje s tvrdnjom.

Također, ista tablica pokazuje kako se sudionici koji provode više od 7 sati dnevno na internetu većinom i najviše slažu s tvrdnjom (80% slaganja), slijede ih sudionici koji dnevno

provode 3 do 5 sati na internetu s 69% slaganja, dok se 51% sudionika koji provode od 5 do 7 sati na internetu slaže s tvrdnjom.

Zatim smo usporedili samoprocjene sudionika po pitanju upoznatosti s pravnim aspektima zaštite osobnih podataka i strategijama prikupljanja podataka s obzirom na navedene parametre.

		Nimalo se ne slažem	Ne slažem se	Niti se slažem niti ne slažem	Slažem se	Potpuno se slažem	*% slaganja*
Upoznat/a sam sa zakonima i pravnim aspektima zaštite osobnih podataka.	**PREDD.**	7 (11%)	10 (15%)	11 (17%)	28 (42%)	10 (15%)	**57%**
	DIPL.	0	7 (24%)	10 (34%)	6 (21%)	6 (21%)	**42%**
	Odličan (5)	0	1	3	1	1	*33%*
	Vrlo dobar (4)	5 (15%)	7 (21%)	6 (18%)	12 (35%)	4 (12%)	**47%**
	Dobar (3)	3 (5%)	11 (20%)	10 (18%)	20 (36%)	12 (21%)	**57%**
	Dovoljan (2)	0	0	2	1	0	*33%*
	Od 1h do 3h	2	3	1	2	1	**33%**
	Od 3h do 5h	0	4 (13%)	8 (27%)	13 (43%)	5 (17%)	**60%**
	Od 5h do 7h	4 (13%)	8 (27%)	2 (7%)	9 (30%)	7 (23%)	**53%**
	Više od 7h	0	4 (15%)	8 (31%)	10 (38%)	4 (15%)	**53%**
Upućen/a sam u strategije koje vlasti i internetske tvrtke koriste za nadzor, prikupljanje, obradu i brisanje osobnih podataka.	**PREDD.**	3 (4%)	10 (15%)	14 (21%)	25 (37%)	16 (23%)	**60%**
	DIPL.	2 (7%)	3 (10%)	2 (7%)	13 (43%)	10 (33%)	**76%**
	Odličan (5)	1	1	0	2	2	*67%*
	Vrlo dobar (4)	3 (10%)	7 (23%)	5 (16%)	11 (35%)	5 (16%)	**51%**
	Dobar (3)	1 (2%)	6 (10%)	10 (17%)	22 (38%)	19 (33%)	**71%**
	Dovoljan (2)	0	0	0	2	1	100%
	Od 1h do 3h	0	3	1	4	1	**56%**
	Od 3h do 5h	3 (10%)	3 (10%)	6 (20%)	11 (37%)	7 (23%)	**60%**
	Od 5h do 7h	1 (3%)	5 (16%)	6 (19%)	10 (32%)	9 (29%)	**61%**
	Više od 7h	1 (4%)	4 (15%)	1 (4%)	12 (44%)	9 (33%)	**77%**

Tablica 31. Upoznatost s pravnim aspektima zaštite podataka i strategijama prikupljanja podataka s obzirom na razinu studija, akademski uspjeh i dnevno korištenje interneta (Izvor: istraživanje autora) (N=98)

Rezultati (Tablica 31.) pokazuju nam kako je 57% sudionika s preddiplomskog studija procijenilo kako se većinom slaže da su upoznati s pravnim aspektima zaštite osobnih podataka u odnosu na 42% sudionika s diplomskog studija. Ista tablica pokazuje nam kako su sudionici većinski dobroga uspjeha procijenili da se većinom slažu s tvrdnjom (57% slaganja) u odnosu

na sudionike većinski vrlo dobrog uspjeha. Također, 33% sudionika s većinski odličnim uspjehom i 33% sudionika s većinski dovoljnim uspjehom procijenilo je slaganje s tvrdnjom. S tvrdnjom upoznatosti s pravnim aspektima zaštite podataka procijenilo je kako se većinom slažu sudionici koji dnevno provode između 3 i 5 sati na internetu (60% slaganja) u odnosu na sudionike koji dnevno provode od 1 do 3 sati na internetu (33% slaganja) i one koji provode od 5 do 7 sati (53% slaganja) te one koji provode više od 7 sati dnevno u jednakom su postotku izrazili slaganje (53% slaganja).

Rezultati (Tablica 31.) pokazuju nam kako je 76% sudionika s diplomskog studija većinom procijenilo kako se slaže da su upućeni u strategije prikupljanja podataka u odnosu na 60% sudionika s preddiplomskog studija. Većinom su procijenili slaganje i sudionici većinski dobroga uspjeha (71% slaganja) u odnosu na one vrlo dobrog uspjeha (51% slaganja s tvrdnjom), dok se s tvrdnjom slaže 67% sudionika s većinski odličnim i svih troje s dovoljnim uspjehom. Većinom su procijenili slaganje s tvrdnjom i sudionici koji internet koriste više od 7 sati dnevno (77% slaganja), dok oni koji koriste internet od 3 do 5 sati pokazuju 60% slaganja, a oni koji koriste internet od 5 do 7 sati 61% slaganja s tvrdnjom. Također, 56% sudionika koji internet koriste od 1 do 3 sata procijenilo je slaganje s tvrdnjom.

Zatim smo usporedili upoznatost sudionika sa strategijama kontrole vlastite privatnosti na internetu s obzirom na navedene parametre.

.

		Nimalo se ne slažem	Ne slažem se	Niti se slažem niti ne slažem	Slažem se	Potpuno se slažem	*% slaganja*
Upoznat/a sam sa strategijama kontrole moje privatnosti na internetu	**PREDD.**	3 (4%)	7 (10%)	15 (22%)	28 (41%)	16 (23%)	**64%**
	DIPL.	0	1 (3%)	4 (13%)	11 (37%)	14 (47%)	**84%**
	Odličan (5)	0	0	1	4	1	*83%*
	Vrlo dobar (4)	2 (6%)	2 (6%)	12 (39%)	7 (23%)	8 (26%)	**49%**
	Dobar (3)	1 (2%)	6 (10%)	6 (10%)	27 (45%)	20 (33%)	**78%**
	Dovoljan (2)	0	0	0	2	1	*100%*
	Manje od 1h	0	0	0	0	1	**100%**
	Od 1h do 3h	0	3 (30%)	3 (30%)	4 (40%)	0	**40%**
	Od 3h do 5h	0	1 (3%)	10 (31%)	14 (44%)	7 (22%)	**66%**
	Od 5h do 7h	2 (7%)	4 (13%)	5 (17%)	12 (40%)	7 (23%)	**63%**
	Više od 7h	1 (4%)	0	2 (8%)	9 (35%)	14 (54%)	**89%**

Tablica 32. Upoznatosti sa strategijama kontrole privatnosti s obzirom na razinu studija, akademski uspjeh i dnevno korištenje interneta (Izvor: istraživanje autora) (N=98)

Rezultati Tablice 32. pokazuju nam kako je 84% sudionika s diplomskog studija većinom procijenilo kako se slaže da su upućeni u strategije kontrole vlastite privatnosti u odnosu na 64% sudionika s preddiplomskog studija. Većinom su procijenili slaganje i sudionici većinski dobroga uspjeha (78% slaganja) u odnosu na one vrlo dobrog uspjeha (49% slaganja s tvrdnjom), dok s tvrdnjom slaže 83% sudionika s većinski odličnim i svih troje s dovoljnim uspjehom. Većinom su procijenili slaganje s tvrdnjom i sudionici koji internet koriste više od 7 sati dnevno (89% slaganja), dok oni koji koriste internet od 3 do 5 sati pokazuju 66% slaganja, a oni koji koriste internet od 5 do 7 sati 63% slaganja s tvrdnjom. Također, 40% sudionika koji internet koriste od 1 do 3 sata procijenilo je slaganje s tvrdnjom.

Zatim smo izračunali prosječan postotak slaganja s prethodnim četirima tvrdnjama kako bi zaključili koje kategorije sudionici samoprocjenjuju najveće znanje po pitanju internetskih politika privatnosti i zaštite osobnih podataka.

	Razumijem što su internetske politike privatnosti i kako one utječu na privatnost mojih osobnih podataka.	Upoznat/a sam sa zakonima i pravnim aspektima zaštite osobnih podataka.	Upućen/a sam u strategije koje vlasti i internetske tvrtke kao što su društveni mediji, pružatelji internetskog bankarstva itd. koriste za nadzor, prikupljanje, obradu i brisanje osobnih podatake.	Upoznat/a sam sa strategijama kontrole moje privatnosti na internetu kao što su redovito brisanje „kolačića“, korištenje firewall-a i sl.	Prosječan postotak slaganja s tvrdnjama (%)
PREDD.	42 (62%)	38 (57%)	41 (60%)	44 (64%)	**60.75%**
DIPL.	22 (73%)	12 (42%)	23 (76%)	25 (84%)	**68.75%**

Tablica 33. Slaganja s tvrdnjama kojima sudionici procjenjuju svoja znanja po pitanjima internetskih politika privatnosti i zaštite osobnih podataka s obzirom na razinu studija (Izvor: istraživanje autora) (N=98)

	Razumijem što su internetske politike privatnosti i kako one utječu na privatnost mojih osobnih podataka.	Upoznat/a sam sa zakonima i pravnim aspektima zaštite osobnih podataka.	Upućen/a sam u strategije koje vlasti i internetske tvrtke kao što su društveni mediji, pružatelji internetskog bankarstva itd. koriste za nadzor, prikupljanje, obradu i brisanje osobnih podatake.	Upoznat/a sam sa strategijama kontrole moje privatnosti na internetu kao što su redovito brisanje „kolačića“, korištenje firewall-a i sl.	Prosječan postotak slaganja s tvrdnjama (%)
vrlo dobar (4)	17 (50%)	16 (47%)	16 (51%)	15 (49%)	**49.25%**
dobar (3)	38 (68%)	32 (57%)	41 (71%)	47 (78%)	**68.50%**

Tablica 34. Slaganja s tvrdnjama kojima sudionici procjenjuju svoja znanja po pitanjima internetskih politika privatnosti i zaštite osobnih podataka s obzirom na prosječnu ocjenu (Izvor:istraživanje autora) (N=98)

Rezultati (Tablica 33.) pokazuju da su kroz prosječno veći postotak slaganja s prethodne četiri tvrdnje veće znanje o internetskim politikama privatnosti i zaštiti osobnih podataka pokazali sudionici diplomske razine studija (68.75%) od sudionika preddiplomske razine (60.75%).

Rezultati (Tablica 34.) pokazuju da su kroz prosječno veći postotak slaganja s prethodne četiri tvrdnje veće znanje o internetskim politikama privatnosti i zaštiti osobnih podataka pokazali sudionici većinski dobrog uspjeha (68.50%) od sudionika većinski vrlo dobrog uspjeha (49.25%).

Zatim smo usporedili znanja o „kolačićima“ na internetu među sudionicima s obzirom na navedene parametre.

Znate li značenje „kolačića“ na internetskim stranicama?			
	Da	**Ne**	**Nisam siguran/na**
PREDD.	46 (67%)	8 (11%)	15 (22%)
DIPL.	26 (87%)	0	4 (13%)
Odličan (5)	5 (83%)	0	1
Vrlo dobar (4)	20 (59%)	4 (12%)	10 (29%)
Dobar (3)	45 (80%)	3 (5%)	8 (14%)
Dovoljan (2)	2 (67%)	1	0
Manje od 1h	1	0	0
Od 1h do 3h	7 (78%)	1 (11%)	1 (11%)
Od 3h do 5h	22 (69%)	3 (9%)	7 (22%)
Od 5h do 7h	20 (65%)	4 (12%)	7 (23%)
Više od 7h	22 (85%)	0	4 (15%)

Znate li postaviti internetski pretraživač tako da ne prima „kolačiće“ bez prethodnog upita?			
	Da	**Ne**	**Nisam siguran/na**
PREDD.	38 (53%)	27 (37%)	7 (10%)
DIPL.	22 (76%)	4 (14%)	3 (10%)
Odličan (5)	4 (67%)	0	2
Vrlo dobar (4)	18 (50%)	16 (44%)	2 (6%)
Dobar (3)	36 (64%)	14 (25%)	6 (11%)
Dovoljan (2)	2 (67%)	1	0
Manje od 1h	1	0	0
Od 1h do 3h	6 (67%)	2 (22%)	1 (11%)
Od 3h do 5h	14 (44%)	14 (44%)	4 (12%)
Od 5h do 7h	17 (55%)	12 (39%)	2 (6%)
Više od 7h	22 (79%)	3 (11%)	3 (11%)

Tablica 35. Znanja u vezi internetskih „kolačića“ s obzirom na razinu studija, akademski uspjeh i dnevno korištenje interneta (Izvor: istraživanje autora) (N=98)

Rezultati iz Tablice 35. pokazuju nam da je 87% sudionika s diplomskoga studija većinom upoznato s internetskim „kolačića“ u odnosu na 67% sudionika s preddiplomskog studija. Sudionici najčešće dobroga uspjeha većinom pokazuju bolju upoznatost s „kolačićima (80% potvrdnih odgovora) u odnosu na one vrlo dobroga (59% potvrdnih odgovora) i dovoljnoga uspjeha (67% potvrdnih odgovora), dok su studenti odličnoga (83% potvrdnih odgovora) također uglavnom upoznati s njima. Nadalje, iz rezultata iz Tablice 35. iščitavamo da sudionici koji koriste internet više od 7 sati dnevno (85% potvrdnih odgovora) većinom pokazuju veću upoznatost s „kolačićima“ u odnosu na one koji ga koriste od 3 do 5 sati (69% potvrdnih odgovora) i od 5 do 7 sati (65% potvrdnih odgovora).

Rezultati iz desnoga dijela iste tablice pokazuju da su sudionici s diplomskog studija većinom (76% potvrdnih odgovora) upoznatiji s postavljanjem internetskog pretraživača tako da ne prima „kolačiće“ bez prethodnog upita u odnosu na sudionike s preddiplomskog studija (53% potvrdnih odgovora). Isto se može reći i za sudionike dobroga uspjeha (64% potvrdnih odgovora) u odnosu na one vrlo dobroga (50% potvrdnih odgovora) te za sudionike koji dnevno provode više od 7 sati na intrenetu (79% potvrdnih odgovora) u odnosu na one koji dnevno koriste internet od 3 do 5 sati (44% potvrdnih odgovora) i one koji ga koriste od 5 do 7 sati (55% potvrdnih odgovora), no u visokom su postotku potvrdno odgovorili i oni koji ga koriste od 1 do 3 sata dnevno (67%). Također, 67% sudionika odličnog uspjeha i 67% sudionika dovoljnog uspjeha odgovorilo je potvrdno na pitanje.

Usporedili smo i odgovore sudionika na pitanje što čine kad su suočeni s uvjetima i odredbama s obzirom s obzirom na razinu studija, akademski uspjeh i dnevno korištenje interneta.

Prilikom preuzimanja aplikacije na mobilni uređaj ili instaliranja aplikacije na računalo, kao korisnik morate prihvatiti uvjete i odredbe. Što uglavnom činite u toj situaciji?			
	Pristajem na uvjete i odredbe bez čitanja istih	*Brzo prođem kroz tekst, pa onda pristanem*	*Pročitam čitavi tekst, pa onda pristanm*
PREDD.	46 (67%)	21 (30%)	2 (3%)
DIPL.	16 (55%)	9 (31%)	4 (14%)
Odličan (5)	4 (67%)	2	0
Vrlo dobar (4)	20 (65%)	10 (32%)	1 (3%)
Dobar (3)	36 (63%)	18 (32%)	3 (5%)
Dovoljan (2)	2 (67%)	1	0
Manje od 1h	0	1	0
Od 1h do 3h	7 (78%)	1 (11%)	1 (11%)
Od 3h do 5h	22 (67%)	10 (30%)	1(3%)
Od 5h do 7h	20 (67%)	9 (30%)	1 (3%)
Više od 7h	,13 (50%)	10 (38%)	3 (12%)

Tablica 36. Ponašanja kada su suočeni s uvjetima i odredbama (Izvor: istraživanje autora) (N=98)

Rezultati iz Tablice 36. pokazuju da sudionici s diplomskoga većinom barem brzo prođu (31%) ili u potpunosti pročitaju (14%) tekst uvjeta i odredbi pri instalaciji aplikacija u odnosu na sudionike s preddiplomskog studija. U podjednakom postotku to čine sudionici svih akademskih uspjeha. S obzirom na dnevnu učestalost korištenja interneta, sudionici koji koriste internet dulje od 7 sati dnevno većinom više čitaju uvjete i odredbe, njih 38% brzo prođe kroz tekst, dok njih 12% pročita čitavi tekst, u odnosu na sudionike koji internet koriste internet od 3 do 5 sati, kojih 30% sudionika brzo prođe kroz tekst, a 3% pročita čitav tekst. Isti postotak sudionika koji internet koriste od 5 do 7 satu dnevno brzo prođe kroz tekst, odnosno pročita čitavi tekst, kao i kod sudionika koji internet koriste od 3 do 5 sati dnevno.

Upoznatost sudionika s pravima omogućenim Općom uredbom o zaštiti podataka s obzirom na navedene parametre usporedili smo tako da smo izračunali prosjek broja prava s kojima upoznati po sudioniku za svaku kategoriju sudionika.

		Prosjek (po sudioniku) broja prava s kojima su upoznati
Za koja ste od navedenih prava koja Vam osigurava GDPR regulativa čuli, odnosno s kojima ste od sljedećih prava upoznati?	**PREDD.**	2.15
	DIPL.	3.42
	Odličan (5)	3.17
	Vrlo dobar (4)	2.09
	Dobar (3)	2.77
	Dovoljan (2)	*1.00 (malen broj sudionika)*
	Manje od 1h	*4.00 (malen broj sudionika)*
	Od 1h do 3h	3.11
	Od 3h do 5h	2.63
	Od 5h do 7h	2.03
	Više od 7h	3.03

Tablica 37. Prosjek broja prava s kojima su upoznati (Izvor: istraživanje autora) (N=98)

Rezulati iz Tablice 37. pokazuju da su u prosjeku većinom s većim brojem prava upoznati sudionici s diplomskoga studija (3.42 prava po sudioniku) u odnosu na sudionik s preddiplomskog (2.15 prava po sudionik). Isto se može reći i za sudionike dobroga uspjeha (2.77 prava po sudioniku) i odličnoga (3.17 prava po sudioniku) u odnosu na sudionike vrlo dobroga uspjeha (2.09 prava po sudioniku) i dovoljnoga uspjeha (1.00 prava po sudioniku). Također većinom su s većim brojem prava upoznati sudionici koji provode više od 7 sati dnevno na intrenetu (3.03 prava po sudioniku) u odnosu na one koji ga koriste manje, a velik prosjek imaju i oni koji ga koriste od 1 do 3 sata (3.11 prava po sudioniku), no broj sudionika iz te kategorije je malen.

Usporedbom odgovora na sljedeće tvrdnje pokušali smo utvrditi koje kategorije sudionika pokazuju veću zabrinutost za svoje osobne podatkena internetu te koje kategorije imaju veće povjerenje u internetske stranice po pitanju zaštite podataka.

(1) – nimalo se ne slažem, (2) – ne slažem se, (3) – niti se slažem niti ne slažem,

(4) – slažem se, (5) – u potpunosti se slažem, (%) – postotak slaganja

		(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(%)*
Vjerujem da su moji osobni podatci sigurni na internetskim stranicama.	**PREDD.**	7 (10%)	21 (31%)	30 (44%)	10 (15%)	0	**15%**
	DIPL.	7 (25%)	8 (28%)	10 (36%)	3 (11%)	0	**11%**
	Odličan (5)	1	1	4	0	0	**0%**
	Vrlo dobar (4)	6 (19%)	8 (26%)	13 (42%)	4 (13%)	0	**13%**
	Dobar (3)	7 (12%)	19 (33%)	22 (39%)	9 (16%)	0	**16%**
	Dovoljan (2)	1	0	2	0	0	**0%**
	Manje od 1h	0	1	0	0	0	**0%**
	Od 1h do 3h	0	2 (22%)	6 (67%)	1 (11%)	0	**11%**
	Od 3h do 5h	6 (19%)	8 (26%)	14 (45%)	3 (10%))	0	**10%**
	Od 5h do 7h	4 (13%)	10 (32%)	11 (35%)	6 (19%)	0	**19%**
	Više od 7h	5 (20%)	7 (28%)	10 (40%)	3 (12%)	0	**12%**

		(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(%)*
Zabrinut/a sam zbog ugroženosti svojih osobnih podataka na internetu.	**PREDD.**	13 (19%)	13 (19%)	14 (20%)	20 (29%)	9 (13%)	**42%**
	DIPL.	2 (7%)	6 (21%)	8 (28%)	8 (28%)	5 (17%)	**45%**
	Odličan (5)	0	2	2	2	0	**33%**
	Vrlo dobar (4)	3 (10%)	5 (16%)	9 (29%)	9 (29%)	5 (16%)	**45%**
	Dobar (3)	11 (19%)	11 (19%)	11 (19%)	16 (28%)	9 (15%)	**43%**
	Dovoljan (2)	1	1	1	1	0	**25%**
	Manje od 1h	0	0	1	0	0	**0%**
	Od 1h do 3h	1 (12,5%)	2 (25%)	2 (25%)	2 (25%)	1 (12,5%)	**37.5%**
	Od 3h do 5h	4 (13%)	7 (23%)	9 (29%)	9 (29%)	2 (6%)	**35%**
	Od 5h do 7h	6 (20%)	4 (13%)	5 (17%)	9 (30%)	6 (20%)	**50%**
	Više od 7h	4 (15%)	5 (19%)	5 (19%)	7 (28%)	5 (19%)	**47%**

Tablica 38. Povjerenje i zabrinutost sudionika po pitanju podataka s obzirom na razinu studija, akademski uspjeh i dnevno korištenje interneta (Izvor: istraživanje autora) (N=98)

Rezultati iz Tablice 38. pokazuju da se sudionici s diplomskoga studija većinom (11%) manje slažu s tvrdnjom vjerovanja da su njihovi osobni podaci sigurni na intrenetskim stranicama u odnosu na sudionike s preddiplomskog studija (15%). Sudionici dobroga uspjeha također se većinom (16%) manje slažu s istom tvrdnjom u odnosu na sudionike vrlo dobroga uspjeha (13%), dok se sudionici odličnoga i dovoljnoga uspjeha uglavnom niti slažu niti ne slažu s tvrdnjom te se 0% tih sudionika slaže s tvrdnjom. Što se dnevne učestalosti korištenja tiče, rezultati iz iste tablice pokazuju da se većinom (10%) najmanje s tvrdnjom slažu sudionici koji internet dnevno koriste od 3 do 5 sati, slijede sudionici koji internet koriste od 1 do 3 sata (11%), pa sudionici koji koriste internet više od 7 sati dnevno (12%). Sudionici koji internet koriste od 5 do 7 sati izrazili su 19% slaganja s tvrdnjom.

Rezultati (Tablica 38.) pokazuju i da se sudionici s diplomskog studija više slažu (45%) s tvrdnjom zabrinutosti po pitanju osobnih podataka na interneta u odnosu na sudionike s preddiplomskog (42%). Gotovo jednak postotak slaganja s tvrdnjom zabrinutosti za svoje osobne podatke pokazuju sudionici vrlo dobroga uspjeha (45%) i sudionici dobroga uspjeha (43%), dok se 33% sudionika odličnog uspjeha i 25% sudionika dovoljnog uspjeha slaže s tvrdnjom. Što se dnevne učestalosti korištenja tiče, ista tablica pokazuja da se više s tvrdnjom

zabrinutosti slažu sudionici koji provode od 5 do 7 sati dnevno na internetu (50%) u odnosu na sudionike koji ga koriste od 1 do 3 sata (37.5%), od 3 do 5 sati (35%) i više od 7 sati dnevno (47%).

Iste smo usporedbe napravili i na temelju odgovora na tvrdnje „Smatram da će internetske tvrtke čuvati povjerljivim ono što o meni saznaju iz mojih aktivnosti na njihovoj internetskoj stranici“ i „Smatram kako nije dobro to što trgovci na internetu mogu saznati osobne podatke o internetskim kupcima bez njihovog pristanka“.

(1) – nimalo se ne slažem, (2) – ne slažem se, (3) – niti se slažem niti ne slažem,
(4) – slažem se, (5) – u potpunosti se slažem, (%) – postotak slaganja

		(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(%)*
Smatram da će internetske tvrtke čuvati povjerljivim ono što o meni saznaju iz mojih aktivnosti na njihovoj internetskoj stranici	**PREDD.**	8 (12%)	23 (34%)	24 (35%)	12 (18%)	1 (1%)	**19%**
	DIPL.	10 (34%)	7 (24%)	4 (14%)	8 (28%)	0	**28%**
	Odličan (5)	1	1	2	2	0	*33%*
	Vrlo dobar (4)	6 (19%)	8 (26%)	12 (39%)	4 (13%)	1 (3%)	**16%**
	Dobar (3)	10 (17%)	20 (35%)	13 (23%)	14 (25%)	0	**25%**
	Dovoljan (2)	1	1	1	0	0	**0%**
	Manje od 1h	0	1	0	0	0	**0%**
	Od 1h do 3h	0	3 (33%)	6 (66%)	0	0	**0%**
	Od 3h do 5h	7 (24%)	7 (24%)	9 (31%)	6 (21%)	0	**21%**
	Od 5h do 7h	3 (10%)	10 (32%)	8 (26%)	9 (29%)	1 (3%)	**32%**
	Više od 7h	8 (32%)	9 (36%)	3 (12%)	5 (20%)	0	**20%**

		(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(%)*
Smatram kako nije dobro to što trgovci na internetu mogu saznati osobne podatke o internetskim kupcima bez njihovog pristanka	**PREDD.**	2 (3%)	2 (3%)	12 (18%)	14 (21%)	38 (56%)	**77%**
	DIPL.	0	2 (7%)	4 (13%)	6 (20%)	18 (60%)	**80%**
	Odličan (5)	0	0	1	0	5	*83%*
	Vrlo dobar (4)	1 (3%)	1 (3%)	3 (10%)	9 (29%)	17 (55%)	**84%**
	Dobar (3)	1 (2%)	3 (5%)	12 (21%)	10 (17%)	32 (55%)	**72%**
	Dovoljan (2)	0	0	0	2	1	*100%*
	Manje od 1h	0	0	0	0	1	/
	Od 1h do 3h	1 (11%)	0	2 (22%)	2 (22%)	4 (44%)	**66%**
	Od 3h do 5h	0	1 (3%)	6 (19%)	7 (22%)	18 (56%)	**78%**
	Od 5h do 7h	0	2 (6%)	5 (16%)	6 (19%)	18 (58%)	**77%**
	Više od 7h	1 (4%)	1 (4%)	4 (15%)	5 (19%)	15 (58%)	**77%**

Tablica 39. Povjerenje i zabrinutost sudionika po pitanju podataka s obzirom na razinu studija, akademski uspjeh i dnevno korištenje interneta (Izvor: istraživanje autora) (N=98)

Rezultati iz Tablice 39. pokazuju da se tvrdnjom „Smatram da će internetske tvrtke čuvati povjerljivim ono što o meni saznaju iz mojih aktivnosti na njihovoj internetskoj stranici“ većinom više slažu (28%) sudionici s diplomskoga studija u odnosu na sudionike s preddiplomskog (19%). Većinom se više s tom tvrdnjom slažu i sudionici dobroga uspjeha (25%) u odnosu na sudionike vrlo dobrog uspjeha, dok se 33% sudionika odličnog uspjeha slaže s tom tvrdnjom te 0% sudionika dovoljnog uspjeha. Većinom se najviše slaž (32%) u s tom tvrdnjom i sudionici koji internet koriste od 5 do 7 sati dnevno.

Ista tablica pokazuje i da se većinom s tvrdnjom „Smatram kako nije dobro to što trgovci na internetu mogu saznati osobne podatke o internetskim kupcima bez njihovog pristanka“ više slažu sudionici s diplomskog studija (80%) u odnosu na sudionike s preddiplomskog (77%). Isto vrijedi i za sudionike vrlo dobroga uspjeha (84%) u odnosu na sudionike dobroga (72%) i odličnog (83%) uspjeha, dok su svih troje sudionika dovoljnog uspjeha također izrazila slaganje s tvrdnjom. Što se dnevne učestalosti korištenja interneta tiče, sve su kategorije sudionika u sličnim postotcima izrazila slaganje s tvrdnjom, međutim sudionici koji dnevno internet koriste internet od 3 do 5 sati (78%) izrazili su više slaganja od ostalih.

Ponovili smo postupak uspoređivanja i na temelju odgovora na tvrdnje „Smeta me kada internetske tvrtke traže moje osobne podatke“ i „Kada me internetske tvrtke pitaju za osobne podatke, dobro razmislim prije nego što ih dam“.

(1) – nimalo se ne slažem, (2) – ne slažem se, (3) – niti se slažem niti ne slažem,
(4) – slažem se, (5) – u potpunosti se slažem, (%) – postotak slaganja

		(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(%)*
Smeta me kada internetske tvrtke traže moje osobne podatke	**PREDD.**	1 (1%)	4 (6%)	16 (22%)	25 (35%)	26 (36%)	**71%**
	DIPL.	0	3 (10%)	5 (17%)	8 (28%)	13 (45%)	**73%**
	Odličan (5)	0	1 (17%)	1 (17%)	2 (33%)	2 (33%)	*66%*
	Vrlo dobar (4)	0	2 (6%)	4 (12%)	14 (44%)	12 (38%)	**82%**
	Dobar (3)	0	4 (7%)	15 (26%)	17 (29%)	22 (38%)	**67%**
	Dovoljan (2)	1	0	0	0	2	**67%**
	Manje od 1h	0	0	0	0	1	/
	Od 1h do 3h	0	1 (11%)	3 (33%)	3 (33%)	2 (22%)	**55%**
	Od 3h do 5h	1 (3%)	3 (9%)	9 (28%)	10 (31%)	9 (28%)	**59%**
	Od 5h do 7h	0	0	5 (16%)	14 (45%)	12 (39%)	**84%**
	Više od 7h	0	3 (12%)	3 (12%)	6 (22%)	14 (54%)	**76%**

		(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(%)*
Kada me internetske tvrtke pitaju za osobne podatke, dobro razmislim prije nego što ih dam	**PREDD.**	0	11 (16%)	12 (17%)	16 (23%)	30 (44%)	**67%**
	DIPL.	0	2 (7%)	4 (14%)	8 (28%)	15 (52%)	**80%**
	Odličan (5)	0	1 (17%)	2 (33%)	0	3 (50%)	*50%*
	Vrlo dobar (4)	0	5 (15%)	5 (15%)	9 (26%)	15 (47%)	**73%**
	Dobar (3)	0	7 (13%)	10 (18%)	13 (23%)	26 (46%)	**69%**
	Dovoljan (2)	0	0	0	2	1	*100%*
	Manje od 1h	0	0	0	1	0	/
	Od 1h do 3h	0	2 (22%)	1 (11%)	2 (22%)	4 (44%)	**66%**
	Od 3h do 5h	0	2 (6%)	8 (25%)	12 (38%)	10 (31%)	**69%**
	Od 5h do 7h	0	8 (25%)	2 (6%)	5 (16%)	17 (53%)	**69%**
	Više od 7h	0	1 (4%)	6 (24%)	4 (16%)	14 (56%)	**72%**

Tablica 40. Zabrinutost po pitanju podataka s obzirom na razinu studija, akademski uspjeh i dnevno korištenje interneta (Izvor: istraživanje autora) (N=98)

Rezultati iz Tablice 38. pokazuju da većinom sudionike diplomskoga studija (73%) više smeta kada ih internetske tvrtke traže njihove osobne podatke u odnosu na sudionike preddiplomskog

studija (71%). Ista je situacija i kod sudionika vrlo dobroga uspjeha (82%) u odnosu na studente dobroga uspjeha (67%), a većinom se s tvrdnjom slažu i sudionici odličnoga (66%) i dovoljnoga uspjeha (67%).Većinom se s tom tvrdnjom više slažu i sudionici koji dnevno provode od 5 do 7 sati na internetu (84%) u odnosu na studente koji na internetu provode više od 7 sati dnevno (76%) i studente koji na internetu provode od 3 do 5 sati (59%) i od 1 do 3 sati (55%).

Rezultati iz desnog dijela iste tablice pokazuju da većinom sudionici diplomskoga studija (80%) dobro razmisle o davanju svojih osobnih podataka na internetu u odnosu na sudionike preddiplomskog studija koji to čine u manjem postotku (67%). Ista je situacija i kod sudionika vrlo dobroga uspjeha (73%) u odnosu na studente dobroga uspjeha (69%), a s tom se tvrdnjom slaže i 50% sudionika odličnog uspjeha i svih troje sudionika dovoljnog uspjeha. Većinom se s tom tvrdnjom više slažu i sudionici koji dnevno provode više od 7 sati na internetu (84%) u odnosu na sudionike koji na internetu provode od 5 do 7 sati dnevno (69%), odnosno sudionike koji na internetu provode od 3 do 5 sati (69%) i od 1 do 3 sati (66%).

Zabrinutost sudionika po pitanju osobnih podataka usporedili smo i na temelju sljedeće dvije tvrdnje.

(1) – nimalo se ne slažem, (2) – ne slažem se, (3) – niti se slažem niti ne slažem, (4) – slažem se, (5) – u potpunosti se slažem, (%) – postotak slaganja

		(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(%)*			*(1)*	*(2)*	*(3)*	*(4)*	*(5)*	*(%)*
Zabrinut/a sam da internetske tvrtke prikupljaju previše osobnih podataka o meni.	**PREDD.**	0	7 (10%)	14 (21%)	25 (37%)	22 (32%)	**69%**	**Smatram problematičnim činjenicu da tvrtke koriste moje internetsku aktivnost za sakupljanje podataka o meni kako bi mi prikazivale odgovarajuće oglase.**	**PREDD.**	4 (6%)	8 (12%)	12 (17%)	18 (26%)	27 (39%)	**65%**
	DIPL.	1 (3%)	5 (17%)	6 (21%)	8 (28%)	9 (31%)	**59%**		**DIPL.**	1 (3%)	5 (17%)	3 (10%)	9 (30%)	12 (40%)	**70%**
	Odličan (5)	0	1 (17%)	2 (33%)	2 (33%)	1 (17%)	*50%*		**Odličan (5)**	0	2	0	0	4	*67%*
	Vrlo dobar (4)	0	8 (25%)	5 (16%)	10 (31%)	9 (28%)	**59%**		**Vrlo dobar (4)**	1 (3%)	1 (3%)	5 (16%)	14 (45%)	10 (32%)	**77%**
	Dobar (3)	1 (2%)	4 (7%)	14 (24%)	21 (36%)	18 (31%)	**67%**		**Dobar (3)**	3 (5%)	9 (16%)	9 (16%)	14 (23%)	23 (40%)	**63%**
	Dovoljan (2)	0	0	0	0	3	*100%*		**Dovoljan (2)**	0	1	0	1	1	*67%*
	Manje od 1h	0	0	1	0	0	/		**Manje od 1h**	0	0	0	0	1	/
	Od 1h do 3h	0	2 (22%)	3 (33%)	1 (11%)	3 (33%)	**44%**		**Od 1h do 3h**	1 (11%)	1 (11%)	2 (22%)	2 (22%)	3 (33%)	**55%**
	Od 3h do 5h	0	5 (16%)	4 (13%)	15 (48%)	7 (23%)	**71%**		**Od 3h do 5h**	2 (6%)	5 (16%)	6 (19%)	6 (19%)	13 (41%)	**60%**
	Od 5h do 7h	0	4 (13%)	8 (26%)	10 (32%)	9 (29%)	**61%**		**Od 5h do 7h**	1 (3%)	1 (3%)	4 (14%)	12 (40%)	12 (40%)	**80%**
	Više od 7h	1 (4%)	2 (8%)	4 (15%)	7 (27%)	12 (46%)	**73%**		**Više od 7h**	1 (4%)	6 (22%)	2 (7%)	9 (33%)	9 (33%)	**66%**

Tablica 41. Zabrinutost po pitanju podataka s obzirom na razinu studija, akademski uspjeh i dnevno korištenje interneta (Izvor: istraživanje autora) (N=98)

Rezultati iz Tablice 41. pokazuju da se s tvrdnjom „Zabrinut/a sam da internetske tvrtke prikupljaju previše osobnih podataka o meni“ većinom više slažu sudionici s preddiplomskog studija (69%) u odosu na sudionike s diplomskog koji se u manjem postotku slažu s tvrdnjom (59%). Također se s tvrdnjom većinom više slažu sudionici dobroga uspjeha (67%) u odnosu na one vrlo dobrog (59%) i odličnog uspjeha (50%), dok se svih troje sudionika dovoljnog uspjeha slažu s tvrdnjom. Većinom se s tvrdnjom više slažu i sudionici koji internet koriste više od 7 sati dnevno (73%) u odnosu na one koji ga koriste od 3 do 5 sati (71%), odnosno 5 do 7 sati (61%), dok se s tvrdnjom slaže 44% sudionika koji internet koriste od 1 do 3 sata.

Rezultati iz iste tablice pokazuju da su ponovno većinom više slaganja s tvrdnjom „Smatram problematičnim činjenicu da tvrtke koriste moje internetsku aktivnost za sakupljanje podataka o meni kako bi mi prikazivale odgovarajuće oglase“ pokazali sudionici s diplomskoga studija (70%) u odnosu na sudionike s preddiplomskog (65%). Također, većinom su više slaganja izrazili sudionici vrlo dobroga uspjeha (77%) u odnosu na sudionika dobroga (63%), dok su studenti odličnoga (67%) i dovoljnoga (67%) također u većini odgovorili sa slaganjem na tvrdnju. S obzirom na dnevnu učestalost korištenja interneta, rezultati iz Tablice 24. pokazuju da se s tom tvrdnjom većinom više slažu sudionici koji ga koriste od 5 do 7 sati dnevno (80%), u odnosu na sudionike koji ga koriste više od 7 sati dnevno (66%), odnosno od 3 do 5 sati dnevno (60%).

Zanimalo nas je i koje se kategorije sudionika najviše slažu s dvjema zaključnim tvrdnjama.

(1) – nimalo se ne slažem, (2) – ne slažem se, (3) – niti se slažem niti ne slažem,
(4) – slažem se, (5) – u potpunosti se slažem, (%) – postotak slaganja

		(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(%)*
Smatram da je nemoguće zaštititi moju privatnost na internetu	**PREDD.**	3 (4%)	8 (12%)	15 (22%)	25 (36%)	18 (26%)	**62%**
	DIPL.	0	5 (18%)	4 (14%)	12 (43%)	7 (25%)	**68%**
	Odličan (5)	0	0	3	1	2	*50%*
	Vrlo dobar (4)	0	3 (9%)	8 (25%)	9 (28%)	12 (38%)	**66%**
	Dobar (3)	3 (5%)	10 (18%)	9 (16%)	26 (46%)	9 (16%)	**62%**
	Dovoljan (2)	0	0	0	1	2	*100%*
	Manje od 1h	0	0	0	0	1	/
	Od 1h do 3h	0	0	2 (22%)	3 (33%)	4 (44%)	**77%**
	Od 3h do 5h	1 (3%)	6 (19%)	10 (32%)	7 (23%)	7 (23%)	**46%**
	Od 5h do 7h	1 (3%)	5 (17%)	6 (20%)	10 (33%)	8 (27%)	**60%**
	Više od 7h	1 (4%)	1 (4%)	2 (8%)	16 (64%)	5 (20%)	**84%**

		(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(%)*
Smatram da prednosti personaliziranih usluga na internetu koje proizlaze iz sakupljanja mojih osobnih podataka nadilaze važnost zaštite osobnih podataka.	**PREDD.**	21 (31%)	17 (25%)	18 (26%)	7 (10%)	5 (7%)	**17%**
	DIPL.	9 (30%)	11 (37%)	7 (23%)	2 (7%)	1 (3%)	**10%**
	Odličan (5)	3 (50%)	0	2 (33%)	1 (17%)	0	*17%*
	Vrlo dobar (4)	12 (39%)	6 (19%)	9 (29%)	2 (6%)	2 (6%)	**12%**
	Dobar (3)	15 (25%)	22 (37%)	13 (22%)	6 (10%)	3 (5%)	**15%**
	Dovoljan (2)	0	0	1	0	1	**50%**
	Manje od 1h	0	0	0	0	1	/
	Od 1h do 3h	2 (22%)	3 (33%)	2 (22%)	1 (11%)	1 (11%)	**22%**
	Od 3h do 5h	9 (28%)	9 (28%)	9 (28%)	2 (6%)	3 (9%)	**15%**
	Od 5h do 7h	13 (42%)	8 (26%)	7 (23%)	2 (6%)	1 (3%)	**9%**
	Više od 7h	6 (24%)	8 (32%)	7 (28%)	4 (16%)	0	**16%**

Tablica 42. Stavovi o mogućnosti očuvanja privatnosti i prednostima personaliziranih usluga na internetu s obzirom na razinu studija, akademski uspjeh i dnevno korištenje interneta (Izvor: istraživanje autora) (N=98)

Rezultati iz Tablice 42. pokazuju da su mišljenja da je nemoguće zaštiti privatnost na internetu većinom više sudionici s diplomskog studija (68%) u odnosu na sudionike s preddiplonskog (62%). Većinom su više toga stava i sudionici vrlo dobroga uspjeha (66%) u odnosu na one dobrog (62%), dok je 50% sudionika odličnog uspjeha označilo slaganje s tom tvrdnjom. Također, većinom su više toga stava i sudionici koji internet koriste više od 7 sati dnevno (84%) u odnosu na one koji ga koriste od 5 do 7 sati (60%), odnosno od 3 do 5 sati (46%). Sudionici koji internet koriste od 1 do 3 sata dnevno također se uglavnom slažu s tvrdnjom (77%).

Rezultati iz Tablice 42. pokazuju da su većinom manje slaganja s tvrdnjom iz desnog dijela tablice izrazili sudionici s diplomskog studija (10%) u odnosu na sudionike s preddiplonskog (17%). Većinom su manje toga mišljenja i sudionici vrlo dobroga uspjeha (12%) u odnosu na one dobrog (15%), dok je 17% sudionika odličnog uspjeha označilo slaganje s tom tvrdnjom. Također, većinom su manje toga stava i sudionici koji internet koriste od 5 do 7 sati dnevno (9%) u odnosu na one koji ga koriste više od 7 sati (16%), odnosno od 3

do 5 sati (15%). Sudionici koji internet koriste od 1 do 3 sata dnevno također su pokazali malo slaganja s tvrdnjom (22%).

4.6. Rasprava

S obzirom na to da je istraživanje provedeno kako bi se testirale postavljene hipoteze, u ovome ćemo potpoglavlju potvrditi ili opovrgnuti hipoteze. Dakle, analizirat ćemo dobivene rezultate koji se odnose na svaku postavljenu hipoteze, nakon čega ćemo zaključiti je li ona potvrđena ili ne.

H1: Studenti Fakulteta elektrotehnike i računarstva, Pravnog fakulteta, Filozofskog fakulteta te Fakulteta organizacije i informatike imaju više znanja o politikama privatnosti i zaštite osobnih podataka te su više zabrinuti zbog ugroženosti osobnih podataka na internetu od studenata ostalih fakulteta Sveučilišta u Zagrebu. Također, više znanja imaju te više zabrinutosti pokazuju studenti na diplomskoj razini studija u odnosu na studente na preddiplomskoj razini studija.

Rezultati istraživanja pokazuju kako studenti FOI-a, FER-a, FSB-a, FFZG-a i PFZG-a imaju najviše znanja o politikama privatnosti i načinima zaštite osobnih podataka. Zaključke o znanjima studenata po pitanjima politika privatnosti i zaštite osobnih podataka izveli smo na temelju odgovora na tvrdnje iz druge kategorije pitanja anketnog upitnika gdje su sudionici morali samoprocijeniti razinu slaganja s tvrdnjama koje ispituju znanja po tim pitanjima. Zaključke o njihovim znanjima izveli smo i na temelju odgovora na pitanja o „kolačićima“ te pitanje o poznavanju prava omogućenih Općom uredbom o zaštiti podataka. Većinom su kroz prosječno najveći postotak slaganja s tvrdnjama iz druge kategorije pitanja anketnog upitnika najveće znanje samoprocijenili studenti FOI-a (81.25%). Slijede ih studenti PFZG-a (71.25%), zatim studenti FER-a (58.75%) pa studenti FSB-a (56.25%) i studenti FFZG-a (45%).

Studenti istih fakulteta pokazuju i najveće znanje po pitanju „kolačića“. Naime, većina je studenata FOI-a (N=18), PFZG-a (N=17), FER-a (N=16) te FSB-a (N=13) upoznata sa značenjem „kolačića“, a po brojnosti studenata koji su upoznati sa značenjem „kolačića“ slijede ih studenti EFZG-a (N=10) i studenti FFZG-a (N=10). Također, za razliku od studenata ostalih fakulteta, većinom studenti FER-a (N=16), FOI-a (N=14), FFZG-a (N=10) te FSB-a (N=10) znaju postaviti internetski pretraživač da ne prima „kolačiće“ bez upita. Uz studente UFZG-a i MEF-a, studenti PFZG-a, FOI-a i FSB-a pokazali su i najveću upoznatost s pravima

omogućenim Općom uredbom o zaštiti podataka. Naime, najviše su oznaka upoznatosti s navedenim pravima označili studenti PFZG-a (91), FOI-a (64) i UFZG-a (46), MEF-a (43) te FSB-a (39).

Pri procjeni znanja sudionika po pitanjima internetskih politika privatnosti uzeli smo u obzir i odgovore na tvrdnju „Smatram da će internetske tvrtke čuvati povjerljivim ono što o meni saznaju iz mojih aktivnosti na njihovoj internetskoj stranici“. S tom su tvrdnjom najmanji postotak slaganja izrazili studenti FER-a (15%), PMF-a (15%) i FFZG-a (15%), a slijede ih studenti FSB-a (21%) i studenti EFZG-a (25%).

Iz svega navedenog proizlazi da na većinu pitanja i tvrdnji koji procjenjuju znanja studenata po pitanjima internetskih politika privatnosti i zaštite osobnih podataka najveća znanja pokazuju studenti FOI-a, FER-a, FSB-a, PFZG i FFZG-a, dok dobro znanje pokazuju i studenti EFZG-a.

Međutim, studenti gotovo svih fakulteta pokazuju zabrinutost za svoje osobne podatke. Ipak, studenti FFZG-a u najvećem su postotku (50%) označili zabrinutost kroz slaganje ili potpuno slaganje s tvrdnjom **„**Zabrinut/a sam zbog ugroženosti svojih osobnih podataka na internetu“, slijede ih studenti FER-a i PFZG-a (45%) te studenti FOI-a i PMF-a (40%).

Također, rezultati istraživanja pokazali su da više znanja o politikama privatnosti i načinima zaštite osobnih podataka i više zabrinutosti za svoje podatke pokazuju studenti diplomske razine studija u odnosu na studente preddiplomske razine studija. Naime, većinom su kroz prosječno veći postotak slaganja s tvrdnjama iz druge kategorije pitanja anketnog upitnika veće znanje samoprocijenili studenti s diplomske razine studija (68.75%) u odnosu na studente s preddiplomske razine studija (60.75%). Osim toga, 87% studenata diplomskog studija upoznato je s prirodom „kolačića“ u odnosu na 67% studenata preddiplomskog studija, dok 76% studenata diplomskog zna postaviti svoj pretraživač tako da ne prima „kolačiće“ u odnosu na 53% studenata preddiplomskog. Studenti diplomskog studija upoznatiji su i s pravima omogućenim Općom uredbom o zaštiti podataka (prosječno 3.42 prava po studentu) od studenata preddiplomskog studija (prosječno 2.15 prava po studentu).

Također, 45% je studenata diplomskog studija izrazilo zabrinutost za svoje osobne podatke u odnosu na 42% studenata preddiplomskog. Usporedili smo i odgovore na tvrdnju „Smatram da će internetske tvrtke čuvati povjerljivim ono što o meni saznaju iz mojih

aktivnosti na njihovoj internetskoj stranici“ te su s tom tvrdnjom manji postotak slaganja izrazili studenti preddiplomskog studija (19%) u odnosu na studente diplomskog studija (28%).

Dakle, naša je prva hipoteza istraživanjem djelomično potvrđena. Naime, studenti fakulteta koje smo naveli u hipotezi procjenili su veće znanje po pitanjima internetskih politika privatnosti i zaštite podataka od studenata ostalih fakulteta, a veće su znanje pokazali i po pitanjima „kolačića“ i prava omogućenih Općom uredbom o zaštiti podataka. Osim studenata FSB-a, čije su mjesto zauzeli studenti PMF-a, većinom su studenti s navedenih fakulteta pokazali i najveću zabrinutost za osobne podatke na internetu. Također, studenti diplomskog studija pokazali su veće znanje po istim pitanjima te veću zabrinutost za osobne podatke od studenata preddiplomskog studija. Ovi razultati djelomično se slažu s rezultatima istraživanja Horvat i Šolić (2020:6) koji su pronašli razlike, iako statistički neznačajne, u znanju i zabrinutosti s obzirom na razinu studija među studentima Sveučilišta u Osijeku. Tim su istraživanjem (2020:7) autori došli do rezultata koji pokazuju da se stariji studenti, odnosno studenti više godine studija, manje rizično ponašaju te su svjesniji rizika koji postoje pri korištenju interneta, unatoč njihovom zaključku i usporedbom s ranijim istraživanjima koji objašnjavaju kako su novije generacije svjesnije o rizicima na internetu te se ponašaju sigurnije.

H2: Studenti s boljim akademskih uspjehom, odnosno većom prosječnom ocjenom, imaju više znanja o politikama privatnosti i načinima zaštite osobnih podataka te su više zabrinuti oko ugroženosti osobnih podataka na internetu.

Našim smo istraživanjem utvrdili da studenti s najčešće dobivenom ocjenom dobar pokazuju više znanja o politikama privatnosti i načinima zaštite osobnih podataka i veću zabrinutost oko ugroženosti osobnih podataka na internetu od studenata s najčešće dobivenom ocjenom vrlo dobar**.** Naime, većinom su kroz prosječno najveći postotak slaganja s tvrdnjama iz druge kategorije pitanja anketnog upitnika veće znanje samoprocijenili studenti dobroga uspjeha (68.50%) od studenata vrlo dobrog uspjeha (49.25%), a najveću razliku u procjenama vidimo kod upućenosti u strategije kontrole vlastite privatnosti na intrenetu gdje je 78% studenata dobrog uspjeha označilo upućenost u odnosu na 49% studenata vrlo dobrog uspjeha. Također, studenti su dobrog uspjeha u prosjeku većinom upoznatiiji s pravima omogućenim Općom uredbom o zaštiti podataka (prosječno 2.77 prava po studentu) od studenata vrlo dobrog uspjeha (prosječno 2.09 prava po studentu).

Osim toga, 80% studenata dobrog uspjeha većinom je upoznatije i s prirodom „kolačića“ od 59% studenata vrlo dobrog uspjeha, kao i s postavljanjem preglednika tako da

ne prima „kolačiće“ gdje je 64% studenata dobrog uspjeha označilo upoznatost u odnosu na 50% studenata vrlo dobrog uspjeha. Međutim, 45% studenata vrlo dobrog uspjeha izrazilo je zabrinutost za svoje osobne podatke na internetu u odnosu na 43% studenata dobrog uspjeha.

Naša je druga hipoteza, dakle, opovrgnuta iz razloga što smo usporedbom rezultata saznali da studenti dobrog uspjeha pokazuju najveće znanje po pitanju osobnih podataka na internetu, dok najveću zabrinutost za svoje osobne podatke na internetu pokazuju studenti vrlo dobrog uspjeha. Ovi su rezultati također različiti od onih dobivenih u istraživanju Horvat i Šolić (2020:7) gdje nije nađena razlika u znanjima i zabrinutosti po pitanju zaštite privatnosti na internetu s obzirom na ocjene među studentima sastavnica Sveučilišta u Osijeku.

H3:Većina studenata se na internetu nastoji zaštititi tako da; koristi VPN mreže kako bi zaštitili svoje podatke na internetu, proučavaju uvjete privatnosti internetskih stranica i ne odgovaraju na neželjenu elektroničku poštu.

Rezultati pokazuju da je naša treća hipoteza istraživanjem opovrgnuta. Naime, u našem istraživanju, kao i u istraživanju autora Irfan, Akhter i Shakeel (2020:1789), studenti koji koriste VPN mreže kako bi očuvali privatnost na internetu su u manjini. U našem uzorku 17% studenata redovito koristi VPN mreže. Također, naše je istraživanje kao i istraživanje autorice Nili Steinfeld (2016:995) dokazalo da studenti većinom uopće ne čitaju uvjete i odredbe korištenja pri pristupu internetskim stranicama i instalaciji aplikacija. U našem uzorku 60% studenata uopće ne čita uvjete i odredbe. Dakle, korištenje VPN mreža i proučavanje uvjeta privatnosti internetskih stranica nisu metode kojima većina studenata nastoji zaštiti svoje podatke na internetu. Ipak, pronašli smo da 99% studenata ne odgovara na neželjenu elektroničku poštu.

Istraživanjem smo ustanovili da studenti većinom redovito koriste sljedeće metode: korištenje snažnih lozinki (75%), korištenje antivirusnih aplikacija (72%), korištenje različitih lozinki za različite račune na internetu (53%) te korištenje dodataka za pretraživače koji blokiraju oglase (49.5%).

H4: Studenti koji koriste internet dulje tijekom dana, u odnosu na one koje koriste kraće, su manje zabrinuti u vezi zaštite osobnih podataka na internetu.

Ova je hipoteza također opovrgnuta. Većinom studenti koji internet koriste od 5 do 7 sati dnevno pokazuju najveću zabrinutost u vezi zaštite osobnih podataka na internetu. Na tvrdnju „Zabrinut/a sam zbog ugroženosti svojih osobnih podataka na internetu“ slaganje je

izrazilo 50% studenata koji internet koriste od 5 do 7 sati dnevno, dok su oni koji ga koriste od 3 do 5 sati dnevno izrazili 35% slaganja, oni koji ga koriste od 1 do 3 sata dnevno 37.5% slaganja, dok je 47% studenata koji internet koriste više od 7 sati dnevno izrazilo zabrinutost. Dakle, rezultati našeg istraživanja pokazuju kako dulje dnevno korištenje internetu nije povezano s manjom zabrinutosti za osobne podatke.

5. ZAKLJUČAK

Pojava interneta i njegova široka primjena penetrirala je svakodnevicu i potpuno izmijenila načine na koje se danas njegovi korisnici informiraju, educiraju, zabavljaju i komuniciraju. Pod najveće prednosti interneta spadaju njegova brzina i doseg, odnosno mogućnost nadilaženja prostorno-vremenskih barijera, a pod njegovim je utjecajem promjenjena i današnja ekonomija koja se u sve većoj mjeri oslanja na internet i komunikacijske tehnologije. Razvijena je tzv. ekonomija osobnih podataka, za koje postoji tržište i na koje je stavljena ekonomska vrijednost. Slijedom toga privatnost je korisnika izložena i podložna manipulaciji i zloupotrebi od strane raznih aktera na internetu. Prikupljanje osobnih podataka korisnika danas je sveprisutan temelj funkcioniranja internetskih tvrtki koje akumulacijom podataka stvaraju detaljne profile ponašanja i afiniteta korisnika. Nekad su ti podatci korišteni u svrhu stvaranja prilagođenog internetskog iskustva (npr. prilagođeni oglasi), a nekad su korišteni u podle svrhe (npr. krađa identiteta). Iz tog razloga, nužno je za korisnike interneta da poduzmu odgovarajuće korake kako bi svoje podatke držali pod vlastitom kontrolom, a to je moguće potaknuti medijskim i informacijskim opismenjivanjem korisnika. Naime, sigurnosna pismenost na internetu jedan je od aspekata tih pismenosti, a koja podrazumijeva razumijevanje i svijest o tome kako se informacije i osobni podaci prate i koriste u internetskom okruženju.

Uzimajući u obzir sve navedeno, odlučili smo provesti istraživanje kojim smo istražili internetske sigurnosne kompetencije studenata Sveučilišta u Zagrebu. Navedenim smo istraživanjem istražili percepciju studenata o svojim sigurnosnim kompetencijama, znanje o metodama prikupljanja podataka i pravnim aspektima zaštite podataka, metode zaštite podataka koje koriste te svijest i zabrinutost u vezi osobnih podataka na internetu. Prije istraživanja postavili smo četiri cilja te jednu glavnu i tri sporedne hipoteze koje su uglavnom opovrgnute. Prvi cilj istraživanja bio je utvrditi postoje li razlike u poznavanju internetskih politika privatnosti i načina prikupljanja podataka te razlike u zabrinutosti oko ugroženosti osobnih podataka na internetu među studenatima s obzirom na fakultet koji pohađaju. Istraživanjem smo utvrdili da razlike postoje te da veće znanje povezano s osobnim podatcima na internetu pokazuju studenti FOI-a, FSB-a, FER-a i PFZG-a u odnosu na studente ostalih fakulteta. U usporedbi sa studentima ostalih fakulteta, najmanje znanja po pitanjima zaštite podataka na internetu pokazali su studenti KIF-a i UFZG-a te PMF-a. Naši rezultati u nesuglasju su s rezultatima istraživanja Horvat i Šolić (2020:6) koji nisu pronašli značajne razlike među studentima različitih sastavnica Sveučilišta J.J. Strossmayera u Osijeku.

Drugi je cilj istraživanja bio istražiti razlikuje li se znanje i zabrinutost o zaštiti osobnih podataka na internetu među studentima s obzirom na akademski uspjeh. Istraživanjem smo utvrdili da postoje razlike u znanju i zabrinutosti studenata po pitanju zaštite osobnih podataka na internetu među studentima s obzirom na akademski uspjeh, odnosno da studenti dobroga uspjeha pokazuju najveće znanje o internetskim politikama privatnosti i načinima zaštite osobnih podataka, a pokazaju i najveću zabrinutost za svoje osobne podatke na internetu. Međutim, brojnost studenata odličnog (N=6) i dovoljnog (N=3) uspjeha u uzorku kojeg smo uspoređivali nedovoljna je za izvlačenje zaključaka o tim kategorijama studenata, stoga smo usporedili rezultate samo studenata vrlo dobrog (N=34) i dobrog (N=55) uspjeha. Ovi su rezultati također različiti od onih dobivenih u istraživanju Horvat i Šolić (2020:7) gdje nije pronađena razlika u znanjima i zabrinutosti po pitanju zaštite privatnosti na internetu s obzirom na ocjene među studentima sastavnica Sveučilišta u Osijeku.

Treći je cilj istraživanja bio istražiti na koje se sve načine studenti nastoje zaštiti kako bi zaštitili svoje osobne podatke na internetu. Analizom rezultata otkrili smo da studenti najčešće koriste sljedeće metode zaštite osobnih podataka: korištenje snažnih lozinki, korištenje antivirusnih aplikacija, korištenje različitih lozinki za različite račune na internetu te korištenje dodataka za pretraživače koji blokiraju oglase.

Četvrti cilj istraživanja bio je istražiti postoji li povezanost između duljine dnevnog korištenja interneta i razine zabrinutosti u vezi zaštite osobnih podataka na internetu. Usporedbom rezultata otkrili smo da studenti koji internet koriste dulje tijekom dana u odnosu na one koji ga koriste kraće pokazuju veću zabrinutost za svoje osobne podatke. Ponovno su naši rezultati u nesuglasju s rezultatima istraživanja Horvat i Šolić (2020:7) gdje nisu pronađene razlike u znanju i zabrinutosti po pitanjima zaštite osobnih podataka među studentima Sveučilišta u Osijeku s obzirom na učestalost korištenja intreneta.

Na temelju provedenog istraživanja zaključujemo da se studenti različitih fakulteta razlikuju po znanju, zabrinutosti i stavovima o zaštiti osobnih podataka. Uvjerljivo najveće znanje o tematici zaštite osobnih podataka na internetu pokazuju studenti FOI-a, FER-a i FSB-a, što se može pripisati informatičkoj prirodi akademskog usmjerenja tih fakulteta. Također, studenti PFZG-a očekivano su se dokazali kao najbolji poznavatelji pravnih aspekata zaštite osobnih podataka. S druge strane, najmanje znanja pokazali su studenti KIF-a, ali i PMF-a i MEF-a, što znači da bi se na tim fakultetima informacijska i medijska pismenost trebala više

uključiti u studijski program na način da fakulteti organiziraju seminare ili kratke tečajeve za studente da postanu potpuno svjesni sigurnosti na internetu.

Istraživanjem smo dokazali da većina studenta svjesno i aktivno poduzima korake kako bi zaštitila svoje podatke na internetu, što pokazuje da je svijest o ugroženosti osobnih podataka na internetu među sudionicima na visokoj razini. S obzirom na to da su studenti kojima je ocjena dobar (3) najčešća prosječna ocjena na ispitima tijekom studija pokazali veće znanje i zabrinutost u vezi osobnih podataka na interenetu, nismo dokazali da je bolji akademski uspjeh povezan s većim znanjem i zabrinutosti u vezi osobnih podataka na internetu. No, temeljem provedenog istraživanja možemo izvući zaključak da su veća zabrinutost i znanje povezani s duljim dnevnim korištenjem interneta među sudionicima, zbog toga što su studenti koji koriste internet više od 7 sati dnevno pokazali veće znanje i zabrinutost po tom pitanju. To se odnosi i na studente diplomske razine studija u odnosu na studente preddiplomske razine studija. Unatoč tome što se u RH učenici medijski opismenjuju u sklopu segmenta medijske kulture na predmetu Hrvatskog jezika, sigurnosne kompetencije studenata preddiplomskog studija na internetu, koje bi trebale biti dotaknute i na predmetu Informatike tijekom osnovnoškolskog i srednjoškolskog obrazovanja, nisu na razini na kojoj bi trebale biti kako bi se moglo govoriti o potpunoj očuvanosti privatnosti studenata na internetu. Budući da je upotreba osobnih podataka od strane aktera, koji su korisniku često nepoznati, stvarnost na internetu, ovaj rad ilustrira da mladi moraju biti educirani o rizicima za njihovu privatnost na način koji zapravo mijenja njihovo ponašanje. Ovim smo istraživanjem, dakle, dobili sliku o tome kako studenti različitih sastavnica Sveučilišta u Zagrebu razmišljaju o temi zaštite osobnih podataka na internetu, a cjelokupan je rad izrađen s ciljem utvrđivanja da je internetska pismenost o privatnosti važan aspekt medijske i informacijske pismenosti.

No, iz razloga što je istraživanje provedeno na relativno malenom uzorku, rezultate je našeg istraživanja potrebno razmatrati kritički. Kako bi se dobila potpuna slika o znanju, stavovima i zabrinutosti studenata po pitanju zaštite osobnih podataka, ovakvo bi se istraživanje trebalo provesti s većim brojem sudionika, a u kojem bi sudjelovali studenti sa svih sastavnica Sveučilišta u Zagrebu, u jednakom broju s diplomskih i preddiplomskih studija. Unatoč ograničenjima našeg istraživanja, smatramo da ovaj rad može koristiti studentima i profesorima kao baza za širenje svijesti o izloženosti privatnosti korisnika interneta te kao motivacija za poduzimanje koraka za zaštitu osobnih podataka na internetu, jer unatoč popularnom mišljenju, poduzimanjem niza odgovarajućih koraka privatnost korisnika na internetu može ostati nedodirnuta.

6. POPIS KORIŠTENIH IZVORA

1. *Bittersweet cookies': new types of 'cookies' raise online security & privacy concerns* (2011.) European Network and Information Security Agency (ENISA) (datum objave: 18. veljače 2011.)
2. Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018.) „Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data" *Communication Research,* 1–25
3. *Forum o upravljanju internetom* (2021.) CARNET, https://www.carnet.hr/projekt/forum-o-upravljanju-internetom/ (datum posjete: 19. veljače 2021.)
4. *Internet Governance for Libraries: A Guide on the Policies and Processes behind the Internet and their impact Part 1*(2021) International Federation of Library Associations, https://www.ifla.org/files/assets/faife/publications/ig_guide_chapter_1.pdf (datum posjete: 20. veljače 2021.)
5. *Model Law on Computer and Computer Related Crime* (2017.) Tajništvo Commonwealtha, https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf
6. *Pravo na zaborav: što sve obuhvaća?* (2018.) GDPR Informer, https://gdprinformer.com/hr/gdpr-clanci/pravo-na-zaborav-sto-sve-obuhvaca (objavljeno: 5. veljače 2018.)
7. *Right to Object* (2021.) Dataguise, https://www.dataguise.com/gdpr-knowledge-center/right-to-object/ (datum posjete: 26. veljače 2021.)
8. *The challenges of internet governance* (2020.) France Diplomacy, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/the-challenges-of-internet-governance/ (posljednja izmjena: ožujak 2020.)
9. *The right to object to the use of your data* (2021.) The Information Commissioner's Office (ICO), internetska stranica, https://ico.org.uk/your-data-matters/the-right-to-object-to-the-use-of-your-data/ (datum posjete: 26. veljače 2021.)
10. *The Right to Restrict Processing* (2021.) MENDIP District Council, internetska stranica, https://www.mendip.gov.uk/article/6276/The-Right-to-Restrict-Processing (datum posjete: 26. veljače 2021.)
11. Dumičić, K., Žmuk, B. (2009.) „Karakteristike korisnika interneta u Hrvatskoj i reprezentativnost internetskih anketa", *Zbornik Ekonomskog fakulteta u Zagrebu*, vol. 7(2): 115–140, https://hrcak.srce.hr/44432
12. *Vaša prava* (2021.) Agencija za zaštitu osobnih podataka, internetska stranica, https://azop.hr/prava-ispitanika/ (datum posjete: 25. veljače 2021.)
13. *Vodič kroz GDPR za početnike* (2021.) GDPR Informer, https://gdprinformer.com/hr/vodic-kroz-gdpr (datum posjete 23. veljače 2021.)
14. *Web Beacon* (2021.) The International Association of Privacy Professionals, https://iapp.org/resources/article/web-beacon/ (datum posjete: 20. veljače 2021.)

15. *What is a botnet attack?* (2021.) Akamai, https://www.akamai.com/us/en/resources/what-is-a-botnet.jsp (datum posjete: 21. veljače 2021.)
16. *What is a Web Beacon?* (2020.) CookiePro, https://www.cookiepro.com/knowledge/what-is-a-web-beacon/ (posljednja izmjena: 21. listopada 2020.)
17. *Zaštita podataka u EU-u* (2021.) Europsko vijeće i Vijeće Europske unije, https://www.consilium.europa.eu/hr/policies/data-protection-reform/ (posljednja izmjena: 5. ožujka 2021.)
18. Mayer, J., Narayanan, A. (2010.) *Do Not Track: Universal Web Tracking Opt-out,* Stanford University Department of Computer Science
19. *Data Protection or Virus Protection?* (2016.) AV-TEST, https://www.av-test.org/en/news/data-protection-or-virus-protection/ (datum objave: 22. rujna 2016.)
20. Peran, S., Raguž, A.(2016.) „Medijska pismenost – obrazovanje studenata i svijest o vlastitoj odgovornosti", *Nova prisutnost : časopis za intelektualna i duhovna pitanja*, vol. 14(3): 379–392, https://hrcak.srce.hr/168715
21. Aimeur, E., Lafond, M. (2013.) „The Scourge of Internet Personal Data Collection*", 2013 International Conference on Availability, Reliability and Security*, Institute of Electrical and Electronics Engineers
22. Horvat, E., Šolić, K. (2020.) „Ispitivanje znanja i ponašanja studenata o pitanjima zaštite privatnosti na internetu metodom socijalnog inženjeringa", *Bilten Hrvatskog društva za medicinsku informatiku,* vol. 26.(2): 3–7, https://hrcak.srce.hr/244843
23. Harlow, A. (2010.) „Online surveys-possibilities, pitfalls and practicalities: the experience of the TELA evaluation", *Waikato Journal of Education*, vol. 15(2), 95–108, https://hdl.handle.net/10289/6163
24. *Protecting personal data in online services: learning from the mistakes of others* (2014.) Information Commissioner's Office, https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf
25. Bande, L. C. (2018.) „Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities", *International Journal of Cyber Criminology*, vol. 12 (1): 9–26, https://www.cybercrimejournal.com/BandeVol12Issue1IJCC2018.pdf
26. Wheatley, S., Maillart, T., & Sornette, D. (2016.) „The extreme risk of personal data breaches and the erosion of privacy", *The European Physical Journal B,* vol. 89 (7):1–17, https://doi.org/10.1140/epjb/e2015-60754-4
27. Bežovan, G. (2002.) „Struktura civilnog društva u Hrvatskoj", *Politička misao : časopis za politologiju*, vol. 39 (1): 63–87
28. *What is Digital Literacy?* (2021.) Common Sense Media, https://www.commonsensemedia.org/news-and-media-literacy/what-is-digital-literacy (datum posjete: 29. veljače 2021.)
29. Bislev, S., Flyverbom, M. (2021.) *Global Internet Governance: What Roles do Businesses Play?,* Copenhagen Business School, https://ecpr.eu/Filestore/paperproposal/dba8c7a7-58e5-4ea7-9ec1-2a2ddc939baa.pdf (datum posjete: 18. veljače 2021.)

30. Bojarski, L., Hofbauer, A., Miileszyk, N. (2014.) *Povelja o temeljnim pravima kao živi instrument: smjernice za civilno društvo,* Rim-Varšava-Beč: CFREU
31. Whitney, L. (2020.) *Most consumers worry about online privacy but many are unsure how to protect it*, TechRepublic, https://www.techrepublic.com/article/most-consumers-worry-about-online-privacy-but-many-are-unsure-how-to-protect-it/ (datum objave: 4. travnja 2020.)
32. *Browser Fingerprinting: The Surveillance You Can't Stop* (2017.) Multilogin, https://multilogin.com/browser-fingerprinting-the-surveillance-you-can-t-stop/ (datum objave: 29. svibnja 2017.)
33. *Protect Your Computer from Viruses, Hackers, & Spies* (2015.) California Department of Justice, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/CIS_12_Computer_protection_DOJ.pdf
34. Bujlow, T., Carela-Espanol, V., Lee, B.-R., Barlet-Ros, P. (2017.) „A Survey on Web Tracking: Mechanisms, Implications, and Defenses*", Proceedings of the IEEE,* vol. 105(8):1476–1510, 10.1109/jproc.2016.2637878
35. Cahn, A., Alfeld, S., Barford, P., & Muthukrishnan, S. (2016.) „An Empirical Study of Web Cookies" *Proceedings of the 25th International Conference on World Wide Web - WWW '16*, https://doi.org/10.1145/2872427.2882991
36. Calandro, E., Gillwald, A., Zingales, N. (2016.) *Mapping Multistakeholderism in Internet Governance: Implications for Africa*, Africa Portal, https://media.africaportal.org/documents/Discussion_paper_-_Mapping_Multistakeholderism_in_Internet_Governance_-_Implic_Zr3Zlht.pdf (datum objave: 26. listopada 2016.)
37. Cook, L. (2014) „The Right to be Forgotten: A Step in The Right Direction for Cyberspace Law and Policy", *Journal of Law, Technology and the Internet,* vol. 6 (18): 121–132, https://core.ac.uk/download/pdf/214110496.pdf
38. Couto, R. (2013.) „Online behavioural advertising: the impact of "cookies" on consumers' privacy", *International Conference on Technologies and Law* (datum: 8. i 9. studeni 2013.)
39. *What Is "Do Not Track" (DNT) and Does It Work?* (2021.) Avast, https://www.avast.com/c-what-is-do-not-track (datum objave: 17. ožujka 2021.)
40. Phua, C. (2009.) „Protecting organisations from personal data breaches" *Computer Fraud & Security*, vol. 2009(1):13–18, https://www.researchgate.net/publication/250726805_Protecting_organisations_from_personal_data_breaches
41. Malik, S. (2008) *Media Literacy and its Importance*, Society for Alternative Media and Research, Islamabad, https://library.fes.de/pdf-files/bueros/pakistan/06542.pdf
42. DeNardis, L. (2015.) „Five Destabilizing Trends in Internet Governance", A Journal of Law and Policy for the Information Society, vol. 12 (1): 113–133, https://core.ac.uk/download/pdf/159571587.pdf
43. Eslahi, M., Salleh, R., & Anuar, N. B. (2012.) „Bots and botnets: An overview of characteristics, detection and challenge", *2012 IEEE International Conference on Control System, Computing and Engineering*, https://www.researchgate.net/publication/261087741_Bots_and_botnets_An_overview_of_characteristics_detection_and_challenges (datum posjete: 21. veljače 2021.)

44. Esteve, A. (2017.) „The business of personal data: Google, Facebook, and privacy issues in the EU and the USA“, *International Data Privacy Law*, vol. 7(1), 36–47
45. Law, N., Woo, D., & Wong, G. (2018.) *A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4,* UNESCO, http://uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf
46. Son, J. B., Robb, T., Charismiadji, I (2011.) „Computer literacy and competency: a survey of Indonesian teachers of English as a foreign language“, *Computer-Assisted Language Learning Electronic Journal (CALL-EJ)*, vol. 12(1): 26-42, http://callej.org/journal/12-1/Son_2011.pdf
47. FaizKhademi, A., Zulkernine, M., & Weldemariam, K. (2015) „FPGuard: Detection and Prevention of Browser Fingerprinting*“, Lecture Notes in Computer Science*, 293–308
48. Što je digitalna pismenost? (2021.) EduLab, https://edulab.hr/sto-je-digitalna-pismenost/ (datum posjete: 29. veljače 2021.)
49. Kemp, S. (2021.) *Digital 2021: Global Overview Report*, DataReportal, https://datareportal.com/reports/digital-2021-global-overview-report (datum objave: 27. siječnja 2021.)
50. Gamal Sayed Ahmed ElSayed Eid, N. (2020.) *The Private Sector's Role in Internet Governance: East and West, Two Sides of the Same Coin*, Sveučilište u Firenci, https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2020_Sayed_Gamal.pdf (datum posjete: 18. veljače 2021.)
51. Ghezzi, A., Pereira, Â. G., & Vesnić-Alujević, L. (2014.) *The Ethics of Memory in a Digital Age*, London: Palgrave Macmillan UK
52. Sundaram, S. (2017.) *Attacking Network Device PART — 4*, Medium, https://iratoon.medium.com/attacking-network-device-part-4-6347d2bb619a (datum objave: 18. lipnja 2017.)
53. Goddard, M. (2017.) „The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact*“, International Journal of Market Research*, vol. 59(6): 703–705, https://doi.org/10.2501/IJMR-2017-050 (objavljeno: 1. studenog 2017.)
54. Streitz, M., i Tynan, R. (2016.) „Are ad-blockers killing the media?“ *Speigel Online's Matthias Streitz in a head-to-head debate with Privacy International's Richard Tynan. Index on Censorship*,vol. 45(2): 78–80. doi:10.1177/0306422016657033
55. Internet Engineering Task Force (2021.) https://www.ietf.org/about/who/ (datum posjete: 19. veljače 2021.)
56. Steinfeld, N. (2016.) „I agree to the terms and conditions: (How) do users read privacy policies online? An eye-tracking experiment“, *Computers in Human Behavior*, vol. 55(2016): 992–1000, https://www.researchgate.net/publication/284233087_I_agree_to_the_terms_and_conditions_How_do_users_read_privacy_policies_online_An_eye-tracking_experiment
57. Gervais, A., Filios, A., Lenders, V., i Capkun, S. (2017.) „Quantifying Web Adblocker Privacy*“, Lecture Notes in Computer Science*, 21–42, https://eprint.iacr.org/2016/900.pdf

58. Esteve, A. (2017.) „The business of personal data: Google, Facebook, and privacy issues in the EU and the USA“, *International Data Privacy Law*, vol. 7(1): 36–47, https://doi.org/10.1093/idpl/ipw026
59. Internet Governance Forum (2021.) https://www.intgovforum.org/multilingual/tags/about (datum posjete: 19. veljače 2021.)
60. Klang, M. (2003.) „Spyware: paying for software with our privacy“, *International Review of Law, Computers & Technology*, vol. 17(3): 313–322
61. Kokot, Ivica (2014.) „Kaznenopravna zaštita računalnih sustava, programa i podataka“, *Zagrebačka pravna revija,* vol. 3(3): 303–330, https://hrcak.srce.hr/141877
62. Kurbalija, J. (2014.) *An Introduction to Internet* Governance, 6. izdanje, Ženeva: DiploFoundation
63. Malhotra, N. K., Kim, S. S., i Agarwal, J. (2004.) „Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model“, *Information Systems Research*, vol. 15(4): 336–355, https://www.jstor.org/stable/23015787
64. Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2014.) „Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS)“, *Reforming European Data Protection Law*, 333–365
65. Zorbaz, O., Demirtaş Zorbaz, S., & Ulaş Kılıç, Ö. (2020.) „Problematic internet use of adolescents: Role of daily hassles and social isolation“, *Addicta: The Turkish Journal on Addictions*, vol. 7(1): 41-47, https://www.addicta.com.tr/en/problematic-internet-use-of-adolescents-role-of-daily-hassles-and-social-isolation-13153
66. Kurbalija, J. (2021.) „The emergence of digital foreign policy“, DiploFoundation
67. Latto, N. (2021.) *What Is Browser Fingerprinting and How Can You Prevent It?*, Avast, https://www.avast.com/c-what-is-browser-fingerprinting (posljednja izmjena: 19. ožujka 2021.)
68. Catts, R., Lau, J. (2008.)"Towards Information Literacy Indicators“, Paris, Francuska: UNESCO, http://www.uis.unesco.org/Library/Documents/wp08_InfoLit_en.pdf
69. Mitchell, I., D. (2012.) „Third-Party Tracking Cookies and Data Privacy“, *SSRN Electronic Journal*, 1–9 http://dx.doi.org/10.2139/ssrn.2058326
70. Musiani, F. (2013.) „Dangerous Liaisons? Governments, companies and Internet governance“, *Internet Policy Review*, 2(1), https://doi.org/10.14763/2013.1.108
71. Nonnecke, B. (2016.) „The transformative effects of multistakeholderism in Internet governance: A case study of the East Africa Internet Governance Forum“, *Telecommunications Policy*, vol. 40(4): 343–352, https://doi.org/10.1016/j.telpol.2015.12.005
72. Nye, Jr., J.S. (2014.) *The Regime Complex for Managing Global Cyber Activities, Belfer Centar za znanost i međunarodne poslove*, Harvard Kennedy, https://www.belfercenter.org/sites/default/files/files/publication/global-cyber-final-web.pdf (datum posjete: 18. veljače 2021.)
73. Opća uredba o zaštiti podataka (2016.) Europski parlament i Vijeće Europske unije, 25. svibnja 2016.

74. Baćak, V. (2006.) „Uzorkovanje upravljano ispitanicima: novi pristup uzorkovanju skrivenih populacija“, *Revija za sociologiju*, vol. 37(3-4): 193–204, https://hrcak.srce.hr/13218
75. Micheli, M., Lutz, C., & Büchi, M. (2018.) „Digital footprints: an emerging dimension of digital inequality“, *Journal of Information, Communication and Ethics in Society*, vol. 6(3): 242-251, https://doi.org/10.1108/JICES-02-2018-0014
76. Panchenko, A., Lanze, F., Zinnen, A., Henze, M., Pennekamp, J., Wehrle, K., & Engel, T. (2016.) „Website Fingerprinting at Internet Scale*“, Proceedings 2016 Network and Distributed System Security Symposium*, 1–15, *http://dx.doi.org/10.14722/ndss.2016.23477*
77. Park, J. S., & Sandhu, R. (2000.) „Secure cookies on the Web“ *IEEE Internet Computing*, vol. 4(4): 36–44
78. Brown, M.R., i Muchira, R. (2004.) „Investigating the Relationship between Internet Privacy Concerns and Online Purchase Behavior“, *J. Electron. Commer. Res.*, vol. 5*:* 62–70
79. Jaha, A. A., Shatwan, F. B., i Ashibani, M. (2008.) „Proper Virtual Private Network (VPN) Solution*“, The Second International Conference on Next Generation Mobile Applications, Services, and Technologies,* 309–314,
80. *How Does Antivirus Work?* (2020.) Standard Office Systems, https://www.soscanhelp.com/blog/how-does-antivirus-work (datum objave: 1. rujna 2020.)
81. Pollach, I. (2007.) „What’s wrong with online privacy policies?“, *Communications of the ACM*, vol. 50(9): 103–108, https://www.researchgate.net/publication/220421895_What's_wrong_with_online_privacy_policies
82. Povelja Europske unije o temeljnim pravima (2016.) Službeni list Europske unije, 202/389, 7. lipnja 2016.
83. Strycharz, J., van Noort, G., Smit, E., & Helberger, N. (2019.) „Protective behavior against personalized ads: Motivation to turn personalization off“, *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 13(2): članak 1., https://doi.org/10.5817/CP2019-2-1 s
84. Kuneva, M. (2009.) *Roundtable on Online Data Collection, Targeting and Profiling*, Bruxelles, govor, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156
85. Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K.-L. (2015.) „The challenges of personal data markets and privacy“, *Electronic Markets*, vol. 25(2): 161–167, https://www.heinz.cmu.edu/~acquisti/papers/SpiekermannAcquistiBohmeHui-EM-2015.pdf
86. Purcell, F., Vernous, G., Wakunuma, K., Akbar, S., Finquelievich, S. (2006.) *Role of Civil Society: Internet Governance and Developing Countries*, DiploFoundation
87. Shan, S., Bhagoji, A. N., Zheng, H., Zhao, B. Y. (2021.) *A Real-time Defense against Website Fingerprinting Attacks*, stručni rad, Sveučilište u Chicagu, https://arxiv.org/pdf/2102.04291.pdf
88. Sipior, J. C., Ward, B. T., & Mendoza, R. A. (2011.) „Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons“ *Journal of Internet Commerce*, vol. 10(1): 1–16

89. Stafford, T. F., Urbaczewski, A (2004.) „Spyware: The Ghost in the Machine“, *Communications of the Association for Information Systems*, vol. 14(15): 291-306, https://aisel.aisnet.org/cgi/viewcontent.cgi?article=3274&context=cais (datum posjete: 21. veljače 2021.)
90. Stevanovic, M., & Pedersen, J. M. (2013.) *Machine learning for identifying botnet network traffic,* Sveučilište u Aalborgu, https://vbn.aau.dk/ws/portalfiles/portal/75720938/paper.pdf (datum posjete: 21. veljače 2021.)
91. Lazić-Lasić, J., Špiranec, S., Banek Zorica, M. (2012.) „Izgubljeni u novim obrazovnim okruženjima – pronađeni u informacijskom opismenjivanju“, *Medijska istraživanja : znanstveno-stručni časopis za novinarstvo i medije*, vol. 18(1), https://hrcak.srce.hr/85384
92. Tankard, C. (2016.) „What the GDPR means for businesses“, *Network Security*, 2016 (6): 5–8
93. *Consumer Attitudes Toward Data Privacy Survey* (2020.) Akamai, https://www.akamai.com/us/en/multimedia/documents/report/akamai-research-consumer-attitudes-toward-data-privacy.pdf (datum posjete: 1. ožujka 2021.)
94. Sideri, M., Gritzalis, S. (2020.) „Are We Really Informed on the Rights GDPR Guarantees?“, u Furnell, S. i Clarke, N. (ur.) *Human Aspects of Information Security and Assurance*, New York: Springer International Publishing, str. 315–326
95. Presthus, W., & Sørum, H. (2018.) „Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation“, *Procedia Computer Science*, vol. 138, 603–611, https://doi.org/10.1016/j.procs.2018.10.081
96. Irfan, H., Akhter, K. J.,Shakeel, R. (2020.) „Cybersecurity and Multidisciplinary Students: A Survey“, *International Journal of Scientific & Engineering Research*, vol. 11(4): 1786–1791, https://www.citefactor.org/journal/pdf/Cybersecurity-and-Multidisciplinary-Students-A-Survey.pdf
97. Labaš, D., Marinčić, P. (2018.) „Mediji kao sredstvo zabave u očima djece“, *MediAnali : međunarodni znanstveni časopis za pitanja medija, novinarstva, masovnog komuniciranja i odnosa s javnostima*, vol. 12(15): 1–32, https://hrcak.srce.hr/195548
98. *These organisations are shaping the Internet: The most important Internet governance actors* (2019.), Internet Governance Forum Berlin, https://www.igf2019.berlin/IGF/Redaktion/EN/Artikel/internet-governance-actors.html (datum objave: 23. svibnja 2019.)
99. Ugovor o funkcioniranju Europske unije (2016.) Službeni list Europske unije, 202/21, 7. lipnja 2016.
100. Upathilake, R., Li, Y., & Matrawy, A. (2015.) „A classification of web browser fingerprinting techniques“, 7th International Conference on New Technologies, Mobility and Security (NTMS)
101. McDonald, A., Cranor, L. (2008.) „The Cost of Reading Privacy Policies“, *A Journal of Law and Policy for the Information Society*, vol. 4(3): 543–568, http://hdl.handle.net/1811/72839
102. Upravljanje Internetom (2021.) Registar nacionalnog internet domena Srbije, https://www.rnids.rs/lat/o-nama/upravljanje-internetom (datum posjete: 18. veljače 2021.)

103. *The Role of Firewalls in Defending Your Data* (2020.) ISG Technology, https://www.isgtech.com/the-role-of-firewalls-in-defending-your-data/ (datum objave: 12. prosinca 2020.)
104. Martin, K. D., & Murphy, P. E. (2016.) „The role of data privacy in marketing“, *Journal of the Academy of Marketing Science*, vol.45(2), 135–155, https://doi.org/10.1007/s11747-016-0495-4
105. Beroš, I. (2020.) „Razlike u razini medijske pismenosti studenata jednopredmetnog preddiplomskog i diplomskog studija pedagogije na Sveučilištu u Zagrebu i Rijeci s obzirom na osobne i odgojno-obrazovne faktore“, *Časopis za odgojne i obrazovne znanosti Foo2rama*, vol. 4(4): 9–28, https://hrcak.srce.hr/251664
106. Ustav Republike Hrvatske (pročišćeni tekst) (2001.) *Narodne novine*, br. 41, 7. svibnja 2001.
107. Duffy, B., Smith, K., Terhanian, G., & Bremer, J. (2005.) „Comparing data from online and face-to-face surveys“ *International Journal of Market Research*, vol. 47(6): 615–639. https://doi.org/10.1177/147078530504700602
108. Špiranec, Sonja (2008.) *Informacijska pismenost : teorijski okvir i polazišta*, Zagreb : Filozofski fakultet, Odsjek za informacijske znanosti, Zavod za informacijske studije
109. Jokić, A., Koljenik, D., Faletar Tanceković, S., Badurina, B. (2016.) „Vještine informacijske i informatičke pismenosti studenata informacijskih znanosti u Osijeku: pilot-istraživanje“, *Vjesnik bibliotekara Hrvatske*, vol. 59(3-4): 63–92, https://hrcak.srce.hr/187610
110. Lee, A.Y.L., So, C.Y.K. (2014.) „Media Literacy and Information Literacy: Similarities and Differences“, *Alfabetización mediática y alfabetización informacional: similitudes y diferencias*. vol. 21(42): 137–146, https://www.revistacomunicar.com/indice-en/articulo.php?numero=42-2014-13
111. Watson, J. (2020.) *How to protect yourself against invisible browser fingerprinting*, Comparitech, https://www.comparitech.com/blog/vpn-privacy/what-is-browser-fingerprinting-how-to-protect-yourself/ (datum objave: 9.listopada 2020.)
112. *What Is ICANN and Why Does It Matter? (*2016.) Data Foundry, https://www.datafoundry.com/blog/what-is-icann (datum objave: 11. srpnja 2016.)
113. Sharma, Y. K., Kaur, C. (2020.) „The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World“, *International Journal of Recent Technology and Engineering*, vol. 8(6): 2336 – 2339, https://www.researchgate.net/publication/340336829_The_vital_role_of_VPN_in_making_secure_connection_over_internet_world
114. Zabawa, T. (2020.) *The Internet and Web Tracking*, Grand Valley State University, https://scholarworks.gvsu.edu/cistechlib/355/
115. Zakon o elektroničkim komunikacijama (2008.) *Narodne novine*, br. 73, 26. lipnja 2008.
116. Zakon o informacijskoj sigurnosti (2007.) *Narodne novine*, br. 79, 30. srpnja 2007.
117. Zakon o provedbi Opće uredbe o zaštiti podataka (2019.) *Narodne novine*, br. 42, 9. svibnja 2018.
118. Zakon o zaštiti osobnih podataka (2003.) *Narodne novine*, br. 103, 26. lipnja 2003.

7. PRILOG

7.1. Anketni upitnik

1. Vaša dob? a. 18-20, b. 21-25, c. 26-30

2. Vaš spol? a. M, b. Ž

3. Koji fakultet pohađate? a. Ekonomski fakultet Sveučilišta u Zagrebu

b. Pravni fakultet Sveučilišta u Zagrebu

c. Filozofski fakultet Sveučilišta u Zagrebu

d. Prirodoslovno-matematički fakultet Sveučilišta u Zagrebu

e. Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu

f. Medicinski fakultet Sveučilišta u Zagrebu

g. Učiteljski fakultet Sveučilišta u Zagrebu

h. Kineziološki fakultet Sveučilišta u Zagrebu

i. Fakultet organizacije i informatike Sveučilišta u Zagrebu

j. Fakultet strojarstva i brodogradnje Sveučilišta u Zagrebu

k. ostalo: _____

4. Na kojoj se razini studija trenutno nalazite? a. Preddiplomski studij b. Diplomski studij

5. Koja je Vaša prosječna ocjena na ispitima tijekom studija? a. 1, b. 2, c. 3, d. 4 e. 5

6. Kolika je prema Vašoj procjeni Vaša prosječna učestalost svakodnevnog korištenja interneta? a. manje od sat vremena dnevno, b. od 1 do 3 sata dnevno, c. od 3 do 5 sati dnevno, d. 5 do 7 sati dnevno, e. više od 7 sati dnevno

---

7. U nastavku se nalazi nekoliko tvrdnji. Pročitajte svaku tvrdnju i procijenite u kojoj se mjeri tvrdnja odnosi na Vas (1 = nimalo se ne slažem, 2 = ne slažem se, 3 = niti se slažem niti se ne slažem, 4 = slažem se, 5 =u potpunosti se slažem):

a. Razumijem što su internetske politike privatnosti i kako one utječu na privatnost mojih osobnih podataka. (1-5)

b. Upućen/a sam u strategije koje vlasti i internetske tvrtke kao što su društveni mediji (npr. Facebook, Twitter), tražilice (npr. Google, Yahoo, Bing), pružatelji internetskog bankarstva itd. koriste za nadzor, prikupljanje, obradu i brisanje osobnih podataka (1-5).

c. Upoznat/a sam sa zakonima i pravnim aspektima mrežne zaštite podataka (1-5).

d. Upoznat/a sam sa strategijama kontrole moje privatnosti na mreži kao što su redovito brisanje „kolačića“, korištenje firewall-a i sl. (1-5).

8. U nastavku se nalazi nekoliko tvrdnji. Pročitajte svaku tvrdnju i odaberite broj koji iskreno odražava koliko često koristite navedene metode zaštite osobnih podataka na interentu.

(1 = nikada, 2 = rijetko, 3 = ponekad, 4 = često, 5 =vrlo često):

a. Koristim antivirusne računalne programe kako bih zaštitio svoje podatke. (1-5)

b. Ne koristim istu lozinku za sve korisničke račune na internetu. (1-5)

c. koristim snažne lozinke (kombinacija velikih i malih slova, brojki i znakova). (1-5)

d. koristim firewall kako bih zaštitio/la svoje podatke i dokumente.. (1-5)

e. ne spajam se na javne WiFi mreže. (1-5)

f. uključim „Ne prati“ (engl. „Do Not Track“) sigurnosnu funkciju na svojem web pretraživaču

g. koristim VPN mreže. (1-5)

h. koristim dodatke za pretraživače koji blokiraju oglase. (1-5)

i. redovito brišem „kolačiće“. (1-5)

j. ne pristupam stranicama koje zahtijevaju obavezno prihvaćanje „kolačića“ za pristup njima. (1-5)

k. ispunim pogrešne podatke o sebi (na primjer, lažno ime ili pogrešna adresa e-pošte) kada se zatraže takve informacije na internetu. (1-5)

Na sljedećim pitanjima označite odgovor(e) koji se odnose na Vas

9. Koju vrstu podataka ste obično voljni dati kako biste ostvarili koristi od online poduzeća kao što su popusti na robu i usluge ili brže/bolje usluge? 1. Ime 2. Prezime 3. E-mail adresu 3. Građanstvo 4. Adresa 5. Broj telefona 6. Datum rođenja 7. OIB 8. broj kartice

10. Ako koristite dodatke za web pretraživače koji blokiraju oglase, koji je ralog Vašeg korištenja dodatka za web pretraživače koji blokiraju oglase? a. Oglasi me nerviraju, b. Kako bih spriječio/la spam poruke, c.Kako bih izbjegao/la da web stranice prikupljaju podatke o meni bez mojeg pristanka, d. Drugi razlozi

11. Za koja ste od navedenih prava koja Vam osigurava GDPR regulativa čuli, odnosno s kojima ste od sljedećih prava upoznati?

a. Pravo pristupa osobnim podacima, b. Pravo na ispravak osobnih podataka, c. Pravo na brisanje osobnih podataka („pravo na zaborav”), d. Pravo na ograničenje obrade osobnih podataka, e. Pravo na prigovor, f. Pravo na prenosivost podataka

12. Koja ste od navedenih prava koja Vam omogućuje GDPR regulativa koristili do sada?

a. Pravo pristupa osobnim podacima, b. Pravo na ispravak osobnih podataka, c. Pravo na brisanje osobnih podataka („pravo na zaborav"), d. Pravo na ograničenje obrade osobnih podataka, e. Pravo na prigovor, f. Pravo na prenosivost podataka, g. sve od navedenih, h. nijedno od navedenih

---

Na sljedećim pitanjima označite jedan odgovor koji se odnosi na Vas.

13. Znate li značenje „kolačića" na mrežnim stranicama? a. znam, b. ne znam, c. nisam siguran/na

14. Znate li postaviti internetski pretraživač tako da ne prima „kolačiće" bez prethodnog upita? a. znam, b. ne znam, c. nisam siguran/na

15. Jeste li do sada promijenili postavke „kolačića" na Vašem web pregledniku? a. jesam 2. nisam, c. nisam siguran/na

16. Jeste li ikada u prošlosti isključili personalizaciju oglasa na Vašem web pretraživaču? a. jesam, b. nisam, c. nisam siguran/na

17. Odgovarate li na neželjenu elektroničku poštu? a. da, b. ne, c. ponekad

18. Prilikom preuzimanja aplikacije na mobilni uređaj ili instaliranja aplikacije na računalo, kao korisnik morate prihvatiti uvjete i odredbe. Što uglavnom činite u toj situaciji? a. Pristajem na uvjete i odredbe bez čitanja istih, b. Brzo prođem kroz tekst bez da pročitam sve, pa onda pristanem, c. Pročitam čitavi tekst, pa onda pristanem

---

19. U nastavku se nalazi nekoliko tvrdnji. Pročitajte svaku tvrdnju i procijenite u kojoj se mjeri tvrdnja odnosi na Vas (1 = nimalo se ne slažem, 2 = ne slažem se, 3 = niti se slažem niti se ne slažem, 4 = slažem se, 5 =u potpunosti se slažem):

a. Koristim Facebook, Twitter ili Google račun za prijavu na druge web stranice. (1-5)

b. Vjerujem da su moji osobni podatci sigurni na web stranicama. (1-5)

c. Zabrinut/a sam zbog ugroženosti svojih osobnih podataka na internetu. (1-5)

d. Smatram da internet postaje utočište za neželjenu elektroničku poštu. (1-5)

e. Smatram da će internetske tvrtke čuvati povjerljivim ono što o meni saznaju iz mojih aktivnosti na njihovoj web lokaciji. (1-5)

f. Smatram kako nije dobro to što online trgovci mogu saznati osobne podatke o mrežnim kupcima bez njihovog pristanka. (1-5)(tvrdnje od d. do f. su preuzete i prilagođene iz Investigating the Relationship Between Internet Privacy Concerns and Online Purchase Behavior, Brown, 2004)

g.Obično me smeta kada internetske tvrtke traže moje osobne podatke. (1-5)

h. Kada me internetske tvrtke pitaju za osobne podatke, dobro razmislim prije nego što ih dam. (1-5)

i. Zabrinut/a sam da internetske tvrtke prikupljaju previše osobnih podataka o meni. (1-5)

j. Smatram personalizirane oglase koji mi se pojavljuju na internetu invazivnima. (1-5)

k. Smatram problematičnim činjenicu da tvrtke koriste moje internetsko ponašanje za sakupljanje podataka o meni kako bi mi prikazivale odgovarajuće oglase (1-5)

k. Oprostio/la bih tvrtki optuženoj zbog kršenja sigurnosti osobnih podataka ako me odmah obavijesti o prekršaju i onome što čini da me zaštiti. (1-5)

l. Smatram da je nemoguće zaštititi moju privatnost na internetu. (1-5)

m. Smatram da prednosti personaliziranih usluga na internetu koje proizlaze iz sakupljanja mojih osobnih podataka nadilaze važnost zaštite osobnih podataka (1-5)