Perspektiva učenika srednje škole o korištenju interneta i društvenih mreža

Švec, Lucija

SVEUČILIŠTE U ZAGREBU

PRAVNI FAKULTET

STUDIJSKI CENTAR SOCIJALNOG RADA

Lucija Švec

PERSPEKTIVA UČENIKA SREDNJIH ŠKOLA O KORIŠTENJU INTERNETA I DRUŠTVENIH MREŽA

DIPLOMSKI RAD

Zagreb, 2022.

SVEUČILIŠTE U ZAGREBU

PRAVNI FAKULTET

STUDIJSKI CENTAR SOCIJALNOG RADA

Diplomski sveučilišni studij socijalnog rada

Lucija Švec

PERSPEKTIVA UČENIKA SREDNJIH ŠKOLA O KORIŠTENJU INTERNETA I DRUŠTVENIH MREŽA

DIPLOMSKI RAD

Ime i prezime mentora: izv. prof. dr. sc. Lucija Vejmelka

Zagreb, 2022.

Sadržaj

Perspektiva učenika srednje škole o korištenju interneta i društvenih mreža

Sažetak:

Korištenje interneta čini svakodnevicu učenika srednjih škola, a najviše vremena provode na društvenim mrežama. Na društvenim mrežama imaju otvorene profile koje koriste za komunikaciju s drugim osobama kao i za dijeljenje raznog sadržaja. Kako bi mogli ostali sigurni tijekom korištenja interneta moraju imati dovoljno znanja i vještina na koji način zaštititi svoje podatke i privatnost na internetu. Cilj ovog diplomskog rada bio je dobiti uvid u doživljaj srednjoškolaca na području Splitsko-dalmatinske županije o korištenju interneta i društvenih mreža, posebice područja sigurnosti, privatnosti i komunikacije na internetu. U ovom kvalitativnom istraživanju sudjelovao je 21 učenik, a podaci su prikupljeni putem fokus grupa. Prvim istraživačkim pitanjem htjelo se doznati kako srednjoškolci opisuju komunikaciju u online okruženju. Sudionici su navodili s kojim se s sve izazovima susreću prilikom online komunikacije te su istaknuli kako im je teže prepoznati sarkazam, ironiju, humor te pravo značenje poslane poruke. Drugo istraživačko pitanje ispituje kako srednjoškolci opisuju sigurnost i privatnost na internetu te kako osiguravaju vlastitu sigurnost i privatnost na internetu. Dobiveni rezultati su pokazali kako se srednjoškolci smatraju sigurnim korisnicima interneta te da su svjesni svih rizika koje njegovo korištenje nosi. Svakako su upoznati s načinima kako se zaštititi u online okruženju i većina ih koristi. Trećim istraživačkim pitanjem ispituju su izazovi koje srednjoškolci prepoznaju prilikom ostvarivanja sigurnosti i privatnosti na internetu. Srednjoškolci su navodili kako se susreću s prijetnjama, vrijeđanjem, lažnim profilima, ali i da su svjesni digitalnog traga koji ostaje prilikom korištenja interneta.

Ključne riječi: korištenje interneta, društvene mreže, srednjoškolci, sigurnost i privatnost, online komunikacija

The perspective of high school students on the use of the Internet and social networks

Abstract:

The use of the Internet makes up the everyday life of high school students, and they spend most of their time on social networks. They have open profiles on social networks that they use to communicate with other people as well as to share various content. In order to stay safe while using the Internet, they must have sufficient knowledge and skills on how to protect their data and privacy on the Internet. The aim of this thesis was to gain insight into the experience of high school students in the Split-Dalmatia County regarding the use of the Internet and social networks, especially in the areas of security, privacy and communication on the Internet. 21 students participated in this qualitative research, and the data was collected through focus groups. The first research question sought to find out how high school students describe communication in the online environment. The participants mentioned the challenges they face when communicating online and pointed out that it is more difficult for them to recognize sarcasm, irony, humor and the true meaning of the sent message. The second research question examines how high school students describe safety and privacy on the Internet and how they ensure their own safety and privacy on the Internet. The obtained results showed that high school students are considered safe Internet users and that they are aware of all the risks that its use entails. They are certainly familiar with ways to protect themselves in the online environment and most use them. The third research question examines the challenges that high school students recognize when achieving security and privacy on the Internet. High school students stated that they encounter threats, insults, fake profiles, but also that they are aware of the digital trail that is left when using the Internet.

Key words: using of Internet, social networks, high school students, saftey and privacy on the Internet, online communication

Izjava o izvornosti

Ja, Lucija Švec (ime i prezime studenta/ice) pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica diplomskog rada te da u radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova te da se prilikom izrade rada nisam koristio/-la drugim izvorima do onih navedenih u radu.

Ime i prezime: Lucija Švec v.r.

Datum: 30.09.2022.

1. Uvod

Internet je globalna mreža koja omogućuje korisnicima da budu u stalnom međusobnom kontaktu. **Korištenje interneta i virtualna komunikacija „sastavni su dio svakodnevnog života mladih koji ga rabe u razne svrhe“ (Vejmelka i sur., 2017.), a prema Državnom zavodu za statistiku (2016.) korisnici interneta najviše su mladi od 16 do 24 godina.** Internet koriste za pretraživanje raznih informacija koje su im potrebne za obrazovanje, no većinu vremena provode na društvenim mrežama. „Društvene mreže postale su iznimno popularni servisi, privlačeći milijune pa i stotine milijuna korisnika“ (Kušić, 2010.). **Društvene mreže promijenile su način komuniciranja te su mladi više okrenuti online komuniciranju putem poruka nego razgovoru licem u lice. Prema istraživanju Flander i sur. (2020.) srednjoškolci najviše koriste društvene mreže**. Njih 42,3% koristi društvene mreže od 1 do 3 sata dnevno, 31,2% od 3 do 5 sati, a 7,8% njih više od 9 sati dnevno. Studenti su također populacija mladih koji najviše vremena provode na društvenim mrežama kao i srednjoškolci. Trećina studenta Hrvatskih studija u Zagrebu posveti do dva sata, odnosno više od dva sata dnevno društvenim mrežama, a tek 10% njih 15 do 30 minuta (Rakić, 2020.). **Što se tiče društvenih mreža najviše koriste YouTube (98%), Instagram (92,4%), WhatsAppom (88,8%) te Facebookom (42,2%) (Flander i sur., 2020.)**. No, svakodnevno korištenje interneta ima svoje prednosti i nedostatke, a posebno za djecu i mlade. U navedenim istraživanjima, djeca i mladi naveli su za što koriste Internet i to predstavlja prednosti koje nudi Internet poput dostupnosti informacija, zabave, komunikacije s prijateljima, gledanja filmova i slušanja glazbe (Flander i sur., 2020., Rakić, 2020**.). S druge strane javljaju se i brojni nedostaci koji mogu utjecati na sam razvoj djece i mladih. Istraživanja su pokazala koliko vremena djeca i mladi provode u online svijetu i to može dovesti do rizika ovisnosti, nasilja, cyberbullinga, ali i do narušavanja privatnosti i sigurnosti na internetu (Livingstone, 2008.). Veliki rizik sigurnosti i privatnost na internetu stvara zaštita privatnih sadržaja koja može biti narušena zbog mogućnosti krađe podataka ili hakiranja, ali i objavljivanja osobnih podataka javnosti za koje „društvene mreže nisu sigurno mjesto“** (Miliša i sur., 2009.).

Stoga, u ovom radu osvrnut ću se na razvoj interneta, definiranje online komunikacije te sigurnosti i privatnosti na internetu. Nadalje prikazat ću rezultate kvalitativnog istraživanja na srednjoškolcima o tome kako opisuju komunikaciju u online okruženju, sigurnost i privatnost na internetu te s kojim izazovima se susreću prilikom osiguravanje iste.

1.1. Razvoj i značaj Interneta za današnjicu

Internet je velika računalna mreža putem koje se međusobno razmjenjuju informacije. Danas, širom svijeta više od 5 milijardi ljudi koristi Internet i uvelike je oblikovao svakodnevni život današnjeg svijeta.[1] Internet je omogućio emitiranje diljem svijeta te postao mehanizam za dijeljenje informacija i interakciju između pojedinca i njihovih računala bez obzira na geografski položaj (Leiner i sur., 2009.). No, razvoj interneta seže u daleku prošlost.

Razvoj interneta prati se od 1950-ih do ranih godina 21. stoljeća. Na njegov razvoj utjecaj su imale razne društvene i tehnološke transformacije, a potporu razvoju dala je Agencija za napredne istraživačke projekte Ministarstva obrane Sjedinjenih Američkih Država (SAD). Stoga, možemo reći da je razvoj interneta potekao iz SAD-a. Povijest interneta započela je 1960-ih godina u Sjedinjenim Američkim Državama za vrijeme hladnog rata (Cohen-Almagor, 2013., prema Luppicini, 2013.). Tijekom tog razdoblja razvila se mreža pod nazivom ARPANET. Mrežom ARPANET željela se postići razmjena podataka između znanstvenika vojnoindustrijskih kompleksa diljem SAD-a. Tada su spojena dva računala, a kasnijih godina su se nastavilo umreživati ostala računala. Uz razvoj ARPANET-a, istodobno razvijale su se druge računalne mreže, što se u konačnici spojilo u jednu globalnu mrežu pod nazivom Internet.[2] Spajanje različitih računalnih mreža omogućilo je stvaranje učinkovite mreže koja se zove Internet i danas (Keefer i Baiget, 2001). Internet je nastavio svoj rast i izvan Sjedinjenih Država ranih sedamdesetih, a 1992. godine je postojalo milijun umreženih računala diljem svijeta. Stoga, osnovana je organizacija pod nazivom „Internet Society“ prema kojoj je Internet dobar za društvo i čovječanstvo. Ubrzo nakon toga Internet je ušao u svakodnevni život ljudi, a u tome je pomoglo i uspostavljanje World Wide Weba, odnosno WWW-a početkom dvadesetih godina 20. stoljeća. WWW servis je omogućio da se Internet koristi u različite svrhe, ne

[1] Worldometers (2022). *Društvo i mediji: Korisnika interneta u svijetu.* Posjećeno 14.06.2022. na mrežnoj stranici Wordometers: https://www.worldometers.info/hr/

[2] Nacionalni portal za učenje na daljinu „Nikola Tesla“. *Uvod u Internet: Krataka povijest Interneta.* Posjećeno 14.6.2022. na mrežnoj stranci Nacionalnog portala za učenje na daljinu „Nikola Tesla“: https://tesla.carnet.hr/mod/book/view.php?id=5428&chapterid=883

samo za razmjenu podataka u poslovanju nego i kao medij koji mogu koristiti sve dobne skupine kroz objavljivanje fotografija, prodaju i nabavu proizvoda, komunikaciju i u novije vrijeme za društvene mreže.[3]

Internet kao globalna mreža dostupna je diljem svijeta te je promijenila svakodnevni život pojedinaca koji ga koriste. Posebno je promijenila i unaprijedila način komuniciranja, čime je Internet postao medij koji prevladava u odnosu na komunikaciju licem u lice. Za sve što je potrebno u životu sada se koristi Internet (Dentzel, 2013.). Internet se uklopio u svakodnevni život te postao sveprisutan u poslovnom svijetu, u školama, sveučilištima, zdravstvu i ostalim dimenzijama koje utječu na život. Ljudi ga koriste u različite svrhe poput surfanja za informacije, igranje online igara ili komunikaciju putem raznih aplikacija i društvenih mreža. Internet može utjecati na svakodnevni život pojedinca kroz bežično povezivanje, odnosno kroz mogućnost pristupa internetu bilo gdje i bilo kada dok je u pokretu. Osim toga, može se stvoriti i digitalni jaz s obzirom na socioekonomski status prema onima koji koriste i onima koji ne koriste Internet (Wellman, 2002.). Najveću promjenu je donio u području komuniciranja gdje je „olakšava brzu razmjenu velikih količina podataka, razmjenu trenutnih poruka, povratne informacije, priloženi tekst, sliku i glas“ (Wellman, 2002:5). Također, pojedinac ima kontrolu s kime će komunicirati, od koga primati poruke, kada i o čemu. To znači da omogućava individualnu prilagodbu s obzirom na korisnikove preferencije. Randall (2001.) je opisao način komuniciranja na internetu kao „komunikaciju koja će biti posvuda , ali budući da ne neovisna o mjestu, neće biti nigdje smještena“ (Randall, 2001:5).

1.2. Cyberprostor

Cyberprostor javlja se za vrijeme dva desetljeća, od ranih 80-ih do prvih nekoliko godina dvadeset i prvog stoljeća. Tijekom ovog razdoblja razvili su se pojmovi kibernetičkog prostora, ali i drugi cyber pojmovi poput cyber kriminala, *cyber bullinga* i slično. Cyberprostor je prikazan kao „virtualna, nefizička mreža pomoću koje su korisnici međusobno komunicirali korištenjem računalnih tehnologija“ (Lupton, 2014.:39).

[3] Ibid.

Također, cyberprostor definiran je kao „virtualno okruženje koje ne postoji u bilo kojem fizičkom obliku, već je složeno okruženje ili prostor koji je rezultat razvoja interneta, uz ljude, organizacije i aktivnosti na svim vrstama tehnoloških uređenja i mreža koji su spojeni na njega (International Organization for Standardization [ISO]. (2012). Pisac W. Gibson 1984. godine u romanu „Neuromancer“ osmislio je izraz *cyberspace* na hrvatskom cyberprostor te ga je opisao kao „vidljivu površinu ili sučelje virtualnog svijeta“. Smatrao je kako u cyberprostoru korisnici žive zamjenski putem svojih avatara i percipiraju iluziju kao stvarnost (Gibson, 1984., prema Greer, 2019.). Stoga, na samom početku, sastojao se od nečijeg digitalnog avatara koji je potpuno odvojen od materijalnog svijeta (Lupton, 2014.). Prema tome, avatar je stanovnik virtualnog svijeta, odnosno on omogućava korisniku da se susretne sa virtualnim svijetom. Njegov zadatak je da posreduje u našem doživljavanju virtualnog svijeta, ali i komunikaciji s drugim ljudima. Avatar se registrira unutar sustava te čini radnje korisnika vidljivima. Pomoću avatara korisnik doživljava virtualni svijet, odnosno podržavaju osjećaj prisutnosti u zajedničkom prostoru (Girvan, 2018.).

Uz Gibsona, različiti autori dali su definicije cyberprostora ozbirom na njihova shvaćanja. Prema Mishri (2016.) cyberprostor je „domena koju karakterizira korištenje međusobno povezanih računala za olakšavanje komunikacije u stvarnom vremenu“ (Mishra, 2016., prema Panwar, 2016.:127). Sličnu definiciju dali su i Gangwar i Narang (2022.) te opisali cyberprostor kao „okruženje stvoreno vezama opipljivog poput računala, nematerijalnog poput aplikacija i usluga te mreža poput interneta i komunikacije“. Iako je cyberprostor apstraktan pojam, može se opisati i kao globalna mreža koja ujedinjuje telekomunikacijske mreže i sustave računalne obrade kako bi korisnici cyberprostora doživjeli novo iskustvo tijekom interakcije, razmjene ideja i dijeljenja informacija (Ionescu, 2014.). Mnogi od autora povezuju cyberprostor s Internetom, stoga su opisali cyberprostor kao „virtualni ili digitalni prostor izgrađen od informacijske strukture koju pružaju globalne mreže kao što je Internet“ (Corrêa, 2019., prema Oliveira, 2019.). Greenberg (2008.) navodi da je cyberprostor postao sinonim za Internet i/ili svjetski web (Greenberg, 2008.).

U konačnici možemo reći da je cyberprostor „međuovisna mreža infrastruktura informacijske tehnologije koja uključuje Internet, telekomunikacijske mreže, računalne

sustave te ugrađene procesore i kontrolore“ (Injac i Šendelj, 2017.). Prema klasifikaciji navedenih autora možemo vidjeti kako Internet ima veliku ulogu u cyberprostoru i čini njegovu veliku cjelinu. Sama definicija cyberprostora važna je jer daje uvid u to kako je nastao internet i koju ulogu internet ima u tom prostoru. Pomoću nje može se objasniti kako informacije putuju internetom i gdje se nalaze prilikom korištenja interneta kao sustava.

1.3. Komunikacija na internetu

Komunikacija na internetu pripada u suvremene oblike komunikacije koja je uvelike promijenila interakciju s drugim ljudima. Sa sobom je donijela mnoge prednosti koje korisnici koriste u svakodnevnom životu, omogućila je komunikaciju s ljudima na drugom kraju svijeta, ali i brzu svakodnevnu interakciju s ljudima koji se ne nalaze u neposrednoj blizini (Skelac, 2015.). Stoga, internetska komunikacija je komunikacija koja se „provodi putem društvenih mreža i različitih platformi koje postoje na internetu“. Korisnici društvenih mreža u provedenim istraživanjima ističu kao razloge korištenja društvenih mreža komunikaciju s prijateljima koje poznaju uživo (90,6%), upoznavanje novih ljudi i dopisivanje s drugima (Flander i sur., 2020; Ciboci i sur., 2020; Machimbarrena i sur., 2018.).

Komunikacija na internetu temelji se na dvije vrste komunikacije, a to su sinkrona i asinkrona komunikacija. Asinkrona komunikacija se ne odvija u realnom vremenu, nego postoji vrijeme kašnjenja između poslanih poruka. Često se online komunikacija odvija na asinkron način, gdje primatelj poruke s odgodom odgovara na poruku koju je primio. Ukoliko osoba s kojom je osoba u interakciji putem društvene mreže odgovara s odgodom na poruku, tada se radi o asinkronoj komunikaciji (AlJeraisy i sur., 2015.). Komunikacija može započeti bez da je druga osoba aktivna, stoga je asinkrona komunikacija najpopularniji oblik online komunikacije jer osobe koje žele razgovarati ne moraju biti na istom mjestu ili državi (Cavus i Bicen, 2009.). Neki od oblika su društvene mreže, elektronička pošta, blogovi i slično.

S druge strane, Paraprotnik (2007.) sinkronu komunikaciju definira kao oblik komunikacije koji se odvija sad i ovdje, odnosno pošiljatelj i primatelj poruke su aktivni na društvenoj

mreži ili drugoj stranici za dopisivanje te šalju i primaju poruke bez kašnjenja. Za razliku od asinkrone komunikacije, tijekom sinkrone komunikacije obje osobe su istovremeno prisutne na mediju i komuniciraju porukom za porukom, kao da razgovaraju govorom licem u lice (Paraprotnik, 2007.). Tijekom sinkrone komunikacije osobe mogu komunicirati jedan na jedan ili u grupi putem „Instant Messaging" aplikacija te audio i video poziva.

1.3.1. Korištenje slikovnih sadržaja u online komunikaciji

Tijekom online komunikacije mladi koriste specifične nove riječi, izraze i znakove kako bi olakšali mrežnu komunikaciju. Dugogodišnje korištenje specifičnih izraza ukorijenilo se u online komunikaciji te su prepoznatljivi svim korisnicima društvenih mreža. Mladi žele što brže i sa što manje napora komunicirati. Stoga se odlučuju za korištenje raznih kratica za riječi ili skupine riječi, posvojili su brojne engleske riječi u hrvatski jezik koje se osim u online komunikaciji koriste i u komunikaciji licem u lice. Javlja se i gubljenje samoglasnika iz riječi, poput „nezz", „pozz", „fkt" i slično. To su obilježja neformalne komunikacije koju mladi često koriste na internetu. Osobe s kojima komuniciraju ih razumiju te komunikacija između njih teče glatko (Kanaet, 2015.).

Kako bi se upotpunilo značenje pisane poruke koje korisnici šalju posežu za dodacima, odnosno za emotikonima ili smajlićima kojima mogu postići bolje razumijevanje poslane poruke. Oni su dio neverbalne komunikacije koja ima veliku ulogu u online komunikaciji. U pisanoj komunikaciji, neverbalna komunikacija ponekad u potpunosti nedostaje pa se upotpunjuje putem slikovnih znakova i simbola (Slelac, 2015.). Rezabek i Cochenour (1998.) definirali su emotikone kao „vizualne znakove formirane od običnih tipografskih simbola koji kada ih se čita predstavljaju osjećaje ili emocije" (Rezabek i Cochenour, 1998. prema Walther i D'addario, 2001.). Emotikoni prikazuju izraze lica, samim time i raspoloženje sudionika interakcije. Oni omogućavaju način kako treba razumjeti poruku, stoga ih i mladi pretežito koriste u svojoj komunikaciji (Herring i Androutsopoulos, 2015.).

Walther i D'addario (2001.) testirali su kako emotikoni utječu na interpretaciju poruka. Rezultati su pokazali kako emotikoni u online komunikaciji izazivaju slične učinke kao i

neverbalni znakovi u komunikaciji licem u lice. Isto je potvrdilo i istraživanje provedeno na srednjoškolcima u Nizozemskoj, gdje su rezultati pokazali kako emotikoni utječu na interpretaciju poruka, odnosno da jačaju intenzitet poslane verbalne poruke. Samim time, autori su zaključili kako emotikoni imaju iste funkcije kao i neverbalna komunikacija (Derks i sur., 2008.).

Korištenje emotikona može pomoći kod nerazumijevanja poruka koje se šalju, poput sarkazma i ironije. Tijekom komunikacije uživo, oni se lako prepoznaju po načinu govora, no u pisanoj komunikaciji to je puno teže. Korištenjem sarkazma tijekom dopisivanja, pošiljatelj ostavlja otvorenu mogućnost da primatelj doslovno protumači poruku bez saznanja da se radi o sarkazmu. U tom slučaju, korištenje emotikona moglo bi pomoći da se sarkastični komentar lakše prepozna (Filik i sur., 2016.). Rezultati istraživanja Walthera i D'addaria (2001.) pokazali su kako su ispitanici povezali „mig" sa sarkazmom u 85% slučajeva. No, to ne znači da je isključivo „mig" zaslužan za prepoznavanje sarkazma, sarkazam su prepoznavali i putem pozitivne poruke s osmijehom.

Prema Kanaet (2015.) mladi često koriste strane riječi u svakodnevnoj mrežnoj komunikaciji, ali i skraćenice koje im olakšavaju komunikaciju jer su brži u pisanju poruka. Također, rezultati su pokazali da aktivno koriste i emotikone, odnosno 98,5% studenta, 96,2% srednjoškolaca te 97,7% osnovnoškolaca. Navode kako ih koriste svakodnevno tijekom neformalne komunikacije.

Zaključno, korištenje slikovnih znakova u komunikaciji na internetu posebno je zanimljiva kao nadopuna razumijevanju napisane poruke. Uz slikovne znakove mladi koriste i druge načine kako bi ubrzali svoju komunikaciju i učinili je što efikasnijom.

1.4. Mladi na internetu

Razvoj novih tehnologija i samog interneta doveo je do promjene u svakodnevnom životu svih dobnih skupina, no posebno je utjecao na socijalizaciju, odrastanje i razvoj mladih, od kojih su neki od rođenja dio Internet svijeta. Potočnik (2007.) navodi kako je razvoj tehnologije i interneta utjecao na „smjer i sadržaj socijalizacije mladih" (Potočnik, 2007., prema Ilišin, i Radin, 2007:107). Internet koriste sve generacije, a posebno su u

fokusu generacija Z i generacija Alfa. Generaciju Z obuhvaćaju mladi rođeni od 1996. godine pa nadalje. To su ljudi koji su u dobi između 7 i 24 godine života te su dosegli dob mlađih odraslih osoba (Rupčić, 2021.). Generaciju Alfa čine djeca i mladi rođeni na križanju generacije Z i novog doba. Za njih je karakteristično da se rađaju u digitalnom okruženju, odnosno da je tehnologija dio njihovog svakodnevnog života (Tootell i sur., 2014.). Mladi većinu vremena tijekom dana provode online, odnosno na internetu. Istraživanje provedeno na učenicima osnovne i srednje škole u Španjolskoj ispitivalo je što mladi rade na internetu? Rezultati za učenike u dobi od 11 do 21 godine pokazali su da njih 90% ima vlastiti mobitel, od kojih 70% ima pristup internetu putem mobilnog uređaja. Što se tiče korištenja interneta putem računala, 96,4% njih ima računalo, a 98,9% njih pristup internetu. Većina učenika navode kako Internet koriste malo, odnosno od 1-2 sata dnevno (67,1%). S obzirom na spol, djevojke su te koje više vremena provode online od mladića. Ispitanici najviše Internet koriste za pretraživanje informacija, komunikaciju, igranje igrica i društvene mreže (Giménez i sur., 2017.).

Istraživanja provedena na hrvatskim učenicima u osnovnim i srednjim školama, kao i na studentima pokazala su slične rezultate. Prema rezultatima istraživanja kojeg su proveli Ciboci i sur. tijekom 2017. godine pokazali su kako većina djece u dobi od 9 do 17 godina ima mogućnost pristupa internetu te da mu najčešće pristupaju kod kuće. Hrvatski učenici također posjeduju mobitele, odnosno pametne telefone (82,4%) u dobi do 9 do 11 godina, dok čak 99,1% njih u dobi od 15 do 17 godina. Istraživanje je pokazalo da u hrvatskoj djeca i mladi provode više do četiri sata dnevno na internetu tijekom tjedna, no ta se brojka povisuje tijekom vikenda (Ciboci i sur., 2020.). Istovjetni rezultati dobiveni su tijekom istraživanja učenika u Dubrovniku o korištenju Interneta, bez obzira posjeduju li računalo ili ne, znaju koristiti Internet. Što se tiče učestalosti spajanja na Internet, njih 65,32% svakodnevno se spaja na Internet do se 9,46% ispitanika ne spaja na Internet (Kunić i sur., 2017.).

Zagrebački osnovnoškolci svaki dan pristupaju internetu (oko 68%), od toga najviše nekoliko puta dnevno, njih 37,5%. Što se tiče vremena provedenog na internetu, njih 35,6% u prosjeku provodi do jednog sata dnevno na internetu, a oko četvrtine ispitanih tri ili više sata dnevno (Nikodem i sur., 2014.). Razlozi spajanja na Internet osnovnoškolaca su glazba

i filmovi kao i komunikacija na društvenim mrežama, a najčešće koriste Facebook ili neki drugu društvenu mrežu za dopisivanje s prijateljima (69%) te za zabavu i igranje računalnih igara (Nikodem i sur., 2014.; Kunić i sur., 2017.). Jednake razloge za korištenje društvenih mreža imaju i srednjoškolci koji navode da ih koriste za komunikaciju s prijateljima, zatim za opuštanje i zabavu te za saznavanje novih informacija koje ih zanimaju. Studenti imaju otvorene profile na društvenim mrežama, svi ispitani imaju otvoren Facebook profil, a više od 80% njih ima i Instagram profil. Prema popularnosti, najviše studenata Hrvatskih studija u Zagrebu koristi Instagram (58%), a nakon toga Facebook (39%) (Rakić, 2020.). Prema učestalosti korištenja društvenih mreža koje mladi koriste u Hrvatskoj na prvom mjestu je YouTube, zatim Instagram, Facebook, WhatsApp, Snapchat te TikTok (Vejmelka i sur., 2022., Matković i sur., 2021.). Važan dobiveni rezultat je prosječan broj prijatelja na društvenim mrežama, prema istraživanju Matković i Vejmelke (2021.) učenici prosječno imaju 357 prijatelja na društvenoj mreži koju najviše koriste, a prosječno 79 prijatelja koje poznaju u stvarnom životu. Takvi rezultati pokazuju rizike za komunikaciju s nepoznatim ljudima, kao i narušavanje sigurnosti i privatnosti na internetu među mladim osobama.

Preliminarni rezultati deSHAME istraživanja u Hrvatskoj provedenog na učenicima u 20 županija i gradu Zagrebu pokazali su zastrašujuće brojke o tome koliko su djeca rizična skupina na internetu. Istraživanje je provedeno tijekom pandemije COVID-19 u Hrvatskoj. Samim time, djeca i mladi postali su učestali korisnici interneta. Rezultati su pokazali kako 26% njih na provodi na internetu više vremena nego prije pandemije, 22% puno više nego prije pandemije, dok 28% njih u jednakoj mjeri kao i prije pandemije (Vejmelka i sur., 2022.). Slične odgovore davali su i učenici tijekom 2021. godine kada su procjenjivali vlastito vrijeme korištenja interneta za vrijeme pandemije. Prema njihovim odgovorima 43,81% učenika koristi Internet više nego prije, a 42,86% se mnogo više koristi nego prije pandemije, dok za 11,9% učenika nema razlike u odnosu na prije pandemije (Matković i Vejmelka, 2021.). Što se tiče rodnih razlika kod učenika srednjih škola, djevojke češće procjenjuju da provode više vremena u online aktivnostima prije pandemije (Matković i sur., 2021.).

Mladi na internetu se suočavaju s raznim rizičnim ponašanjima, ono što se istaknulo su rizična online seksualna ponašanja. Rezultati su pokazali kako gotovo 40% mladih

izjavljuje kako je primilo sadržaje seksualne tematike od njima poznatih osoba, ali i od nepoznatih. Ono što je zabrinjavajuće da 10% učenika šalje vlastite seksualne sadržaje drugima, dok 4% njih ih šalje nepoznatim osobama. Kao razloge navodili su da su to učinili zbog ucjene i prijetnje, na nagovor druge osobe, dok je 5% mladih nepoznatim osobama svojevoljno poslalo takav sadržaj. Više od 90% mladih je svjedočilo seksualnom uznemiravanju na internetu, kroz objavljivanje golih slika, pogrdnih riječi, vrijeđanje, lažne profile i lažna predstavljanja. No, kada se pojavi takav problem, rijetko uključuju odrasle osobe u rješavanje istog. Najčešće sami rješavaju problem te uz vršnjačku podršku (Vejmelka i sur., 2022.).

Rezultati dosadašnjih istraživanja pokazuju da mladi veliki dio dana provode na internetu, posebno na društvenim mrežama te se suočavaju s raznim rizicima zbog kojih trebaju biti oprezni, posebno oko dijeljenja podataka kako ne bi došlo do zlouporabe istih.

1.5. Sigurnost i privatnost na internetu

Sigurnost i privatnost na internetu predstavljaju jednu od najizazovnijih tema u online svijetu. Tijekom korištenja novih tehnologija koje obuhvaćaju Internet, javljaju se novi problemi koji se tiču sigurnosti i privatnosti. Potrebno je osigurati privatnost ljudi na internetu kako bi se zaštitio njihov identitet kao i osobni podaci (Mayer, 2009.). Pojedini pristupi nisu usuglasili praksu o povezanosti sigurnosti i privatnosti ili o potpunom odvajanju ta dva pojma. Pfleeger (1988.) smatrao je kako su aspekti privatnosti neraskidivo povezani s računalnom sigurnošću. No, u okviru ovog ulomka odvojeno ću definirati ova dva aspekta.

Sigurnost na internetu vodi se pod različitim terminima, od računalne sigurnosti, mrežne sigurnosti, informacijske sigurnosti ili cyber sigurnosti. Svaka od njih se definira na drugačiji način. Povezujući cyberprostor i cyber sigurnost, cybersigurnost se odnosi na „aktivnosti koje stranke s interesom trebaju poduzimati kako bi uspostavile i održale sigurnost u cyberprostpru“ (ISO, 2012.). Prema međunarodnom standardu ISO/IEC 27032:2012 informacijska sigurnost se bavi „zaštitom tajnosti, privatnosti, cjelovitosti i dostupnosti informacija u cjelini kako bi služila potrebama odgovarajućeg korisnika informacija“ (ISO, 2012.). Dok, prema Zakonu o informacijskoj sigurnosti ona se definira

kao stanje „povjerljivosti, cjelovitosti i raspoloživosti podataka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda“.

U online svijetu korisnici putem svojih društvenih mreža iznose svoje osobne podatke, kako putem objavljivanja tako i putem komunikacije s drugim korisnicima kada nisu ni svjesni koliko su podataka otkrili. Iako postoje brojne sigurnosne postavke i postavke zaštite privatnosti, brojni korisnici ne uspijevaju u potpunosti zaštititi svoje osobne podatke od neželjenih pristupa (Raad i Chbeir, 2013.). Kada su korisnici izmijenili svoje zadane postavke privatnosti, samo u 39% slučajeva to odgovara očekivanjima, što pokazuje da čak i korisnici koji su svjesni privatnosti imaju poteškoća tijekom ispravnog upravljanja i održavanja njihovih postavki privatnosti (Lui i sur., 2011.). Stoga, privatnost uključuje „prikrivanje osobnih podataka kao i mogućnost kontrole onoga što se događa s tim informacijama“ (Gürses i sur., 2006.). Sami korisnici imaju mogućnost regulirati postavke privatnosti, zaštititi se od neželjenih upada i krađe osobnih podataka, odnosno očuvati svoju privatnost na internetu, a posebno na društvenim mrežama (Elmendili i sur., 2018.).

Do kršenja privatnosti najčešće dokazi tijekom korištenja društvenih mreža. To uključuje neželjene kontakte, hakiranje, krađu identiteta, dijeljenje neželjenog sadržaja te pristup trećih osoba društvenim mrežama drugih osoba, odnosno njihovim osobnim podacima (Debatin i sur., 2009.). Istraživanje Debatin i sur. na uzorku 119 američkih mladih osoba pokazalo da je 18% njih izjavilo da je imalo negativna iskustva s zaštitom privatnosti na društvenoj mreži Facebook, a to su uhođenje i uznemiravanje, tračevi ili krađa podataka (Debatin i sur., 2009:93). Osim navedenih prijetnji, mladi se suočavaju i s lažnim profilima na društvenim mrežama koji pokazuju nisku razinu privatnosti. Istraživanje provedeno na srednjoškolcima u Zagrebu i Čakovcu pokazalo je da je gotovo 50% učenika poigravalo s vlastitim lažnim predstavljanjem (Perić i sur., 2021.). U neobjavljenom istraživanju na osnovnoškolcima i srednjoškolcima rezultati su pokazali da je 23,1% ispitanika također lažno predstavljalo na internetu (Varga, 2011.). Rezultati istraživanja koje se bavilo temom privatnosti na društvenim mrežama, a posebno postavkama privatnosti na društvenoj mreži Facebook pokazali su da postavke privatnosti odgovaraju očekivanjima korisnika samo u 37% vremena i gotovo uvijek korisnici sadržaj izlažu većem broju korisnika nego to

očekuju (Lui i sur., 2011.). Slične rezultate pokazalo je i istraživanje provedeno na 232. mlade osobe u dobi od 18 do 35 godina gdje više od pola ispitanika (56%) smatra da je dovoljno upoznato s postavkama privatnosti na Facebooku. Njih 18% smatra da su u potpunosti upoznati s postavkama, dok 25% njih se izjasnilo da su nedovoljno upoznati s postavkama privatnosti na Facebooku (Borovac, 2014.). Prema istraživanju Matković i sur. (2021.) na osnovnoškolcima i srednjoškolcima, 91,9% osnovnoškolaca navodi da zna koristiti sigurnosne postavke na društvenim mrežama, no iako znaju ne koriste ih svi, stoga 79% njih koristi sigurnosne postavke na društvenim mrežama. Javni profili dostupni su u 17,6% osnovnih škola te su djevojčice te koje značajnije koriste sigurnosne postavke u odnosu na dječake. Nešto više srednjoškolaca (96,5%) zna koristi sigurnosne postavke, a 88% ih zaista koristi na svojim društvenim mrežama. Za razliku od osnovnoškolaca, dječaci su ti koji imaju češće javne profile. U odnosu na prvi val istog istraživanja provedenog 2017. godine, drugi val je pokazao porast poznavanja sigurnosnih postavki među učenicima osnovnih i srednjih škola (Matković i sur., 2021.). Studenti također paze na sigurnosne postavke na društvenim mrežama gdje imaju kreirane profile, njih 85% potvrđuje da zna koristiti sigurnosne postavke (Matković i sur., 2020.).

Izazovno je štititi privatnost korisnika na društvenim mrežama jer su osobni podaci široko dostupni unutar online svijeta. Tome doprinose i saznanja kako sami korisnici nisu stručnjaci za postavljanje postavki privatnosti na društvenim mrežama gdje se najviše krši privatnost. Zbog toga je potrebno stvoriti bolje postavke privatnosti kako bi se ojačala privatnost korisnika, njihovih osobnih podataka i odnosa koje su uspostavili u virtualnom svijetu.

1.5.1. Načini zaštite privatnosti na internetu

Svaki korisnik interneta ima mogućnost osigurati svoju privatnost kroz postavke privatnosti koje može sam postaviti na društvenim mrežama. Samozaštita temelji se na tome da korisnici razmisle prije objavljivanja osobnih i povjerljivih informacija, poput imena i prezimena, e-mail adrese, telefona, adrese stanovanja i brojnih drugih podataka koji bi ih mogli lako identificirati. To se odnosi i na objavljivanje fotografija ili videozapisa, označavanje drugih osoba na fotografijama, kao i na označavanje lokacije

gdje se trenutno netko nalazi.[4] U anketi provedenoj za potrebe pisanja završnog rada na 100 ispitanika, rezultati su pokazali kako su najzastupljeniji odgovori ponekad i često, odnosno 33% ispitanika ponekad, a 31% njih označuje bliske osobe i prijatelje na objavama na društvenim mrežama. Time se može ugroziti njihova privatnost u slučaju krađe podataka (Bolšec, 2021.).

Nadalje, privatnost se može zaštititi načinom prijavljivanja u račune preko društvene mreže. Europska Komisija (2019.) savjetuje kako treba pripaziti tijekom prijava na internetu. Potrebno je biti oprezan s upisivanjem osobnih podataka tijekom prijave i ukoliko je moguće, sigurnije je odabrati mogućnost kreiranja novog računa na stranici na koju se prijavljuje. Društvene mreže temelje se na virtualnim prijateljima, ali i na onima koje poznajemo i u stvarnom životu. No, potrebno je razmisliti prije prihvaćanja zahtjeva za prijateljstvom poznajemo li tu osobu i uživo i je li profil stvaran ili možda lažan. Najčešće se događaju zlouporabe na način da se izmisli ime i postavi slika profila koja je primamljiva drugim korisnicima. Na takav način se brzo uspostavlja komunikacija s nepoznatim ljudima na internetu. Istraživanje provedeno 2014. godine o privatnosti na društvenoj mreži Facebook pokazalo je kako većina ispitanika prihvaća prijatelje koje dobro poznaju (39,9%) i poznanike, 41,3%. Što znači da više od 2/3 ispitanika prihvaća za prijatelje samo osobe koje zna u stvarnom životu (Borovac, 2014.). Odnosno, 57% ispitanika se izjasnilo da nikad ne prihvaća zahtjeve od stranaca, a 33% njih je odgovorilo da rijetko prihvaća zahtjeve stranaca. To pokazuje kako mlade osobe koji su bili sudionici ovog istraživanja zaštićuju svoju privatnost na način da ne prihvaćaju zahtjeve za prijateljstvo za koje nisu sigurni da ih poznaju u stvarnom životu (Bolšec, 2021.).

Očuvanje zaštite privatnosti postiže se i korištenjem adekvatnih lozinki, odnosno snažnih zaporaka koje je teško otkriti. Prilikom registracije na pojedinu društvenu mrežu ili stranicu potrebno je odabrati korisničko ime i lozinku. Kako bi se zaštitilo od zloporabe profila, potrebno je redovito mijenjati postavljene lozinke, obično svaki mjesec ili nekoliko puta

[4] Europska komisija, predstavništvo u Hrvatskoj (2019). *Zaštitite svoju privatnost na društvenim mrežama*, Posjećeno 16.06.2022. na mrežnoj stranici Europske komisije: https://croatia.representation.ec.europa.eu/index_hr

mjesečno. Zloporaba se može dogoditi ako druga osoba sazna nečiju lozinku te joj nanese štetu u online svijetu (Varga, 2011.). Stoga, kako bi se osobni podaci zaštitili „bilo bi dobro da se koriste što složenije lozinke“ (Bolšec, 2021.). Lozinka koja je dovoljno jaka trebala bi sadržavati minimalno sedam znakova, kombinaciju velikih i malih slova, brojeva te znakova. Važno je da ta lozinka ne bude javno dostupna kako ne bi došlo do krađe postavljene lozinke (Varga, 2011.). Prema istraživanju koje je provela Bolšec (2021.) pitanja koja su vezana uz lozinke ispitanici su odgovorili kako njih 51% ne koristi istu lozinku za više društvenih mreža, dok njih 48% to radi. Što se tiče forme same lozinke, lozinke 98% ispitanika imaju više od 6 znakova, 75% ispitanika u lozinkama imaju uključena velika i mala slova, a 60% njih brojeve, znakove i simbole. Istraživanje provedeno u među ispitanicima Medicinske škole, rezultati pokazuju kako mladi korisnici imaju lozinke bolje kvalitete. Njih 36,9% odgovorilo je kako da je izričito važno periodično mijenjanje lozinka, doke je 22,8% njih odgovorilo kako rijetko koristi različite zaporke za različite internetske usluge (Vojnović, 2017).

Očuvanje privatnosti se „usredotočuje se na zaštitu osjetljivih informacija prvenstveno korištenjem tehnika kao skrivanje korisničkih identiteta i modificiranja podataka“ (Raad i Chbeir, 2013.). No i dalje je potrebno informirati o načinima zaštite privatnosti, što govore i ispitanici istraživanja, njih 94% smatra kako je to svakako potrebno, a posebno za mlade ljude (Bolšec, 2021.). Stoga, važno je naučiti načine zaštite privatnosti na internetu kako bi se kao korisnici osjećali sigurnije. Nakon što se postave postavke koje osiguravaju sigurnost i privatnost na internetu, potrebno je educirati se o novim postavkama sigurnosti i privatnosti na internetu te ih koristiti na način koji omogućava najvišu razinu zaštite. Prikaz dosadašnjih istraživanja o sigurnosti i privatnosti na internetu, a posebno na društvenim mrežama pokazuje kako djeca i mladi često nisu svjesni opasnosti s kojima se mogu suočiti tijekom korištenja interneta. Kako bi se smanjila mogućnost dovođenja u takvu situaciju, potrebno je informirati djecu i mlade o svim štetnim posljedicama te načinima kako da zaštite svoje podatke. Kako bi to bilo učinkovito, potrebno ih je educirati prije samog otvaranja profila na društvenim mrežama (Matković i sur., 2020.).

1.6. Elektroničko nasilje

Tijekom korištenja interneta mogu se pojaviti rizici, a to su napadi od strane zlonamjerne osobe. Djeca i mladi se mogu susresti s nasiljem na internetom koje obuhvaća povrede u obliku uznemirujućih i prijetećih poruka, poticanja mržnje, daljnjeg vršnjačkog nasilja, vrijeđanja, širenja lažnih informacije i uvrjedljivih komentara te osobnih podataka (Varga, 2011.).

Navedena ponašanja pripadaju pod pojam elektroničkog nasilja ili *cyberbullinga*. *Cyberbulling* je engleski naziv za elektroničko nasilje, odnosno nasilje preko interneta. Definira se kao „agresivan, namjeran čin koji predvodi grupa ili pojedinac, koristeći elektroničke oblike kontakata, više puta i tijekom vremena protiv žrtve koja se ne može lako sama obraniti sama“ (Olweus, 1993., prema Smith i sur., 2008.:376). Pri definiranju elektroničkog nasilja Hinduja i Patchin (2015.) vode se „kriterijima klasičnog vršnjačkog nasilja, kao opetovanog i namjernog nanošenja štete drugima posredstvom digitalnih tehnologija i elektroničkih uz prisutnu neravnotežu snaga između pojedinca koji čini i onoga tko je žrtva nasilja“. Znanje mladih o nasilju na internetu pokazalo je istraživanje provedeno na 180 mladih osoba, gdje je većina iskazala kako točno zna što je *cyberbulling*, njih 73%, 24% zna otprilike, a samo 4 mladih ne zna što je nasilje na internetu. Među maloljetnicima njih 71% točno zna značenje pojma, dok je kod punoljetnih osoba taj broj veći, odnosno 74%. Mladi (97%) prepoznaju *cyberbulling* prema tvrdnjama ako što su „širenje laži ili objavljivanje fotografija koje za cilj ima osramotiti nekoga na društvenim mrežama te u tvrdnji slanje pogrdnih poruka ili prijetnji putem platformi za dopisivanje“ (Opačić i sur., 2021.). Dosadašnja istraživanja provedena na temu *cyberbullinga* pokazala su kako je određeni broj djece i mladih imalo iskustva s nasiljem na internetu. Ciboci i sur. (2020.) su otkrili da je tijekom 2017. godine u Republici Hrvatskoj 7% djece u dobi do 9 do 17 godina imalo iskustva s nasiljem na internetu, točnije da se netko prema njima ponašao na povrjeđujući ili neugodan način. Također, istraživanje je pokazao kako su elektroničkom nasilju više izložena starija djeca, 11,8% djece u dobi od 15 do 17 godina (Ciboci i sur., 2020.). Analizirajući slučajeve iz Centra Luka Ritz, autorice Divić i Jolić (2019.) saznale su kako je svako četvrto dijete imalo iskustvo *cyberbullinga* (25,8%), a iskustvo doživljaja nekog oblika elektroničkog nasilja prisutno je u 21,3% slučajeva. Takve

rezultate pokazuju i naredna dva istraživanja, gdje su ispitanici potvrdili da ju bili žrtve nasilja na internetu, neki od njih jednom (17%), a neki i više puta (13%) (Opačić i sur., 2021., Bolšec, 2021.). Što se tiče oblika elektroničkog zlostavljanja među vršnjacima koje se javlja prema analizi dokumentacije slučajeva rizičnih ponašanja djece i mladih u virtualnom okruženju korisnika Centra Luka Ritz, ispitanici su naveli 31,7% njih da je to slanje ružnih poruka ili slika drugima, dok njih 27% smatra je najčešći oblik nasilja nasilje putem interneta među vršnjacima (Divić i Jolić, 2019.).

Istraživanje Vejmelke i sur. (2016.) ispitalo je rizična ponašanja adolescenata u online okruženju. Rezultati su pokazali kako postoje razlike među mladima koji su uključeni u nasilničko ponašanje na internetu, s obzirom na uloge sudjelovanja u istome. Prema tome, 11,7% adolescenata doživljava nasilje, 11,5% njih provodi nasilnička ponašanja, 27,5% istovremeno čini i doživljava takva ponašanja, dok 49,3% adolescenata ne sudjeluje u takvim ponašanjima na internetu. Što se tiče razlike u spolu, rezultati su pokazali kako nema razlike u čestini sudjelovanja u činjenju nasilja na internetu. Istraživanjem promatrana je i povezanost između online aktivnosti i elektroničkog nasilja te se češće doživljavanje nasilja na internetu povezuje s duljim vremenom provedenim igrajući igre i upotrebom društvenih mreža. Rezultati su pokazali neznačajnu povezanost između uporabe društvenih mreža i činjenja elektroničkog nasilja među mladima, no pojava nasilja javlja se među mladima koji igraju online igrice. Umjesto uporabe društvenih mreža za činjenje nasilja, adolescenti više koriste *instant* poruke koje koriste za nasilnička ponašanja. S obzirom na razinu ovisnosti o internetu i činjenju i doživljavanju nasilja, rezultati su pokazali značajne razlike ovisno o stupnju ovisnosti o internetu. Tako, mladi koji pokazuju blagu, umjerenu ili visoku razinu ovisnosti češće čine nasilje na internetu od mladih koji ne pokazuju znakove ovisnosti o internetu (Vejmelka i sur., 2016.). Tijekom 2020. godine Vejmelka i Matković provele su kvantitativno istraživanje na studentima o problematičnom korištenju interneta tijekom pandemije Covid-19. Rezultati su pokazali kako 78,08% ispitanika nije sudjelovalo u činjenju i doživljavanju elektroničkog nasilja. No, sukladno istraživanju iz 2016. (Vejmelka i sur.) i ovim istraživanjem se pokazalo kako postoje različite uloge u činjenju i doživljavanju elektroničkog nasilja. Također, istovjetni rezultati dobiveni su kod rodnih razlika u činjenju i doživljavanju elektroničkog nasilja te

čestini provođenja vremena u raznim online aktivnostima i doživljavanju online nasilja (Vjemelka i sur., 2016., Vejmelka i Matković, 2021.). Što se tiče elektroničkog nasilja tijekom pandemije Covid-19, više od jedne četvrtine ispitanika bilo je počinitelj ili žrtva online nasilja, njih 12,75% bile su žrtve, 5,7% njih našlo se u ulozi počinitelja, dok je istovremeno 8,3% ispitanika doživljavalo i činilo nasilje na internetu (Vejmelka i Matković, 2021.).

Razlikujemo dvije vrste elektroničkog nasilja, a to su „izravan ili direktan napad i napad preko posrednika ili indirektan napad" (Batori i Ćurin, 2020.:105). Tijekom direktnog napada nasilnik izravno vrši nasilje nad žrtvom, a indirektan napad ima posrednika, odnosno drugu osobu koja za nasilnika vrši napad. (Batori i Ćurin, 2020.). Uz navedeno napadi se vrše na način da se uznemiruje osobu u virtualnoj grupi ili pojedinačno.

Willard (2007.) razlikuje nekoliko vrsta nasilja putem interneta, a to su vrijeđanje, uznemiravanje, ogovaranje i klevetanje te isključivanje. Vrijeđanje obuhvaća korištenje vulgaran rječnik, uvrede i prijetnje kako bi se ponizila druga osoba. Uznemiravanje je nasilje koje traje u kontinuitetu gdje nasilnik konstantno šalje uvredljive i neprijateljske poruke. Ogovaranje i klevetanje odnosi se na objavljivanje lažnih izjava na internetu, uvredljivih informacija kako bi se ugrozila reputacija druge osobe. Isključivanje je postupak kada se namjerno izbacuje osobu iz online grupe. Navedene vrste nasilja naveli su i ispitanici koji su imali iskustva s elektroničkim nasiljem. Divić i Jolić (2019.) saznale su kako je socijalno isključivanje doživjelo svako četvrto dijete (21,3%), ogovaranje i klevetu (13,1%,), a 9,8% uznemiravanje i uhođenje. Sa ovim rezultatima poklapaju se i rezultati istraživanja Cibocija i sur. (2020.) koji pokazuju da se najčešće iskustvo elektroničkog nasilja odnosilo na „primanje povrjeđujućih ili neprimjernih poruka (61%), zatim isključivanje iz grupe ili aktivnosti (33%) te objavljivanje i prenošenje povrjeđujućih poruka tamo gdje ih drugi mogu vidjeti" (Ciboci i sur., 2020.:24).

Počinitelji nasilja na internetu se najčešće nalaze u okolini žrtve te mogu biti njemu bliske osobe. Mladi koji su doživjeli nasilje navode kako su nasilnici bili učenici iz razreda (60%) ili iz drugog razreda u istoj školi (31%). No, nasilje čine i bliski prijatelji uz one osobe koje im nisu toliko bliske (Opačić i sur., 2021.).

Elektroničko nasilje ostavlja posljedice za same žrtve, a nedostatak sigurnosti na internetu dovodi do toga da se i samo nasilje događa.

2. Teorijsko polazište istraživanja

Teorijsko polazište na kojem planiram temeljiti rezultate provedenog istraživanja je teorija planiranog ponašanja. Korištena je za potpunije razumijevanje istraživanog fenomena. Ajzen (1991.) razvio je teoriju planiranog ponašanja koja služi za predviđanje i razumijevanje ljudskog ponašanja. Sama teorija je proširena teorija razložne akcije koja je ograničena stupnjem kontrole nad ponašanjem. Važnu ulogu u teoriji ima namjera ponašanja, koju određuju tri elementa, a to su: stavovi prema specifičnom ponašanju, subjektivna norma i percipirana kontrola ponašanja. Stav prema specifičnom ponašanju „odnosi se na stupanj do kojeg osoba ima povoljnu ili nepovoljnu procjenu ili ocjenu ponašanja o kojem je riječ“ (Ajzen, 1991.;188). Subjektivna norma „odnosi se na percipirani društveni pritisak da se izvede ili ne izvede ponašanje“ (Ajzen, 1991.;188). Dok se percipirana kontrola ponašanja odnosi na percipiranu lakoću ili poteškoću izvođenja ponašanja, odnosno koliko kontrole ima osoba nad time hoće li ili neće izvršiti ponašanje. Što osoba ima veću namjeru to je veća vjerojatnost da će doći do ostvarenja određenog ponašanja. Kako bi se namjera realizirala kroz ponašanje, ponašanje mora biti pod voljnom kontrolom. Pri tome, prema teoriji planiranog ponašanja ponašanje je zajednička funkcija namjere i percipirane kontrole ponašanja. Točno predviđanje ponašanja omogućeno samo ako su ispunjeni određeni uvjeti. Na samom početku to su namjera i percipirana kontrola ponašanja koji moraju biti u skladu s ponašanjem koje se predviđa (Ajzen, 1991.). Kada bismo željeli predvidjeti hoće li korištenje interneta kod mladih osoba biti rizično, tada bismo prvo trebali procijeniti namjeru da li će to biti rizično ponašanje ili neće te percipiranu kontrolu nad tim ponašanjem. Zatim, da bi se točno predvidjelo ponašanje komponente, namjera i percipirana kontrola ponašanja moraju ostati stabilne u intervalu između procjene i promatranja ponašanja. Posljednji uvjet koji mora biti ispunjen kako bi se točno predvidjelo ponašanje odnosi se na percipiranu kontrolu ponašanja, odnosno sama kontrola mora odražavati realnu kontrolu (Ajzen, 1991.). No, sama teorija je proširena novom varijablom, a to je da su stavovi određeni uvjerenjima o ponašanju. Uvjerenja o

ponašanju odnose se na posljedice istraživanog ponašanja, kao i na procjenu tih posljedica, odnosno ako korisnik interneta smatra da je njegovo korištenje pravilno, da je osigurao privatnost kroz zaštitu podataka na internetu imat će pozitivne stavove i neće se osjećati nesigurno dok će koristiti Internet. No, ako korisnik ima razmišljanja kako nije u potpunosti zaštitio svoje podatke i da postoji mogućnost zlouporabe kroz podatke ili fotografije, tada će imati negativne stavove prema korištenju interneta i biti će više na oprezu. Uz uvjerenja o ponašanju, teorija je proširena kroz subjektivnu normu, odnosno subjektivna norma je određena normativnim injunktivnim i normativnim deskriptivnim uvjerenjima. Normativno injunktivna uvjerenja odnose se na to što važne osobe u okruženju druge osobe očekuju u pogledu istraživanog ponašanja, a normativno deskriptivna uvjerenja odnosi se na želje pojedinca da se ponašaju u skladu s očekivanjima njima važnih osoba. Uz to, percipirana kontrola ponašanja proširena je kontrolnim uvjerenjima koji obuhvaćaju prisutnost čimbenika koji mogu otežati ili olakšati ostvarenje ponašanja te snagu kontrolnih čimbenika koja se odnosi na to koliki utjecaj imaju ti čimbenici na ostvarenje ponašanja. Ajzen (1991.;206) smatra kako „stavovi prema ponašanju, subjektivne norme u odnosu na ponašanje i percipirana kontrola nad ponašanjem obično predviđaju namjere ponašanja s visokim stupnjem točnosti“. Također, namjera, percepcija kontrole ponašanja, stav prema ponašanju i subjektivna norma otkrivaju drugačiji aspekt ponašanja i on može poslužiti da se potakne promjena ponašanja (Ajzen, 1991.). Stoga, teorija planiranog ponašanja može dati znanstveni doprinos za preventivne intervencije i implikacije za budući rad.

3. Cilj i istraživačka pitanja

Cilj ovog istraživanje je dobiti uvid u doživljaj srednjoškolaca na području Splitsko-dalmatinske županije o korištenju interneta i društvenih mreža, posebice područja sigurnosti, privatnosti i komunikacije na internetu.
Na temelju definiranog cilja postavljena su sljedeća istraživačka pitanja:

1. Kako srednjoškolci opisuju komunikaciju putem online okruženja?
2. Kako srednjoškolci opisuju sigurnost i privatnost na internetu i na koji način osiguravaju vlastitu sigurnost i privatnost na internetu?

3. Koje izazove srednjoškolci prepoznaju prilikom ostvarivanja vlastite sigurnosti i privatnosti na internetu?

4. Metoda

U skladu sa ciljem istraživanje odabran je kvalitativni pristup prikupljanja i analize prikupljenih podataka. Za prikupljanje podataka koristile su se fokus grupe, a pri analizi prikupljenih odgovora koristila sam tematsku analizu.

4.1. Sudionici

Prilikom odabira sudionika koristio se kriterijski namjerni uzorak. Odabrana ciljana populacija su učenici trećeg razreda srednjih škola s područja Splitsko-dalmatinske županije. Broj sudionika je 21, od čega 18 djevojaka i 3 mladića. Prosječna dob sudionika je 17 godina, a 18 učenika pohađa treći razred srednjih škola, dok 3 učenice pohađaju četvrti razred srednje škole. Sudionici pohađaju Zdravstvenu školu, Ekonomsku i upravnu školu, Školu likovnih umjetnosti, Turističku školu i Jezičnu gimnaziju u Splitu. Za učenike o kojima imamo informacije o mjestu stanovanja, dvije učenice su s otoka, četiri učenika/ce dolaze iz manjih gradova kao što su Trilj, Sinj, Kaštela, iz manjih mjesta su tri učenika/ce, dok pet učenika/ce dokaze iz Splita. Kriteriji odabira sudionika su institucije koje žele sudjelovati te učenici koji žele sudjelovati.

4.2. Postupak prikupljanja podataka

Služba za mentalno zdravlja Nastavnog zavoda za javno zdravstvo Splitsko dalmatinske županije provela je kvalitativno istraživanje u studenom i prosincu 2021. godine. Prikupljanje podataka provedeno je u okviru obrazovnih institucija, točnije Zdravstvene škole, Ekonomske i upravne škole i Ženskog đačkog doma Split. Metoda prikupljanja podataka koja se koristila je fokus grupa. Fokus grupe „su posebna tehnika grupnog razgovora koja za cilj ima dublje spoznavanje istraživanje pojave“ (Milas, 2005.). Također, fokusne grupe možemo definirati kao intervjue sa grupama koje se okupljaju u određenom prostoru, a sudionici međusobno razgovaraju oko relevantne teme istraživanja (Perecman i Curran, 2006.). Do sada se provelo tri vala kvantitativnih istraživanja na ovu temu i sakupljeno je dovoljno podataka na području Splitsko-dalmatinske županije o

korištenju interneta te se željelo fokusnim grupama dobiti nove informacije od samih sudionika koje nisu još znanstveno utvrđene. Istraživanje je provedeno u suradnji s obrazovnim institucijama. Stručni suradnici odabrali su učenike, a učenici su odlučili žele li sudjelovati u istraživanju. Sudionici odabrani su po navedenim kriterijima za odabir.

Za provođenje istraživanja tražile su se dozvole i suglasnosti, Suglasnost upravnog odjela za provedbu istraživanja, kulturu, tehničku kulturu i sport Splitsko dalmatinske županije, odobrenje nacrta istraživanja Etičkog povjerenstva Nastavnog zavoda za javno zdravstvo, ali i pisano odobrenje ravnatelja/ice da se kvalitativno istraživanje može provesti u okviru institucije.

Prilikom provođenja istraživanja poštovale su se smjernice Etičkog kodeksa u istraživanju s djecom, što u našem konkretnom slučaju znači da su roditelji informirani kako će njihova djeca sudjelovati u fokus grupama i da je sudjelovanje za djecu bilo **dobrovoljno.** U informiranom pristanku nalaze se sve potrebne informacije o provedbi istraživanja s kojim su upoznati sudionici fokus grupa, te oni imaju mogućnost odustati u svakom trenutku od istraživanja. Za prikupljanje informiranog pristanka roditelja i suglasnosti učenika korišteni su standardni školski obrasci koji su ostali u školama kao dio njihove dokumentacije. U svim dokumentima je navedeno da će se susreti snimati, za što je prethodno zatraženo odobrenje od sudionika, da će snimke poslužiti samo za transkripte, a uvid u transkripte imali su samo istraživači.

Provedeno je 10 fokus grupa u trajanju od 45 minuta do sat vremena i 30 minuta u prostorijama doma i škola.

4.3. Mjerni instrumenti

Na početku susreta učenici su usmeno upoznati sa svrhom i ciljem istraživanja. Prikupljanje općih podataka o sudionicima provedeno je na početku fokus grupa gdje su učenici zamoljeni da kažu nešto o sebi. Tematske cjeline koje su se obrađivale tijekom fokus grupa su vrijeme koje mladi provode na internetu, na ekranima, na društvenim mrežama, odnosno kompulzivno korištenje interneta, zatim sadržaji na internetu te komunikacija na internetu, odnosno sigurnost i nasilje na internetu. Voditelj fokus grupa postavljao je potpitanja, saturacija podataka.

Pitanja za provođenje fokus grupa osmišljena su unaprijed s obzirom na teme te se nalaze u prilogu 5.

4.4.Obrada podataka

Za obradu podataka ovog istraživanja korištena je tematska analiza. Tematska analiza obuhvaća analizu glavnih tema pronađenih u kvalitativnim istraživanjima. Prema Braun i Clarke (2006.) tematska analiza je proces identificiranja, analiziranja i izvještavanja prema tzv. obrascima (temama) koje se prepoznaju unutar podataka. Tijekom tematske analize korištena je deskriptivna metoda koja se temelji na doživljajima, iskustvima i mišljenju ispitanika. Analiza se temeljila na induktivnoj analizi, odnosno „odozdo prema gore". Prema induktivnom pristupu identificirane teme su povezane s podacima koji su dobiveni od samih ispitanika (Patton, 1990., prema Braun i Clarke, 2006.) Kako su podaci prikupljeni putem fokus grupa, identificirane teme povezane su s konkretnim pitanjima koji su bili postavljeni sudionicima fokus grupa. Stoga, induktivna analiza je „proces kodiranja podataka bez pokušaja da ih se uklopi u prethodno postojeći okvir kodiranja" (Braun i Clarke, 2006.:83).

Tematska analiza sastoji se od 6 faza, koje su korištene i tijekom ove obrade podataka. Prvi korak obuhvaćao je upoznavanje sa podacima, odnosno čitanje podataka i zapisivanje početnih ideja. Zatim je slijedilo generiranje početnih kodova gdje su se kodirali zanimljive značajke podataka na sustavan način, uspoređujući podatke koji su relevantni kod. Treća faza bila je traženje tema, odnosno razvrstavanje kodova u potencijalne teme te prikupljanje svih podataka koji su relevantni za svaku temu. Četvrta faza bila je analiza dobivenih tema, provjera preklapanja te postoje li podteme kao i potkrepljuju li podaci u potpunosti formulirane teme. Peta faza obuhvaćala je završno definiranje tema i šesta faza pisanja izvještaja o rezultatima istraživanja. Sama analiza uključuje stalno kretanje natrag i naprijed između odabranih podataka, kodova i definiranih tema (Braun i Clarke, 2006.).

5. Rezultati istraživanja i rasprava

U nastavku slijedi prikaz rezultata istraživanja prema postavljenim istraživačkim pitanjima. Rezultati su prikazani kroz tematska područja koja se odnose na opis

komunikacije putem online okruženja, doživljaj sigurnosti i privatnost na internetu, kao i na načine na koje srednjoškolci osiguravaju vlastitu sigurnost i privatnost na internetu te koje izazove prepoznaju prilikom ostvarivanja vlastite sigurnosti i privatnosti na internetu. Također, prikazat će se i rasprava o istima.

5.1. Kako srednjoškolci opisuju komunikaciju putem online okruženja?

Prvim istraživačkim pitanjem htjelo se saznati kako srednjoškolci opisuju komunikaciju putem online okruženja, odnosno s čime se srednjoškolci susreću kada komuniciraju putem online okruženja. Komunikacija putem online okruženja obuhvaća dvije teme (vidjeti *Tablicu 5.1.*): 1) Izazovi tijekom online komunikacije, 2) Načini razgovora tijekom online komunikacije.

Tablica 5.1. *Komunikacija putem online okruženja*

TEMA	**KATEGORIJE**
Izazovi tijekom online komunikacije	Poteškoće u izražavanju emocija u online komunikaciji Mogućnost jednostavnijeg lažiranja emocija Teže je prepoznati sarkazam i ironiju Teže je prepoznati humor Nedostatak neverbalne komunikacije Razlike u značenju poruke Izjednačavanje online komunikacije i komunikacije uživo Virtualna dezinhibicija
Načini razgovora tijekom online komunikacije	Razgovor kroz gifove Korištenje slikovnih sadržaja u online komunikaciji Korištenje slang-a Korištenje drugačijeg vokabulara Korištenje internih fora

Izazovi tijekom online komunikacije

Sudionici opisuju komunikaciju putem online okruženja kroz izazove s kojima se susreću u odnosu na komunikaciju uživo, Na samom početku sudionici naveli su da imaju

poteškoće u izražavanju emocija u online komunikaciji, što je potkrijepljeno izjavom: *„Ako se posvađam s nekim, lakše mi je uživo vidjeti je li toj osobi stvarno žao ili nije. Ovako samo reče: oprosti i makne se. (...); ne znam kako izražavati emocije, ajmo reći* (UČ9)". Usporedno s poteškoćama u izražavanju emocija, sudionici navode kako je putem online komunikacije postoji **mogućnost jednostavnijeg lažiranja emocija**: „*Pa ovo virtualno može više biti lažno. Nitko ne može svoje osjećaje toliko dobro prenijeti kao što bi uživo prema nekome, ne znam* (UČ10)". Sudionici navode kako im je **teže prepoznati sarkazam i ironiju***: „Meni je problem komunikacije što ne znam je li nešto sarkazam (...); jel ironija kada netko nešto napiše* (UČ11)". Uz sarkazam i ironiju, sudionici navode da **teže prepoznaju humor:** „(…) *Ili ako se smije, napiše hahahaha ne znam je li to smijeh ili je to više* (…); *(...) Ne znaš je li mislila više iz zezancije ili je mislila ozbiljno. Što je uopće mislila, koji je to odgovor* (UČ11)".

Nadalje, sudionici navode **nedostatak neverbalne komunikacije:** „*Jer nema tona pa ne znaš što je osoba zapravo mislila pod tom porukom (UČ11)"*. Nedostatak neverbalnih znakova također ima posljedice na interpretaciju poruke, kao što je i sudionik istraživanja primijetio. Samim time dolazi do **razlika u značenju poruke:** *„Da, na primjer dvije iste poruke: Jesi li normalna? – to može biti nešto skroz ozbiljno. I jesi li normalna i ☺, to je kao šala* (UČ20)".

Pojedini sudionici istraživanja **izjednačavaju online komunikaciju i komunikaciju uživo:** „*Meni je komunikacija apsolutno ista* (UČ21); *Da, meni isto. Poruke šaljem i onda uživo samo nastavim* (UČ18)". No, sudionici smatraju da dolazi do **virtualne dezinhibicije:** „*Neke stvari se uživo bojimo reći, ajmo reći na neki način, kad smo preko poruka, onda dobijemo neki vjetar u leđa, neku hrabrost i onda ćeš preko poruka reći tko zna što, i onda opet uživo…* (UČ15)" .

Ovakvi rezultati u skladu su s dosadašnjim istraživanjima u kojima se pokazalo kako se javljaju izazovi u online komunikaciji. To su potvrdili i Shannon i Weaver (1949) koji navode da je prvi izazov online komunikacije točno prenošenje simbola komunikacije, a zatim koliko osoba koja je primatelj poruke može protumačiti dobivene simbole (Shannon i Weaver, 1949., prema Best i sur., 2014.). Posebno je teško ispravno razumjeti sarkazam

i ironiju zbog odsutnosti obilježja koja se koriste u komunikaciji licem u lice, kao što su ton glasa i izraz lica. Stoga, eksperiment koji su proveli Filik i sur., (2016) na doslovnim i sarkastičnim komentarima pokazao je kako su doslovni komentari ocijenjeni sarkastičniji kada su popraćeni emotikonom nego bez njih. Nasuprot tome, sarkastični komentari nisu ocijenjeni kao sarkastičniji kada je emotikon bio prisutan u odnosu na odsutan. Nadalje, Walther i D'addario (2001.) proveli su eksperiment kojim su rezultati pokazali kako emotikoni imaju ograničeni utjecaj na interpretaciju poruka. Nastavno na njihov eksperiment, Derks i sur., (2008.) svojom studijom pokazali su kako emotikoni utječu na tumačenje online poruka. Njihova studija je otkrila kako su emotikoni korisni u jačanju intenziteta poruke te da se pozitivna poruka s osmijehom ocjenjuje pozitivnije od pozitivne čiste poruke. Dobiveni rezultati provedenog istraživanja u skladu su s istraživanjem (Derksa i sur., 2008., Filka i sur., 2016., Walther i D'addario 2001.). Prema navodima srednjoškolaca primijećeno je kako se u njihovoj online komunikaciji javljaju situacije koje spadaju u virtualnu dezinhibicijau, koja je prema nalazima Sulera (2004.) zaslužna za otvoreniju, manje suzdržaniju i opuštenu komunikaciju (Suler, 2004., prema Vejmelka, 2020.).

Načini razgovora tijekom online komunikacije

Srednjoškolci izjavljuju kako su svoju komunikaciju u online okruženju prilagodili sebi i svojem načinu izražavanja kroz različite načine komuniciranja. Sudionici istraživanja navode kako **razgovaraju kroz gifove:** „*Ja sa prijateljicom pričam kroz gifove* (UČ19)", **koriste slikovni sadržaj u online komunikaciji:** „(…) *da se mi možemo dopisivati preko stickera* (UČ18); *Slali bi tako te smajliće i naljepnice …* (UČ19)". Uz to, među srednjoškolcima popularno je **korištenje slang-a**, no sudionicima istraživanja se takav način komunikacije u online okruženju ne sviđa. Navode kako: „*„a e".. to mi je tako nepristojno, kao da me se hoće skinut s dnevnog reda* (UČ15); *Ja mrzim taj glupi slang: štae, kakoe* (UČ21)". Također, primjećuju promjene kod osoba s kojima razgovaraju uživo i u online okruženju, pa tako navode **korištenje drugačijeg vokabulara:** „*Mene živcira kada netko piše književno a govori drugačije, ili obrnuto* (UČ15); *Neke osobe kao da su drugačije iza mobitela. Koriste drugačiji vokabular i ne znam* (UČ11)". Srednjoškolci navode kako svakodnevno **koriste interne fore** u komunikaciji međusobno: „(…) mi

imamo toliko tih internih fora, (…) i *mi ono umiremo, gušimo se od smijeha a nitko drugi ništa ne razumije* (UČ18)".

Izmjenjivanje poruka putem simbola kod srednjoškolaca preraslo je u korištenje naprednijih načina komunikacije koje uvelike upotpunjuju napisanu poruku. To potvrđuju i istraživanja koja pokazuju kako mladi koriste u komunikaciji na društvenim mrežama koriste izraze na engleskom jeziku, kao i skraćenice koje samo oni međusobno razumiju (Popović, 2012.,). Istraživanje provedeno na mladima pokazalo je kako 67,8% sudionika komunicira putem slanja glasovnih poruka, slanjem tekstualnog sadržaja (69,4%), slanjem gifova (63,4%), što je istovjetno dobivenim rezultatima za potrebe ovog rada (Valenti, 2021.). Istraživanje provedeno na studentima, srednjoškolcima i osnovnoškolcima pokazalo je kako 98,5% studenata, 69,2% srednjoškolca te 97,7% osnovnoškolaca koristi emotikone u online komunikaciji (Kanaet, 2015.).

5.2. Kako srednjoškolci opisuju sigurnost i privatnost na internetu i na koji način osiguravaju vlastitu sigurnost i privatnost na internetu?

Drugim istraživačkim pitanjima htjelo se saznati kako srednjoškolci opisuju sigurnost i privatnost na internetu te na koji način osiguravaju vlastitu sigurnost i privatnost na internetu. Zbog same preglednosti rada podijelit će se ovo istraživačko pitanje na dva dijela. Sigurnost i privatnost na internetu obuhvaća tri teme (vidjeti *Tablicu 5.2.*): 1) Doživljaj sigurnosti, 2) Dozvole prilikom korištenja interneta te 3) Doživljaj privatnosti.

Tablica 5.2. *Sigurnost i privatnost na internetu*

TEMA	KATEGORIJE
Doživljaj sigurnosti	Sigurnost izjednačavaju sa privatnosti Osjećaj anonimnosti Promišljeno ponašanje u online okruženju Smatraju da sigurno koriste Internet Posjedovanje znanja o sigurnosti na internetu Razlozi zbog kojih ne upotrebljavaju znanje o sigurnosti na internetu Prihvaćanje poznatih osoba kao prijatelja na društvenim mrežama

	Mogućnost izbora prilikom ponašanja u online okruženju Izjednačavanje sigurnosti na internetu sa zaštitom osobnih podataka
Dozvole prilikom korištenja interneta	Korištenje kolačića kao postavke sigurnosti Davanje dopuštenja Imaju javne profile na društvenim mrežama Korištenje privatnih profila na društvenim mrežama
Doživljaj privatnosti	Znaju definirati privatnost na internetu Znaju koji su privatni podaci na internetu Svijest o riziku objave različitih sadržaja Javni karakter interneta

Doživljaj sigurnosti

Kroz temu **doživljaj sigurnosti** sudionici su opisali kako oni doživljavaju sigurnost na internetu. Mnogi od njih su prilikom definiranja sigurnosti na internetu **sigurnost izjednačili sa privatnosti.** Sudionici navode: „(…) *a sigurnost je način kako ćemo zaštiti svoju privatnost* (UČ2); *Sigurnost i privatnost mogu ići zajedno jer ako je privatnost ugrožena, možemo reći i da je sigurnost ugrožena* (UČ6); *Sigurnost je sposobnost da nitko ne vidi našu privatnost* (UČ11)". Stoga, možemo zaključiti kako srednjoškolci smatraju da su sigurnost i privatnost povezane, što i sami navode: „*Povezano je, da. Preko tih lozinki. Naša privatnost je povezana sa tom sigurnosti…* (UČ18); *Ja mislim da su sigurnost i privatnost zapravo jako povezani* (UČ20)". Svoj doživljaj sigurnosti sudionici su povezali s **osjećajem anonimnosti**, odnosno da ako nitko ne zna za njih na internetu da su oni sigurni, „*Pa da se osjećam sigurno i da znam da mi nitko ne može nauditi.* (UČ9); *Sigurnost je da mi znamo da neće nitko ući u te slike* (UČ11)". Nadalje, sudionici sigurnost na internetu potvrđuju kroz **promišljeno ponašanje u online okruženju**. Samim time, smatraju da su sigurni na internetu i da im se ništa loše ne može dogoditi, što potvrđuju i izjavama: „(…) *Zato ja govorim da sam sigurna, jer razmišljam o svojim postupcima na internetu, razmišljam u šta ću uć, u šta neću uć.* (…) (UČ20); *Da, ako mi se javi netko koga ne znam, razmišljat ću jesmo li se možda negdje sreli, što želi. ili Ako mi pošalje zahtjev, razmišljat ću je li znam tu osobu ili ne* (UČ2)". Nastavno na promišljeno ponašanje u

online okruženju, sudionici su kroz razgovor rekli kako **smatraju da sigurno koriste Internet**, odnosno: *„(...)osjećam se sigurno na onim stranicama što ja znam, što koristim.* (UČ13); *Smatram da mi nitko neće ukrasti moje slike, ne vidim razlog zašto bi nekome trebala moja slika…Prati mi profil samo prijatelji* (UČ7)". S obzirom na godine sudionika, do sada su imali prilike čuti o sigurnosti na internetu, stoga su svojim izjavama dali do znanja da **posjeduju znanja o sigurnosti na internetu:** „*Ne znamo sve, ali mislim da dosta toga znamo.* (UČ8); *Većinu znamo* (UČ6)". No i dalje, postoje oni koji se ne pridržavaju naučenih stvari vezanih uz sigurnost na internetu te su se pojavili **razlozi zbog kojih ne upotrebljavaju znanje o sigurnosti na internetu**, a to su: „*(...) ali da ne obraćaju toliko pozornost.* (UČ11); *Ne razmišljaju o sigurnosti zbog trenutačnog užitka* (UČ12)". Kako bi zaštitili svoju sigurnost na internetu, srednjoškolci **prihvaćaju poznate osobe kao prijatelje na društvenim mrežama**. Kažu: „*(...) prihvaćam prijatelje koje ja želim, koje znam (...) (*UČ18); *(...) Kao prvo, na Instagramu prihvaćam samo osobe koje znam i s kojima sam dobra* (UČ7)". Nadalje, smatraju kako imaju **mogućnost izbora prilikom ponašanja u online okruženju,** odnosno da „*. Ti biraš sam što ćeš stavljati na svoje mreže i kako ćeš se ponašati (...) Mislim da naš pristup internetu je točno onako kako mi želimo, kako mi razmišljamo, kako mi gledamo na to (...) Svatko ima legitimno pravo da radi što želi* (UČ20)". Pri razmišljaju o sigurnosti na internetu, srednjoškolci su **sigurnost na internetu izjednačili s zaštitom osobnih podataka,** odnosno smatraju kako: „*Ono, ne bojim se za svoj život. da će netko moje podatke uzimati. u tom smislu* (UČ2); *Sigurnost podrazumijeva da nitko ne ukrade podatke, broj mobitela (...)* (UČ7); *Da se naši osobni podaci ne dijele bez našeg dopuštenja* (UČ8)".

Mnogi se osjećaju sigurno na internetu jer se promišljeno ponašaju u online okruženju te posjeduju znanja o sigurnosti na internetu (Leko, 2019.) dok neki navode kako se ne osjećaju sigurno zbog rizika koji se mogu pojaviti prilikom korištenja interneta. No, autorica Löfgren-Mårtenson (2008) navodi kako su mladi svjesni rizika kada su izloženi na internetu. Kako bi se smanjili mogući rizici, mladi na internetu posežu za onime što im je dobro poznato, kao što je prihvaćanje njima poznate osobe na društvenim mrežama. Brojna dosadašnja istraživanja potvrdila su ove dobivene rezultate. Autor Kušić (2010) navodi kako 92,7% učenika odabire prijatelje na Facebooku na temelju poznanstva u

stvarnom životu, što je potvrđeno i u istraživanjima (Leko, 2019., Ciboci i sur., 2020., Divić i Jolić, 2019., Lough i Fisher, 2016., Matković i Vejmelka, 2021.). Što se tiče zaštite osobnih podataka, istraživanje provedeno na učenicima srednjih škola kroz pitanje o brzi za dostupnost osobnih podataka na društvenoj mreži Facebook pokazalo je kako 36,8% učenika brine i štiti svoje osobne podatke dok 32,1% to ne čini (Bračko, 2022.).

Dozvole prilikom korištenja interneta

Sudionici istraživanja su se prilikom opisivanja sigurnosti i privatnosti na Internetu osvrnuli na dozvole koje je javljaju prilikom korištenja interneta. Ono što su primijetili da se javljaju **kolačići kao postavke sigurnosti.** Smatraju kako sami kolačići nisu sigurni te da mogu naštetiti njihovim osobnim podacima.

Sve stranice i aplikacije traže kolačiće, ali traže i pristanak da dozvolite pristup podatcima (kontaktima, porukama, fotografijama). Tada naše fotografije nisu sigurne. (UČ13); *To za kolačiće uvijek me traži a ja recimo moram provjeriti neku informaciju na toj stranici* (UČ9).

Povezano s kolačićima koji se pojavljuju prilikom ulaska na stranicu na internetu, javlja se i prozor gdje se mora dati dopuštenje kako bi se pretražila informacija koja nam je potrebna. Stoga su se sudionici osvrnuli na **davanje dopuštenja.** Prema njihovim izjavama, svjesni su da sami dajemo dopuštenja i na taj način dovodimo u rizik naše osobne podatke. Ponekad je to trenutak nepažnje te tim odobrenjem dopustimo korištenje osobnih podataka, a da to zapravo ni ne znamo. „I *sami dajemo dopuštenje našim kontaktima i fotografijama* (…) *jer oni dobiju naše dopuštenje kroz male detalje. Mi to na brzinu prihvatimo, ne gledamo što je to. Oni uz pomoć toga dobiju dopuštenje da koriste naše podatke a mi zapravo za to ne znamo* (UČ11)“. Što se tiče društvenih mreža i otvorenih profila na istima, razlikuju se oni koji **imaju javne profile na društvenim mrežama** i oni koji **koriste privatne profile na društvenim mrežama.** Srednjoškolci smatraju ukoliko je osoba sigurna u svoje postavke sigurnosti i privatnosti da može imati otvoren profil.

Može on prihvatiti i ne prihvatiti i imati otvoreni profil ako je on siguran u tome da ima otvoreni profil i da mu nitko ništa ne može, što je skroz ok. Ja se s time slažem, ako si ti siguran sam u sebe, ako si siguran i stavljaš neke normalne stvari i sadržaj, ok, izvoli, drži svoj profil otvoren. Ali, opet

i ti ljudi koji imaju otvoren profil, na primjer, koliko god se tebi čini njih svak prati, nije, oni reguliraju to. (UČ20)

No, većina srednjoškolaca ipak štiti svoju privatnost na internetu, a posebno na društvenim mrežama tako što: „ … *imamo privatne profile.* (UČ3); … *imam zaključani račun/profil da ne može svatko vidjeti* (UČ6)".

Dozvole prilikom korištenja interneta, a posebno tzv. kolačići koriste se kako bi prikupljali podatke o korisniku i njegovom uređaju, no ne koriste se za prikupljanje osjetljivih podataka nego kako bi poboljšali korisničko iskustvo prilikom korištenja interneta (Bračko, 2022.). Čitanje uvjeta korištenja prilikom otvaranja profila na društvenim mrežama, prema istraživanju pokazuje da to korisnici uglavnom ne rade i daju dozvole za koje nisu sigurni (Justament, 2017.). Dobiveni rezultati vezani uz vidljivost profila, odnosno o javnim i privatnim profila u skladu su s istraživanjem koje je provela Leko (2019.) gdje sudionici istraživanja navode kako im je profil uglavnom zaključan, dok ima nekoliko njih kojima profil mogu vidjeti i osobe koje im nisu prijatelji na društvenim mrežama. Oni koji imaju javne profile smatraju kako se nema što vidjeti na njihovim profilima ili da ih drugi ljudi ne mogu prepoznati zbog promjena u boji kose ili slično (Leko, 2019.). Autori Lough i Fisher (2016) navode kako je u njihovom istraživanju 56,5% osoba postavilo svoje profile kao javne, dok je 39,1% njih postavilo svoje profile kao privatne. Istraživanje Poliklinike za zaštitu djece i mladih grada Zagreba o iskustvima i ponašanjima djece na internetu i na društvenoj mreži Facebook pokazalo je kako 63% djece iskazuje da im je profil vidljiv osoba koje poznaju, 17% i drugim osim osobnim prijateljima, 8% njih ima javni profil da ga svi mogu vidjeti dok 12% njih nije sigurno je li im profil javan ili privatan.[5] Dok je istraživanje Grmuše i sur (2018) pokazalo da najviše ispitanika ima djelomično javan profil, zatim oni kojima je profil u potpunosti privatan, te manji broj sudionika kojima je profil javan za sve. Slične rezultate pokazalo je i istraživanje

[5] Poliklinika za zaštitu djece i mladih grada Zagreba (2014). *Istraživanje o iskustvima i ponašanjima djece na internetu i na društvenoj mreži Facebook.* Posjećeno 20.09.2022. na mrežnoj stranici Poliklinike za zaštitu djece i mladih grada Zagreba: https://www.poliklinika-djeca.hr/istrazivanja/istrazivanje-o-iskustvima-i-ponasanjima-djece-na-internetu-i-na-drustvenoj-mrezi-facebook-2/

Matković i Vejmelke (2021.) gdje javno dostupne profile ima 17,6% učenika, od kojih 22,6% dječaka i 14,3% djevojčica.

Što se tiče broja profila na društvenim mrežama, kvalitativno istraživanje Vejmelke i sur. (2020.) pokazalo je kako sudionici imaju više od jednog profila na društvenim mrežama te da preferiraju društvenu mrežu Instagram u odnosu na Facebook. Istraživanje Vejmelke i sur. (2022.) pokazalo je kako 42% mladih aktivno koristi 2 ili više profila na istoj društvenoj mreži. Navode kako je Instagram kao društvena mreža lakša za korištenje, posebno na mobilnim uređajima. Osim toga, prednost su dali vizualnoj komunikaciji, putem fotografija i videozapisa u odnosu na tekstualnu komunikaciju (Vejmelka i sur., 2020.).

Doživljaj privatnosti

Uz opis doživljaja sigurnosti, sudionici su definirali i **doživljaj privatnosti na internetu.** Ono što se pokazalo je da srednjoškolci **znaju definirati privatnost na internetu.** Definirali su je ovako:

Privatnost su one stvari koje želimo zadržati za sebe … (UČ13); *Privatnost naša je nešto što samo mi znamo i nešto što ne dijelimo sa svakim s kim se upoznajemo* (UČ18); *Privatno je ono što je moje, što znam samo ja i ta osoba koje se tiče*. *To je privatnost* (UČ20).

Osim definiranja privatnosti na internetu, srednjoškolci **znaju koji su privatni podaci na internetu:** „*To su na primjer neke obiteljske stvari, nešto što tu osobu tišti, ili joj je neugodno iznijeti neke stvari.* (UČ2); *Privatni podaci koje ne želimo na internetu je sve ono kako bi nas netko mogao identificirati (broj mobitela, Lokacija, škola)* (UČ7)". Također, izrazili su **svijest i riziku objave različitih sadržaja** što se odnosi na „*Čim je nešto javno objavljeno, percipira se da možeš dijeliti*. (UČ8); *Svi moramo biti svjesni da svaki sadržaj koji objavimo može bilo gdje završiti* (UČ7)". Nadalje, vidimo da su srednjoškolci svjesni **javnog karaktera interneta,** odnosno da je to javna mreža koja je dostupna svima, pa tako i podaci koji su objavljeni na internetu. „*Ako je nešto već na internetu nije narušavanje privatnosti. u svijetu interneta zapravo uopće nema privatnosti*… (UČ7); *Svi promatramo Internet kao javnu stvar* (…) (UČ8)".

Prema dobivenim rezultatima vidimo da su sudionici istraživanja dobro upoznati s privatnosti na internetu, odnosno da su svjesni svih rizika koje sa sobom nosi narušavanje

privatnosti. Svjesni su da je Internet javna mreža koja i da koliko se god trudili zaštiti se, uvijek im se može dogoditi da nisu dovoljno sigurni na internetu. Narušavanje privatnosti je česta pojava, iako ponekad nismo svjesni da se to događa, to potvrđuje i istraživanje Bolšec (2021.), ali i Justament (2017.). U kvalitativnom istraživanju Vejmelke i sur. (2020.) sudionici su naveli kako su svjesni se osobni podaci mogu zloupotrijebiti za krađu podataka, a da se to posebno odnosi na fotografije, putem kojih se može osramotiti žrtva. Također, upoznati su s važnosti zaštite internetske privatnosti i nedijeljenja osobnih podataka.

5.2.1. Kako srednjoškolci opisuju sigurnost i privatnost na internetu i na koji način osiguravaju vlastitu sigurnost i privatnost na internetu?

Drugi dio istraživačkog pitanja odnosi se na to kako srednjoškolci osiguravaju vlastitu sigurnost i privatnost na internetu, odnosno što sve čine kako bi zaštitili svoje osobne podatke koje objavljuju na internetu. Osiguravanje vlastite sigurnosti i privatnosti na internetu sastoji se od jedne teme (vidjeti *Tablicu 5.2.1.*): 1) Načini osiguravanja sigurnosti i privatnosti na internetu.

Tablica 5.2.1. *Osiguravanje vlastite sigurnosti i privatnosti na internetu*

TEMA	KATEGORIJE
Načini osiguravanja sigurnosti i privatnosti na internetu	Ne iznošenje osobnih podataka Nepristupanje drugih našim osobnim porukama i pozivima Korištenje zaštitnih lozinki Zaštita aplikacija putem poruke i generiranog koda Dvostruka zaštita prilikom prijave na korisnički profil na društvenoj mreži Korištenje sigurnih stranica

Srednjoškolci su naveli na koji način osiguravaju vlastitu sigurnost i privatnost na internetu. Navode da je način osiguravanja sigurnosti i privatnosti **ne iznošenje osobnih podataka:** „*Ne iznositi svoje podatke javno, (...) osobne, (...) oib, adresu, broj mobitela*.

(UČ2); (…) *ne objavljivati sve o našem životu* (UČ9)". Ukoliko **nema pristupa drugih našim osobnim porukama i pozivima,** to znači da je osigurana sigurnost i privatnost. Sudionici istraživanja navode: „Pa da *nitko nema pristup mojim porukama, pozivima, slikama i da ne može stupiti u kontakt s nama bez naše dozvole* (UČ11); *Da se ne moramo bojati da će netko gledati u naše poruke ili snimati razgovore i tako to* (UČ14)". Važna stavka prilikom korištenja interneta je **korištenje zaštitnih zaporki.** Zaporke moraju biti određene snage kako bi štitile sve osobne podatke koji su upisani prilikom otvaranja profila na društvenim mrežama. Sudionici istraživanja navode da su pažljivi oko postavljanja zaporki te ih poneki mijenjanju svakih nekoliko mjeseci kako bi zaštita i dalje bila djelotvorna. „*Stavljamo snažne lozinke* (UČ8); *Lozinke koje koristimo koje samo mi znamo* (UČ14); *Da lozinke nisu vidljive i javne* (UČ7)". Također, pojedine aplikacije omogućavaju zaštitu podataka na način da se upisuju **kodovi koji se pošalju putem poruke**. Sudionici su spomenuli kako su uključili ovu postavku sigurnosti i na taj način osigurali nemogućnost provale u njihov račun na internetu. Oni kažu:

I onda sam maksimalno zaštitio mail, nekako, kad se ideš prijaviti da se treba dobiti poruka i da ja sa mobitela moram prihvatiti (UČ15); (…) *kada ti netko pokuša ući u profil da se tebi automatski pošalje na tvoj mobitel poruka da ti netko pokušava ući i jesi li to ti* (generirani kod) (UČ14).

Istu mogućnost pružaju i društvene mreže kroz **dvostruku zaštitu prilikom prijave na korisnički profil na društvenoj mreži.** Naposlijetku, sigurnost i privatnost može se očuvati **korištenjem sigurnih stranica.** Pod time sudionici misle na stranice preko kojih mogu gledati razne sadržaje, poput serija i filmova. „(…) *Mislim to za filmove i to, postoji drugi način da bi gledali filmove. Postoje Netflix, postoje sigurne stranice tako da to mi uopće nije važno za viruse* (UČ20)". Također, koriste one stranice koje su provjerene kao sigurne i na kojima se oni osjećaju sigurni. „Tipa, *osjećam se sigurno na onim stranicama što ja znam, što koristim* (UČ13)".

Ovi rezultati pokazuju kako su naši sudionici istraživanja upoznati s načinima kako da osiguraju sigurnost i privatnost na internetu. Dosadašnja istraživanja su u skladu s dobivenim rezultatima. U istraživanju koji je proveo Vojnović (2017.), 51% učenika je izjavilo kako nikad ne iznose osobne podatke na društvene mreže. Iste rezultati dobiveni

su i u istraživanju koje je proveo Justamnet (2017.). S druge strane, u istraživanju Perić i sur. (2021.) malo manje od polovice učenika je reklo kako su objavljivali tuđe fotografije bez dopuštenja, kao i da im ne smeta kada to drugi rade. Istraživanje Hrabrog telefona i Poliklinike za zaštitu djece i mladih grada Zagreba (2013.) pokazuje kako čak 85% djece dijeli svoje ime i prezime, 38% e-mail adresu, a njih 43% svoje privatne fotografije.[6] Istovjetne rezultati dobiveni su i u istraživanju koje je provela Bolšec (2021.) gdje 93% ispitanika dijeli privatne fotografije na društvenim mrežama, zatim informacije o školovanju (76%), ali i događaje iz života poput izleta. Što se tiče korištenja lozinki, zaštite aplikacija putem generiranog koda i dvostruke zaštite prilikom prijave na korisnički profil na društvenoj mreži, dobiveni rezultati su u skladu s dosadašnjim istraživanjima. Istraživanja pokazuju kako je važno učestalo mijenjanje zaporki, ali i korištenje različitih lozinki za pojedine aplikacije i društvene mreže (Vojnović, 2017.). S time se slaže i Varga (2011.) koji navodi da može doći do zlouporabe ukoliko se sazna tuđa lozinka. Prema istraživanju Opačić i sur. (2021.) mladi su vrlo malo skloni dijeljenu lozinki s drugima (Vejmelka i sur., 2020.), dok istraživanje Bolšec (2021.) pokazuje kako 48% ispitanika koristi istu lozinku za sve društvene mreže.

5.3. Koje izazove srednjoškolci prepoznaju prilikom ostvarivanja vlastite sigurnosti i privatnosti na internetu?

Treće istraživačko pitanje odnosi se na izazove koje srednjoškolci prepoznaju prilikom ostvarivanja vlastite sigurnosti i privatnosti na internetu. Izazovi prilikom ostvarivanja sigurnosti i privatnosti na internetu sastoje se od jedne teme (vidjeti *Tablicu 5.3.*): 1) Izazovi prilikom ostvarivanja sigurnosti i privatnosti na Internetu.

[6] Poliklinika za zaštitu djece i mladih grada Zagreba (2013). *Our study: How much time children in Croatia use the Internet and Facebook and risks.* Posjećeno 20.09.2022. na mrežnoj stranici Poliklinike za zaštitu djece i mladih grada Zagreb: https://www.poliklinika-djeca.hr/english/featured/directors-note/our-study-how-much-time-children-in-croatia-use-the-internet-and-facebook-and-risks/

Tablica 5.3. *Izazovi prilikom ostvarivanja sigurnosti i privatnosti na internetu*

TEMA	KATEGORIJE
Izazovi prilikom ostvarivanja sigurnosti i privatnosti na internetu	Prijetnje putem lažnog profila Svijest o postojanju lažnih profila i lažnom predstavljanju Postojanje fake profila na društvenim mrežama Razlikovanje lažnog predstavljanja i fake profila Vrijeđanje putem društvenih mreža Provaljivanje u profile na društvenim mrežama Rizični / neprovjereni online izvori Digitalni trag/otisak

Izazovi prilikom ostvarivanja sigurnosti i privatnosti na internetu

Sudionici istraživanja naveli su niz izazova s kojim se susreću prilikom ostvarivanja vlastite sigurnosti i privatnosti na internetu. Prvo na što su se osvrnuli su lažni profili. Sudionici navode kako se susreću s **prijetnjama putem lažnog profila.** Jedna sudionica je rekla kako se susrela s takvim prijetnjama:

(…) *upadne mi neki lažni profil, kao prijetio: Naći ću te, dobit ćeš ovo-ono! Dobivala sam te neke prijetnje* ali to nisam shvaćala ozbiljno jer je to *lažni profil i želi me uplašiti taj netko s kim nisam u dobrim odnosima i to.. Napravila je taj lažni profil* i *počela pisati svašta da bi se ja pripala, da ne bi izlazila iz kuće, nešto u tom smislu.* (UČ2).

Nadalje, srednjoškolci imaju **svijest o postojanju lažnih profila i lažnom predstavljanju.** Kažu kako je u njihovom okruženju bilo situacija gdje su sami bili žrtve napada s lažnog profila ili su to bili njihovi prijatelji. „*Mog prijatelja iz razreda su zezali s lažnog profila*. (UČ11); *(...) Netko je napravio kao njen lažni profil i nije se nikada saznalo tko je to napravio* (UČ14)". Fake profili najčešće se otvaraju na društvenim mrežama te su i sami srednjoškolci primijetili **postojanje fake profila na društvenim mrežama.** Sudionici istraživanja kažu kako mogu prepoznati radi li se o lažnom profilu po neki značajkama poput slike profila ili zajedničkih prijatelja, no i da ima onih koji na to ne obraćaju previše pažnju i prihvate lažne profile kao prijatelje na svojim društvenim mrežama. „*Može se i ne*

vidit, teško. Ja bar vidim da je fake profil, zato što vidim da je bar, neki ljudi, neka ženska, ako ima taj fake profil, vidim žensku profilnu, imat će onako random muške ljude koji prihvate bilo koga. (UČ19); Zato kažem, *svi smo različiti i zato neki ljudi ne obraćaju pažnju tko njih prati i onda tu dolaze fake profili*. (UČ17)". Od stvarnih profila na društvenim mrežama, sudionici navode dodatna obilježja putem kojih **razlikuju lažno predstavljanje i fake profile.** Smatraju kako se može odmah prepoznati lažno predstavljanje po ponašanju na društvenim mrežama, npr.:

(…) *i to baš znam da je fake profil jer niti ima jednu sliku ili ako ima to je onda jedna slika prije 53 tjedna, što to nije, ono, ljudi stavljaju bar malo češće slike. I ono, vidim po pratiteljima, vidim po slikama i po storijima, i ono, baš znam, da je fake*. (UČ19); *Ako objave 5 slika u jednom danu..to mi je znak za fake profil.* (UČ8).

Osim lažnih profila, kao izazov su naveli **vrijeđanje putem društvenih mreža.** Do toga je došlo od strane nepoznate osobe na temelju podrijetla osobe koja se vrijeđala. Učenik kaže: „*Meni se dogodilo da je netko preko Whatsapp-a zvao* i *vrijeđao zbog podrijetla majčinog imena.* (UČ8)". Uz vrijeđanje, javlja se i **provaljivanje u profile na društvenim mrežama.** To je česta pojama, posebno među srednjoškolcima. Oni kažu da je to svakako dokaz manje sigurnosti na internetu jer se samom provalom na profil mogu ukrasti osobni podaci. Ako se nisu osobno susreli s provalom na njihov profil na društvenoj mreži, poznaju druge kojima je to učinjeno. „*Pa, provaljivanju u profil na instagramu. To je manjak sigurnosti. Jer samim tim da nam netko uzme naš profil, ima naše slike, poruke i sve ostalo. (UČ18*); Ja poznajem *par ljudi kojima je hakira profil*. (UČ7)". Učenici su kao izazov naveli i **rizične, odnosno neprovjerene online izvore.** Pod time su mislili na nesigurne stranice preko kojih mogu sakupiti viruse na računalo, preko kojih zatim može doći do krađe podataka.

Većinom su mi kao nesigurne. (...) ali tipa neke stranice, kada idem gledati neki film, to mi je toliko nesigurno, da ću pokupiti neki virus i tako to (UČ19); Da, *ako uđem na neku stranicu i ono piše mi error, nećemo ulaziti na te neke stranice. Sumnjičave* (UČ9).

Ono u što su uvjereni da postoji je **digitalni trag/otisak.** Upoznati su s njime i navode: „ *Jedan put kada nešto staviš, to je gotovo, to ostaje* (UČ18); *Sve što je objavljeno na internetu ostaje trajno zapisano* (UČ11)".

Prilikom ostvarivanja sigurnosti i privatnosti na internetu javljaju se razni izazovi s kojima se korisnici interneta, a posebno društvenih mreža moraju suočiti. Dobiveni rezultati u skladu su s dosadašnjim istraživanjima na istu temu (Varga, 2011., Marczi, 2014.,Vjemelka i sur., 2016., Machimbarrena i Garaigordobil, 2018., Ciboci i sur., 2020.,Vejmelka i sur., 2020., Vejmelka i Matković, 2021., Opačić i sur., 2021., Perić i sur., 2021., Bolšec, 2021.). Navedeni izazovi pripadaju pod pojam *Cyberbullinga* s kojim se susreće sve veći broj djece na internetu. Machimbarrena i Garaigordobil (2018.) u svojem istraživanju došli su do rezultata od 5 najrasprostranjenijih ponašanja na internetu, a to su uvrjedljive poruke i pozivi za prestrašivanje, ucjene ili prijetnje putem poziva ili interneta, kleveta iznošenjem laži preko interneta o nekoj osobi kako bi se zanemarila prava drugih. „7% djece u dobi od 9 do 17 godina imalo je iskustvo da se netko ponašao prema njima na povrjeđujući ili neugodan način, dok je 4,5% djece priznalo nasilno ponašanje prema drugima" (Ciboci i sur., 2020.). Dok je prema istraživanju Opačić i sur. (2021.) 97% mladih prepoznalo nasilje na internetu u tvrdnjama koje se odnose na *Širenje laži ili objavljivanje fotografija koje za cilj ima osramotiti nekoga na društvenim mrežama, slanje pogrdnih poruka ili prijetnji putem platformi za dopisivanje.* Također, isto su prepoznali u tvrdnji *Lažno predstavljanje i slanje neugodnih poruka u ime druge osobe.* O krađi identiteta i lažnom predstavljanju govore i mladi u istraživanju Vejmelke i sur. iz 2020. Anketa koju je provela Bolšec (2021.) sadržavala je pitanje koje se odnosilo na digitalni otisak, što su spomenuli i srednjoškolci kao izazov prilikom osiguravanja sigurnosti i privatnosti na internetu. Prema tom istraživanju, 38% ispitanika zna što je digitalni otisak, 22% njih nije čulo za taj pojam, dok 40% njih nije sigurno što taj pojam znači. Svakako je digitalni otisak važan dio Interneta koji nije potrebno zanemariti.

6. Implikacije istraživačkih nalaza i značaj za socijalni rad

Dobiveni rezultati mogu imati koristi u daljnjem istraživanju ove teme. Mogućnosti korištenja rezultata su raznoliki te mogu biti usmjereni na različite populacije i dobne skupine. Rezultati su pokazali s kojim izazovima se srednjoškolci suočavaju prilikom online komunikacije, ali i prilikom osiguravanja sigurnosti i privatnosti na internetu, na koje sve načine komuniciraju u online okruženju, te kako doživljavaju sigurnost i privatnost na internetu. U budućnosti se svakako mogu koristiti za planiranje preventivnih programa, ali i za zagovaračke akcije. Ova tema je bezvremenska te se pojavom novih generacija javljaju i novi problemi koje Internet nosi sa sobom. Svakako se može osvrnuti na edukaciju mladih, ali i roditelja, nastavnika. S djecom i mladima se mogu provesti razne radionice, ali i događaji u koje bi bili uključeni kroz razne aktivnosti. Djeca i mladi najbolje uče na temelju iskustva te bi svakako ovoj tematici pomogle tribine u kojima bi se razgovaralo o raznim situacijama s kojima su se djeca i mladi susreli na internetu.

Tema korištenja interneta, a posebno društvenih mreža važna je za socijalni rad, odnosno za sve stručnjake koji rade u tom području, a posebno s djecom i mladima. Internet je pojava koja se brzo razvija te kompetentni stručnjaci moraju biti u korak s modernim znanjima u svijetu suvremene tehnologije. Kako bi mogli zaštiti djecu i mlade moraju usvajati nova znanja o internetu, posebno o rizicima i izazovima koji su trenutno aktualni, ali i razvijati vještine koje će im pomoći da što adekvatnije riješe probleme koji se javljaju među djecom i mladima koji su aktivni korisnici interneta od najranije dobi. U tome im mogu pomoći broje edukacije gdje bi stekli dodatna znanja i vještine, ali i dobili uvide o tome kako je djeci odrastati u digitalnom dobu. Uz navedeno, stručnjaci koji se bave ovim temama trebali bi raditi na tome da se djecu i mlade što više upozna s rizicima koje Internet nosi, što kroz direktan rad s njima, ali i educiranje javnosti o štetnosti nepravilnog korištenja interneta. Svakako otvorenost prema ovoj temi će potaknuti i mlade da se uključe u rad organizacija i na taj način daju svoj doprinos. Ukoliko nema otvorenosti prema ovoj temi, javljat će se sve više slučajeva gdje će doći do kršenja sigurnosti i privatnosti na internetu, a djeca i mladi neće biti spremni povjeriti se odraslima o tome što im se dogodilo. Smatrat će da odrasli neće razumjeti što im se dogodilo i kako da im pomognu. Socijalni radnici mogu raditi na prevenciji kroz preventivne programe, na način da utvrde koja

znanja i vještine nedostaju djeci i mladima kako bi što sigurnije koristili Internet. To s mogu ostvariti kroz direktan rad s njima kroz radionice u školama. Potrebno je uključiti roditelje i nastavnike, kako bi ih se educiralo o tome kako da zaštite dijete ukoliko im se ono povjeri da je postao žrtva na internetu. Brojna predavanja i obilježavanje važnijih datuma u godini koja se odnose na korištenje interneta mogu pružiti dodatna znanja za cijelu javnost o tome kako sigurno koristiti Internet, pri čemu glavnu ulogu imaju stručnjaci koji se bave ovom tematikom. Također, stalno provođenje istraživanja i dobivanje aktualnih rezultata može pomoći stručnjacima da utvrde u kojem području trebaju najviše raditi s djecom i mladima jer će ova tematika biti aktualna još dugi niz godina, posebno jer se javlja sve veća upotreba suvremenih tehnologija kod djece vrtićke dobi. Pravilnom edukacijom tako male djece može se postići manje nasilja na internetu, ali i kršenja sigurnosti i privatnosti (Raguž i sur., 2021.).

7. Zaključak

Tijekom godina Internet je proširio svoju korisničku populaciju te je sve veći broj djece i mladih koji svakodnevno koriste Internet. Kako bi pravilno koristili internet sve blagodati koje on nudi, potrebno je imati određena znanja, a potom i vještine kako se maksimalno osigurati i zaštititi svoju privatnost na internetu. Uz to potrebno je i znati kako pravilno komunicirati u online okruženju i na koje sve razlike postoje u online komunikaciji i komunikaciji uživo. Rezultati ovog kvalitativnog istraživanja pokazuju kako srednjoškolci opisuju svoju komunikaciju u online okruženju, odnosno s kojim izazovima se susreću u online komunikaciji u odnosu na komunikaciju uživo te na koje sve načine međusobno komuniciraju putem društvenih mreža. Osim online komunikacije, u skladu s postavljenim istraživačkim pitanjima, srednjoškolci su opisali kako doživljavaju sigurnost i privatnost na internetu te s kojim izazovima se susreću prilikom očuvanja iste. Dobiveni rezultati su pokazali da su srednjoškolci svjesni rizika koje sa sobom nosi narušavanje sigurnosti i privatnosti te smatraju da imaju do sada dovoljno znanja i vještina kako bi se zaštitili prilikom korištenja interneta, što su pokazali i svojim izjavama o tome na koje sve načine mogu sačuvati sigurnost i privatnost na internetu. Srednjoškolci navode izazove s kojima se susreću na internetu, odnosno na društvenim mrežama, a na koje treba obratiti pažnju i usmjeriti daljnje preventivne programe i edukacije u tom smjeru.

Ova tema je svakako aktualna te dobiveni rezultati mogu pomoći u daljnjem radu stručnjaka, kroz organiziranje raznih zagovaračkih akcije, otvorenih tribina, video predavanja, ali i kroz direktan rad s djecom i mladima u školama ili organizacijama koje se bave tom tematikom. Njihova uloga u ovoj tematici je izrazito važna jer je potrebno educirati i zaštititi djecu od najranije dobi. Iako rezultati pokazuju pokazuju kako srednjoškolci imaju znanja o tome kako se zaštititi na internetu, kroz ne otkrivanje osobnih podataka, korištenje zaštitnih lozinki, duple zaštite na profilima na društvenim mrežama i dalje postoje razni rizici i opasnosti koje se mogu javiti prilikom nepažnje. Internet je mjesto gdje se mogu saznati brojne informacije, ukoliko se koristi na pravilan način neće doći do zlouporabe podataka ili narušavanja sigurnosti i privatnosti. Dobrom edukacijom roditelja, nastavnika, djece i mladih mogu se postići dobre navike korištenja interneta koje neće nikome štetiti.

Literatura:

1. AlJeraisy, M. N., Mohammad, H., Fayyoumi, A., & Alrashideh, W. (2015). Web 2.0 in education: The impact of discussion board on student performance and satisfaction. *Turkish Online Journal of Educational Technology-TOJET*, *14*(2), 247-258.
2. Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50,* 179-211.
3. Batori, M., & Ćurlin, M. (2020). Nasilje putem interneta među adolescentima. *Zdravstveni glasnik, 6*(1), 104-114.
4. Bračko, P. (2022). *Navike djece srednjoškolskog uzrasta u korištenju interneta i društvenih mreža*. Diplomski rad. Zagreb: Fakultet organizacije i informatike.
5. Best, P., Manktelow, R., & Taylor, B. (2014). Online communication, social media and adolescent wellbeing: A systematic narrative review. *Children and Youth Services Review, 41,* 27–36.
6. Buljan Flander, G., Selak Bagarić, E., Prijatelj, K., & Čagalj Farkas, M. (2020). Ispitivanje aktualnih trendova u korištenju društvenim mrežama kod učenika prvog i trećeg razreda srednjih škola u Hrvatskoj. *Kriminologija & socijalna integracija: časopis za kriminologiju, penologiju i poremećaje u ponašanju*, *28*(2), 277-294.
7. Bolšec, L. (2021). *Zaštita privatnosti na društvenim mrežama*. Završni rad. Zagreb: Filozofski fakultet, Odsjek za informacijske i komunikacijske znanosti.
8. Borovac, N. (2014). *Strategije očuvanja privatnosti u okviru modernih društvenih medija*. Diplomski rad. Osijek: Filozofski fakultet, Odsjek za informacijske znanosti.
9. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101.
10. Cavus, N., & Bicen, H. (2009, svibanj). *The Most Preferred Free E-mail Service Used by Students*. Rad izložen na konferenciji: „9th International Educational Technology Conference (IETC2009)“, Ankara, Turkey.

11. Cohen-Almagor, R. (2013). Internet history. U: Luppicini, R. (ur.), *Moral, ethical, and social dilemmas in the age of technology: Theories and practice* (str. 19-39). IGI Global.
12. Corrêa, C. H. (2019). Screen Time and the Logic of Identification in the Networked Society. U: Oliveira, L. (ur.), *Managing Screen Time in an Online Society* (str. 99-121). IGI Global.
13. Derks, D., Bos, A. E., & Von Grumbkow, J. (2008). Emoticons and online message interpretation. *Social Science Computer Review*, *26*(3), 379-388.
14. Divić, K., & Jolić, I. (2019). Rizično ponašanje djece i mladih u virtualnom okruženju–Iskustvo Centra za pružanje usluga u zajednici „Savjetovalište Luka Ritz ". *Napredak: Časopis za interdisciplinarna istraživanja u odgoju i obrazovanju*, *160*(3-4), 265-290.
15. Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of computer-mediated communication*, *15*(1), 83-108.
16. Dentzel, Z. (2013). How the internet has changed everyday life. *Ch@ nge*, *19*.
17. Economy-pedia (2022). *Rječnik: Internetska komunikacija*. Posjećeno 20.06.2022. na mrežnoj stranici Economy-pedia: https://hr.economy-pedia.com/11041101-online-communication.
18. Europska komisija, predstavništvo u Hrvatskoj (2019), *Zaštitite svoju privatnost na društvenim mrežama*, Posjećeno 16.06.2022. na mrežnoj stranici Europske komisije: https://croatia.representation.ec.europa.eu/index_hr
19. Elmendili, F., Moustir, A., & El Idrissi, Y. E. B. (2018). Privacy preserving on social networks: new Policies and approaches. U Mohamed B. A., Abdelhakim B. A., & Ali Y. (ur.), *Proceedings of the 3rd International Conference on Smart City Application.* (str. 1-9). New York: Association for Computing Machinery.
20. Filik, R., Țurcan, A., Thompson, D., Harvey, N., Davies, H., & Turner, A. (2016). Sarcasm and emoticons: Comprehension and emotional impact. *Quarterly Journal of Experimental Psychology*, *69*(11), 2130-2146.

21. Gangwar, S., & Narang, V. (2022). A Survey on Emerging Cyber Crimes and Their Impact Worldwide. U: Information Resources Management Association (ur.), *Research Anthology on Combating Cyber-Aggression and Online Negativity* (str. 1583-1595). IGI Global
22. Girvan, C. (2018). What is a virtual world? Definition and classification. *Educational Technology Research and Development*, *66*(5), 1087-1100.
23. Gibson, W. (1984.). Neuromancer. U: Greer, C. (ur.), *Crime and Media*, (str. 86-94). Routledge
24. Giménez, A. M., Luengo, J. A., & Bartrina, M. (2017). What are young people doing on Internet? Use of ICT, parental supervision strategies and exposure to risks. *Electronic Journal of Research in Educational Psychology, 15(3)*, 533-552.
25. Greenberg, G. S. (2008). CMC and the nature of human/machine interface. U: Kelsey, S. i St. Amant, K. (ur.), *Handbook of Research on Computer Mediated Communication* (str. 230-239). IGI Global.
26. Grmuša, T., Tomulić, A.M. i Anđelić, V. (2019). Zaštita privatnosti djece i maloljetnika na društvenoj mreži Facebook: navike i iskustva roditelja. *Communication Management Review, 04* (01), 78-97.
27. Gürses, S., Berendt, B., & Santen, T. (2006). Multilateral security requirements analysis for preserving privacy in ubiquitous environments. U Berendt B., & Menasalvas E. (ur.), *Proceedings of the UKDU Workshop* (str. 51-64).
28. Herring, S. C., & Androutsopoulos, J. (2015). Computer-mediated discourse 2.0. *The handbook of discourse analysis*, *2*, 127-151.
29. Ionescu, A. C. (2014). Cyber Identity: Our Alter-Ego?. U: Information Resources Management Association (ur.), *Cyber Behavior: Concepts, Methodologies, Tools, and Applications* (str. 57-70). IGI Global.
30. Injac, O., & Šendelj, R. (2017). National security policy and strategy and cyber security risks. U: Information Resources Management Association (ur.), *Identity Theft: Breakthroughs in Research and Practice* (str. 100-128). IGI Global.

31. International Organization for Standardization [ISO]. (2012) ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. Preuzeto s https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.
32. Justament, D. (2017). *Zaštita privatnosti na internetu.* Zagreb: Hrvatski studiji. Odjel za komunikologiju.
33. Kanae, V., 2015. *Utjecaj društvenih mreža na svakodnevni rječnik mladih ljudi.* Završni rad. Zagreb: Filozofski fakultet. Odsjek za informacijske znanosti.
34. Keefer, A., & Baiget, T. (2001). How it all began: a brief history of the Internet. *Vine*.
35. Kušić, S. (2010). Online društvene mreže i društveno umrežavanje kod učenika osnovne škole: navike facebook generacije. *Život i škola, LVI* (24), 103-125.
36. Kunić, I., Vučković Matić, M., & Sindik, J. (2017). Korištenje društvenih mreža kod učenika osnovne škole. *Sestrinski glasnik*, *22*(2), 152-158.
37. Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... & Wolff, S. (2009). A brief history of the Internet. *ACM SIGCOMM Computer Communication Review*, *39*(5), 22-31.
38. Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New media & society*, *10*(3), 393-411.
39. Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing facebook privacy settings: user expectations vs. reality. U Thiran, P. & Willinger, W. (ur.), *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (str. 61-70). New York: Association for Computing Machinery.
40. Lough, E., Fisher, M. H. (2016): Internet use and online safety in adults with Williams syndrome. Journal of Intellectual Disability Research, 60 (10), 1020-1030.
41. Lupton, D. (2014). *Digital sociology*. Routledge.

42. Löfgren-Mårtenson, L. (2008): Love in Cyberspace: Swedish young people with intellectual disabilities and the Internet. Scandinavian Journal of Disability Research, 10 (2), 125-138.
43. Marczi, S. (2014). *Odnosi među mladima u virtualnom svijetu*. Diplomski rad. Osijek: Filozofski fakultet, Odsjek za pedagogiju.
44. Machimbarrena, J. M., Calvete, E., Fernández-González, L., Álvarez-Bardón, A., Álvarez-Fernández, L., & González-Cabrera, J. (2018). Internet risks: An overview of victimization in cyberbullying, cyber dating abuse, sexting, online grooming and problematic internet use. *International journal of environmental research and public health*, *15*(11), 2471.
45. Matković, R. i Vejmelka, L. (2022). Online aktivnosti, e-učenje i roditeljska uloga kod osnovnoškolaca za vrijeme pandemije COVID -19. *Medijske studije, 13* (25), 3-26.
46. Matković, R., Vejmelka, L., Ključević, Z. (2021, rujan). *Impact of COVID 19 on the Use of Social Networks Security Settings of Elementary and High School Students in the Split-Dalmatia County*. Rad izložen na konferenciji: „2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO)“, Opatija.
47. Matković, R., Vejmelka, L., Ključević, Z. (2020, rujan). *Use of security settings on social networks of elementary and high school students in the Split-Dalmatia County*. Rad izložen na konferenciji: „2020 43th International Convention on Information, Communication and Electronic Technology (MIPRO)“, Opatija.
48. Mayer, C. P. (2009). Security and privacy challenges in the internet of things. *Electronic Communications of the EASST, 17*.
49. Machimbarrena, J., & Garaigordobil, M. (2018). Prevalence of Bullying and Cyberbullying in the Last Stage of Primary Education in the Basque Country. *The Spanish Journal of Psychology, 21*, E48.
50. Mishra, O. N. (2016). Cyberspace, Choice, and Consumer Welfare: Linking the Triad. U: Panwar, U. S. (ur.), *Handbook of Research on Promotional Strategies and Consumer Influence in the Service Sector* (str. 125-137). IGI Global

51. Miliša, Z., Tolić, M., & Vertovšek ,N. (2009). *Mediji i mladi : prevencija ovisnosti o medijskoj manipulaciji*. Zagreb: Sveučilišna knjižara.
52. Nikodem, K., Mirošević, J. K., & Nikodem, S. B. (2014). Internet i svakodnevne obaveze djece. Analiza povezanosti korištenja interneta i svakodnevnih obaveza zagrebačkih osnovnoškolaca. *Socijalna ekologija: časopis za ekološku misao i sociologijska istraživanja okoline*, *23*(3), 211-236.
53. Nacionalni portal za učenje na daljinu „Nikola Tesla“. *Uvod u Internet: Kratka povijest Interneta.* Posjećeno 14.6.2022. na mrežnoj stranci Nacionalnog portala za učenje na daljinu „Nikola Tesla“: https://tesla.carnet.hr/mod/book/view.php?id=5428&chapterid=883
54. Olweus, D. (1993). *Bullying at school: What we know and what we can do*. Oxford: Blackwell
55. Opačić, A., Jovović, I., Radat, K. & Majstorivić K. (2021.) *Iskustva mladih na internetu: korištenje interneta i nasilje na internetu – rezultati istraživanja.* Zagreb: Udruga za unaprjeđenje kvalitete življenja LET. Posjećeno 18.06.2022. na mrežnoj stranici Udruge za unaprjeđenje kvalitete življenja: https://udruga-let.hr/wp content/uploads/2021/06/Iskustva-mladih-na-internetu.pdf
56. Patton, M. Q. (1990). *Qualitative evaluation and research methods*. SAGE Publications.
57. Poliklinika za zaštitu djece i mladih grada Zagreba (2014). *Istraživanje o iskustvima i ponašanjima djece na internetu i na društvenoj mreži Facebook.* Posjećeno 20.09.2022. na mrežnoj stranici Poliklinike za zaštitu djece i mladih grada Zagreba: https://www.poliklinika-djeca.hr/istrazivanja/istrazivanje-o-iskustvima-i-ponasanjima-djece-na-internetu-i-na-drustvenoj-mrezi-facebook-2/
58. Popović, I. (2012). Problemi međugeneracijske komunikacije zbog utjecaja društvenih mreža. *Informatologia*, *45* (4), 333-341.
59. Potočnik, D. (2007). Mladi i nove tehnologije. U: Ilišin, V. i Radin, F. (ur.), *Mladi: problem ili resurs*, (str. 105-136). Zagreb: Institut za društvena istraživanja.
60. Pfleeger, C. P. (1988). *Security in computing*. Prentice-Hall, Inc..

61. Perić, S., Sekulić-Štivčević G. & Marušić-Brezetić, D. (2021). Etičko korištenje interneta i lažni profili. *Nastavnička revija: Stručni časopis Škole za medicinske sestre Vinogradska, 2*(1), 3-20.
62. Praprotnik, T. (2007). Jezik u (kon) tekstu računalno posredovane komunikacije. *Medijska istraživanja, 13*(2), 85-96.
63. Raad, E., & Chbeir, R. (2013). Privacy in online social networks. *Security and Privacy Preserving in Social Networks*, 3-45.
64. Randall, N. (2001). Stay in Touch. *PC Magazine,*101-104.
65. Rakić, D. (2020). *Navike korištenja društvenih mreža studenata Hrvatskih studija*. Diplomski rad., Zagreb1. Fakultet Hrvatskih studija, Odsjek za komunikologiju.
66. Raguž, A., Buljan Flander, G. i Boričević Maršanić, V. (2021). Uporaba modernih tehnologija kao rizik za seksualno zlostavljanje i iskorištavanje djece i adolescenata putem interneta. *Kriminologija & socijalna integracija, 29* (2), 226-247.
67. Rezabek, L., & Cochenour, J. (1998). Visual cues in computer-mediated communication: Supplementing text with emoticons. *Journal of visual literacy*, *18*(2), 201-215.
68. Rupčić, N. (ur.), (2021). *Značajke post-milenijalaca ili generacije z kao novih sudionika na tržištu rada.* Šibenik: Veleučilište u Šibeniku.
69. Skelac, I. (2015). Stewart Tubbs: Komunikacija–principi i konteksti. *Sociologija i prostor: časopis za istraživanje prostornoga i sociokulturnog razvoja*, *53*(2 (202)), 186-190.¸
70. Suler, J. (2004). The online disinhibition effect. Cyberpsychology and behavior, 7 (3), 321-326.
71. Shannon, C. E., & Weaver, W. (1949). A mathematical model of communication: University of Illinois Press.
72. Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of child psychology and psychiatry*, *49*(4), 376-385.

73. Tootell, H., Freeman, M., & Freeman, A. (2014). Generation alpha at the intersection of technology, play and motivation. *2014 47th Hawaii international conference on system sciences*, 82-90.
74. Valenti, L., 2021. *Utjecaj društvenih mreža na komunikaciju među mladima: sociološko istraživanje.* Završni rad. Split: Filozofski fakultet, Odsjek za sociologiju.
75. Varga, M. (2011). Zaštita elektroničkih podataka. *Tehnički glasnik, 5*(1), 61-73.
76. Vejmelka, L., Strabić, N. i Jazvo, M. (2017). Online aktivnosti i rizična ponašanja adolescenata u virtualnom okruženju. *Društvena istraživanja, 26* (1), 59-78.
77. Vejmelka, L. (2020). Komunikacija među partnerima u digitalno doba: mogućnosti obiteljske medijacije. *Ljetopis socijalnog rada, 27* (2), 341-368.
78. Vejmelka, L., Matkovic, R., & Borkovic, D. K. (2020). ONLINE AT RISK! ONLINE ACTIVITIES OF CHILDREN IN DORMITORIES: EXPERIENCES IN A CROATIAN COUNTY. *International Journal of Child, Youth and Family Studies*, *11*(4.1), 54-79.
79. Vejmelka, L. & Matković, R. (2021) Online Interactions and Problematic Internet Use of Croatian Students during the COVID-19 Pandemic. *Information*, 12 (10), 399.
80. Vejmelka, L., Ramljak, T., Rajter, T., Matković, R., Škorić, V. & Jurinić, J. (2022). *Predstavljanje preliminarnih rezultata deSHAME istraživanja u Hrvatskoj* (Power Point prezentacija). Posjećeno 27.09.2022. na mrežnoj stranici Centra za sigurniji internet:https://www.dansigurnijeginterneta.org/wpcontent/uploads/2022/02/deSHAME1CROmediji.pdf
81. Vojnović, N. (2017). *Ispitivanje svjesnosti srednjoškolaca Medicinske škole u Osijeku o privatnosti i zaštiti na Internetu*. Završni rad. Osijek: Medicinski fakultet, Sveučilišni preddiplomski studij sestrinstva.
82. Wellman, B., Quan-Haase, A., Boase, J., & Chen, W. (2002). Examining the Internet in everyday life. *Euricom Conference on e-Democracy* , 1-18.
83. Willard, N. E. (2007). *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Illionis: Research press.

84. Walther, J. B., & D'addario, K. P. (2001). The impacts of emoticons on message interpretation in computer-mediated communication. *Social science computer review, 19*(3), 324-347.
85. Worldometers (2022). *Društvo i mediji: Korisnika interneta u svijetu.* Posjećeno 14.06.2022. na mrežnoj stranici Wordometers: https://www.worldometers.info/hr/
86. Zakon o informacijskoj sigurnosti. *Narodne novine,* 79/09.

Prilozi:

Prilog 1: Prikaz rezultata s izjavama sudionika za komunikaciju putem online okruženja

TEME:	KATEGORIJE:	IZJAVE SUDIONIKA:
Izazovi tijekom online komunikacije	Poteškoće u izražavanju emocija u online komunikaciji	Bolje je komunicirati uživo. Ako se posvađam s nekim, lakše mi je uživo vidjeti je li toj osobi stvarno žao ili nije. *Ovako samo reče: oprosti i makne se. (UČ9)* *Ne znam kako izražavati emocije, ajmo reći.* (UČ9)
	Mogućnost jednostavnijeg lažiranja emocija	*Pa ovo virtualno može više biti lažno. Nitko ne može svoje osjećaje toliko dobro prenijeti kao što bi uživo prema nekome, ne znam.* (UČ10) *Mogu se lažirati osjećaji. Ono, govoriš nekome „Sviđaš mi se" a zapravo ono, potpuno da te nije briga za tu osobu.* (UČ14)
	Teže je prepoznati sarkazam i ironiju	Meni je problem komunikacije što *ne znam je li nešto sarkazam.* (UČ11) *Ne možemo razumjeti je li sarkazam ili nije (...)* (UČ14) *(...) jel ironija kada netko nešto napiše.* (UČ11)

	Teže je prepoznati humor	(…) *Ili ako se smije, napiše hahahaha ne znam je li to smijeh ili je to više…* (UČ11) *(…) Ne znaš je li mislila više iz zezancije ili je mislila ozbiljno. Što je uopće mislila, koji je to odgovor.* (UČ11)
	Nedostatak neverbalne komunikacije	Jer nema tona pa *ne znaš što je osoba zapravo mislila pod tom porukom*. (UČ11) *Ne možeš ništa sigurno znati.* (UČ10)
	Razlike u značenju poruke	A je, *kada napišeš neku poruku i ne napišeš tipa „hahahah" ili neki smajlić, to može imati skroz neki drugi kontekst.* (UČ21) Da, trebali bi biti isti, da imaju jedno značenje, tipa kada ja pošaljem poruku mami a ona ne razumije taj smajlić, *jer ima drugo značenje njoj, a mi međusobno imamo drugo značenje.* (UČ18) Da, na primjer dvije iste poruke: *Jesi li normalna? – to može biti nešto skroz ozbiljno. I jesi li normalna i ☺, to je kao šala .*(UČ20)

	Izjednačavanje online komunikacije i komunikacije uživo	*Meni je komunikacija apsolutno ista*. Ne ulazim u neku dublju komunikaciju s nekim s kim stvarno nisam dobra. Isto mi je. (UČ21) *Da, meni isto. Poruke šaljem i onda uživo samo nastavim.* (UČ18)
	Virtualna dezinhibicija	Neke stvari se uživo bojimo reći, ajmo reći na neki način, kad smo preko poruka, *onda dobijemo neki vjetar u leđa, neku hrabrost i onda ćeš preko poruka reći tko zna što, i onda opet uživo*… (UČ15) *Meni se on (pokazuje na (UČ15) probahati preko poruka a onda drugi dan: što je bilo? a nije ništa, nije ništa hahahahahaha*. (UČ16)
Načini razgovora tijekom online komunikacije	Razgovor kroz gifove	Ja sa prijateljicom *pričam kroz gifove.* (UČ19)
	Korištenje slikovnih sadržaja u online komunikaciji	*Pa staviš emotikon.* (UČ14) (…) *da se mi možemo dopisivati preko stickera* i mi ono umiremo, gušimo se od smijeha a nitko drugi ništa ne razumije. (UČ18) *Slali bi tako te smajliće i naljepnice* i mi smo umirali od smijeha. (UČ19) *A ti stickeri i to… razumijemo se jer iza*

		svakog stickera ima priča. I onda kada ona meni pošalje, ja znam o čemu ona priča. i koristimo neke nadimke koji uopće nisu vezani. (UČ18)
	Korištenje slang-a	Ili *„a e“.. to mi je tako nepristojno, kao da me se hoće skinut s dnevnog reda.* (UČ15) Kada napišem *DOBRO, to je dobro a kada napišem DOBROE, to je dobro je, aj kao…* (UČ18) Ne pišem ja tako. *Ja napišem DOBRO E.* (UČ20) *Ja mrzim taj glupi slang: štae, kakoe.* (UČ21)
	Korištenje drugačijeg vokabulara	*Mene živcira kada netko piše književno a govori drugačije, ili obrnuto*. To nema smisla. (UČ15) Neke osobe kao da su drugačije iza mobitela. *Koriste drugačiji vokabular i ne znam.* (UČ11)

	Korištenje internih fora	(…) mi *imamo toliko tih internih fora*, (…) i *mi ono umiremo, gušimo se od smijeha a nitko drugi ništa ne razumije*. (UČ18) Slali bi tako te smajliće i naljepnice *i mi smo umirali od smijeha.* (UČ19)

Prilog 2: Prikaz rezultata s izjavama sudionika za sigurnost i privatnost na internetu

TEME:	**KATEGORIJE:**	**IZJAVE SUDIONIKA:**
Doživljaj sigurnosti	Sigurnost izjednačavaju sa privatnosti	(…) *a sigurnost je način kako ćemo zaštiti svoju privatnost*. (UČ2) *Da će me netko uhoditi, pronaći,* u tom smislu sam ja pomislila. (UČ2) *Pa, da nas nitko ne može pronaći*…. (UČ13) *Sigurnost je to koliko znamo čuvati privatnost, iako čim nešto stavimo na Internet to više nije privatno*. (UČ7) *Sigurnost i privatnost mogu ići zajedno jer ako je privatnost ugrožena, možemo reći i da je sigurnost ugrožena*. (UČ6) *Ako vodimo računa o privatnosti tada ćemo imati i sigurnost.* (UČ8) *Sigurnost je sposobnost da nitko ne vidi našu privatnost*. (UČ11) *Povezano je, da. Preko tih*

		lozinki. Naša privatnost je povezana sa tom sigurnosti, znači nama treba ta šifra za ući na naš profil, koji je opet naša privatnost i zaštićena je sa tom šifrom al opet smatram da postoji razlika između sigurnosti i privatnosti. (UČ18) *Ja mislim da su sigurnost i privatnost zapravo jako povezani.* (UČ20)
	Osjećaj anonimnosti	*Nitko me ne zna, nitko mi ne prijeti, nigdje me nema.* (UČ3) *Pa da se osjećam sigurno i da znam da mi nitko ne može nauditi.* (UČ9) *Sigurnost je da mi znamo da neće nitko ući u te slike.* (UČ11)
	Promišljeno ponašanje u online okruženju	(…) *Zato ja govorim da sam sigurna, jer razmišljam o svojim postupcima na internetu, razmišljam u šta ću ući, u šta neću ući*. (…) (UČ20) Da, *ako mi se javi netko koga ne znam, razmišljat ću jesmo li se možda negdje sreli, što želi. ili Ako mi pošalje zahtjev, razmišljat ću je li znam tu osobu ili ne*. (UČ2)

	Smatraju da sigurno koriste Internet	Tipa, *osjećam se sigurno na onim stranicama što ja znam, što koristim.* (UČ13) *Smatram da mi nitko neće ukrasti moje slike, ne vidim razlog zašto bi nekome trebala moja slika…Prati mi profil samo prijatelji.*(UČ7)
	Razlozi zbog kojeg ne upotrebljavaju znanje o sigurnosti na internetu	*(…) ali da ne obraćaju toliko pozornost.* (UČ11) *Ne razmišljaju o sigurnosti zbog trenutačnog užitka.* (UČ12)
	Posjedovanje znanja o sigurnosti na internetu	*Mislim da znaju (…)* (UČ 11) *Ne znamo sve, ali mislim da dosta toga znamo.* (UČ8) *Većinu znamo.* (UČ6)
	Prihvaćanje poznatih osoba kao prijatelja na društvenim mrežama	*(...) prihvaćam prijatelje koje ja želim, koje znam. (…) (*UČ18) (...) Kao prvo, na instagramu *prihvaćam samo osobe koje znam i s kojima sam dobra.* (UČ7) (…) *A kad sam na Instagramu i društvenim tim, tu sam u sklopu sa svim bliskima, tu mi je kao ok* (…) (UČ19)

		Tako je, tako je. Točno to. *Ti biraš sam što ćeš stavljati na svoje mreže i kako ćeš se ponašati.* To je to. (UČ20) To smo svi svjesni toga. Kao i sve, ima i loše i dobre strane, *ti biraš šta ćeš. Ti biraš. Mislim da naš pristup internetu je točno onako kako mi želimo, kako mi razmišljamo, kako mi gledamo na to*. (UČ20) *Svatko ima legitimno pravo da radi što želi.* (UČ20)
	Mogućnost izbora prilikom ponašanja u online okruženju	
	Izjednačavanje sigurnosti na internetu sa zaštitom osobnih podataka	Ono, ne bojim se za svoj život. *da će netko moje podatke uzimati*. u tom smislu. (UČ2) Sigurnost podrazumijeva *da nitko ne ukrade podatke, broj mobitela* (…) (UČ7) Da se *naši osobni podaci ne dijele bez našeg dopuštenja.* (UČ8)

Dozvole prilikom korištenja interneta	Korištenje kolačića kao postavke sigurnosti	*Sve stranice i aplikacije traže kolačiće, ali traže i pristanak da dozvolite pristup podatcima (kontaktima, porukama, fotografijama).* Tada naše fotografije nisu sigurne. (UČ13) *To za kolačiće uvijek me traži* a ja recimo moram provjeriti neku informaciju na toj stranici. (UČ9)
	Davanje dopuštenja	*Zato svi dajemo dopuštenja* a svjesni smo da nam mogu ući u fotografije i sve al svi računaju neće meni (…) *Sami dajemo dozvole prilikom korištenja aplikacija*. (UČ13) I *sami dajemo dopuštenje našim kontaktima i fotografijama* (…) *jer oni dobiju naše dopuštenje kroz male detalje. Mi to na brzinu prihvatimo, ne gledamo što je to. Oni uz pomoć toga dobiju dopuštenje da koriste naše podatke a mi zapravo za to ne znamo.* (UČ11)
	Imaju javne profile na društvenim mrežama	Može on prihvatiti i ne prihvatiti i imati *otvoreni profil ako je on siguran u tome da ima otvoreni profil i da mu nitko ništa ne može, što je skroz ok.* Ja se s time slažem, *ako si ti siguran sam u sebe, ako si siguran i stavljaš neke normalne stvari i sadržaj, ok, izvoli, drži svoj profil otvoren.*

		Ali, opet i ti ljudi koji imaju otvoren profil, na primjer, koliko god se tebi čini njih svak prati, nije, oni reguliraju to. (UČ20) (…) *Ima ljudi koji imaju otvorene profile, koji vole imati više pratitelja, prate više ljudi, oni ne obraćaju pažnju ko mi*. (UČ17)
	Korištenje privatnih profila na društvenim mrežama	Mislim, *imamo privatne profile.* (UČ3) Ne dijelim baš privatne informacije, *imam zaključani račun/profil da ne može svatko vidjeti.* (UČ6) *Na instagramu možemo staviti da nam je račun privatan*, To znači prije nego nas želi pratiti i vidjeli naše fotografije i ono što mi objavljujemo mora poslati zahtjev. I onda mi možemo vidjeti hoćemo li odobriti tu osobu ili nećemo. Ako ju ne odobrimo, neće moći ništa vidjeti. (UČ13)
Doživljaj privatnosti	Znaju definirati privatnost na internetu	*Privatnost su one stvari koje želimo zadržati za sebe … Dakle, privatnost je nešto što želimo zadržati za sebe*. (UČ3) *Privatnost je nešto što želimo zadržati za sebe*. (UČ2) Još bih dodala da je *privatnost to što mi želimo zadržati za sebe pa da se osjećamo sigurno ako to ne objavimo*. (UČ1)

		Privatnost naša je nešto što samo mi znamo i nešto što ne dijelimo sa svakim s kim se upoznajemo, ono prvi put sad ću ja nekome ispričati sve o sebi, *jer to je moja privatnost i ja biram kome ću to reći*. (UČ18) *Privatno je ono što je moje, što znam samo ja i ta osoba koje se tiče*. To je privatnost. (UČ20) Pa uvijek postoji ta neka *privatnost koju ne treba znati druga osoba. (…) Privatnost treba ostaviti za sebe*. (UČ2) Ja imam instagram i recimo, *ne želim da svaki detalj iz mog života ti ljudi znaju.* (UČ7)
	Znaju koji su privatni podaci na internetu	*To su na primjer neke obiteljske stvari, nešto što tu osobu tišti, ili joj je neugodno iznijeti neke stvari.* (UČ2) *Privatni podaci koje ne želimo na internetu je sve ono kako bi nas netko mogao identificirati (broj mobitela, Lokacija, škola)*. (UČ7) *Pod privatnost spadaju naši pozivi, poruke i fotografije.* (UČ11) *Pa ako ne objavljujemo privatne podatke*. (UČ7)
		Čim je nešto javno objavljeno, percipira se da možeš dijeliti. (UČ8)

	Svijest o riziku objave različitih sadržaja	Ako se npr. Šalje u wapp grupi, *možemo reći da je privatnije i da osoba to želi dijeliti samo s onima kojima šalje, ako je na društvenim mrežama onda je drugačije.* (UČ7) Primjer , *čim se nešto objavi gubim kontrolu jer svatko može nešto s tim raditi.* (UČ6) *Svi moramo biti svjesni da svaki sadržaj koji objavimo može bilo gdje završiti.* (UČ7) (…) *i svi smo odgovorni za ono što stavljamo i što se događa.* (UČ8) (…) *jer svatko se mora zapitati kako bi se osjećao da netko dijeli nešto o njima i da to dođe u krive ruke.* (UČ6) Ne možemo imati kontrolu toliko. *Ono što smo mi objavili može netko screenat i proslijediti dalje.* (UČ2)
	Javni karakter interneta	*Ako je nešto već na internetu nije narušavanje privatnosti. u svijetu interneta zapravo uopće nema privatnosti…* (UČ7) *Svi promatramo Internet kao javnu stvar* (…) (UČ8) *Mislim da je ta privatnost zasjenjena, jer oni dobiju naše dopuštenje kroz male detalje* (UČ11)

Prilog 3: Prikaz rezultata s izjavama sudionika za osiguravanje vlastite sigurnosti i privatnosti na internetu

TEMA	KATEGORIJE	IZJAVE SUDIONIKA
Načini osiguravanja sigurnosti i privatnosti na internetu	Ne iznošenje osobnih podataka	*Ne iznositi svoje podatke javno, (...) osobne, (...) oib, adresu, broj mobitela.* (UČ2) *Sve s osobne iskaznice ne ide na Interne.* (UČ3) (…) *ne objavljivati sve o našem životu*… (UČ9) (…) *i ne davati pristup svojim informacijama različitim stranicama.* (UČ10)
	Nepristupanje drugih našim osobnim porukama i pozivima	Pa da *nitko nema pristup mojim porukama, pozivima, slikama i da ne može stupiti u kontakt s nama bez naše dozvole.* (UČ11) I ono što je UČ11 rekao, *one poruke, da je to samo za nas a ne za druge ljude.* (UČ13) Da se ne moramo bojati da *će netko gledati u naše poruke ili snimati razgovore i tako to.* (UČ14)
	Korištenje zaštitnih lozinki	*Stavljamo snažne lozinke.* (UČ8) *Ja svakih par mjeseci mijenjam lozinku*, doduše jer ja sama zaboravim. (UČ7)

		Možemo često mijenjati lozinke… (UČ9) *Da napravimo neku zaštitu lozinke* i takve stvari. (UČ10) *Lozinke koje koristimo koje samo mi znamo.* (UČ14) *Koristiti lozinke..* (UČ10) *Da lozinke nisu vidljive i javne.* (UČ7)
	Zaštita aplikacija putem poruke i generiranog koda	*I onda sam maksimalno zaštitio mail, nekako, kad se ideš prijaviti da se treba dobiti poruka i da ja sa mobitela moram prihvatiti.* (UČ15) Kada mi se netko želi ulogirati u Instagram, *ja moram poslati kod, na broj*. (UČ19) (…) *kada ti netko pokuša ući u profil da se tebi automatski pošalje na tvoj mobitel poruka da ti netko pokušava ući i jesi li to ti* (generirani kod). (UČ14)
	Dvostruka zaštita prilikom prijave na korisnički profil na društvenoj mreži	Pa koliko znam, nedavno kako se instagram ažurirava, ono, *svakodnevno kako ima nešto novo, oni imaju ono nešto dupla zaštita sa e-mailom* (UČ19) *Na instagramu se može postaviti dodatna zaštita.* (UČ14)

	Korištenje sigurnih stranica	(…) Mislim to za filmove i to, postoji drugi način da bi gledali filmove. *Postoje Netflix, postoje sigurne stranice tako da to mi uopće nije važno za viruse.* (UČ20) Tipa, *osjećam se sigurno na onim stranicama što ja znam, što koristim* (UČ13)

Prilog 4: Prikaz rezultata s izjavama sudionika za izazove ostvarivanja vlastite sigurnosti i privatnosti na internetu

TEME:	**KATEGORIJE:**	**IZJAVE SUDIONIKA:**
Izazovi prilikom ostvarivanja sigurnosti i privatnosti na internetu	Prijetnje putem lažnog profila	(…) *upadne mi neki lažni profil, kao prijetio: Naći ću te, dobit ćeš ovo-ono! Dobivala sam te neke prijetnje* ali to nisam shvaćala ozbiljno jer je to *lažni profil i želi me uplašiti taj netko s kim nisam u dobrim odnosima i to.* Ali nisam se puno sekirala oko toga. (UČ2) Napravila je taj lažni profil i *počela pisati svašta da bi se ja pripala, da ne bi izlazila iz kuće, nešto u tom smislu.* (UČ2)
		Meni se dogodilo da je netko preko Whatsapp-a

	Vrijeđanje putem društvenih mreža	zvao i *vrijeđao zbog podrijetla majčinog imena.* (UČ8)
	Provaljivanje u profile na društvenim mrežama	Pa, *provaljivanju u profil na instagramu.* To je manjak sigurnosti. Jer samim tim da nam netko uzme naš profil, ima naše slike, poruke i sve ostalo. (UČ18) Ja poznajem *par ljudi kojima je hakira profil*. (UČ7)
	Svijest o postojanju lažnih profila i lažnom predstavljanju	*Mog prijatelja iz razreda su zezali s lažnog profila*. (UČ11) *Ono, zezamo se pa napravimo lažni profil.* (UČ10) *(…) Netko je napravio kao njen lažni profil i nije se nikada saznalo tko je to napravio.* (UČ14)
	Postojanje fake profila na društvenim mrežama	A ti, *ajmo to tako reći „Fake profili" koji vas tako žele pratiti, ne uzimaju oni ime i prezime od nekoga tko je nama blizak i to*, (…) (UČ20) Može se i ne vidit, teško. *Ja bar vidim da je fake profil, zato što vidim da je bar, neki ljudi, neka ženska, ako ima taj fake profil, vidim žensku profilnu, imat će onako random muške ljude koji prihvate bilo koga*.

		(UČ19) Zato kažem, *svi smo različiti i zato neki ljudi ne obraćaju pažnju tko njih prati i onda tu dolaze fake profili*. (UČ17)
	Razlikovanje lažnog predstavljanja i fake profila	*Jednostavno, stave druge i pošalju vam zahtjev i žele vas pratiti*, ali to se baš vidi. (UČ20) (…) i to baš znam da je fake profil *jer niti ima jednu sliku ili ako ima to je onda jedna slika prije 53 tjedna, što to nije, ono, ljudi stavljaju bar malo češće slike. I ono, vidim po pratiteljima, vidim po slikama i po storijima, i ono, baš znam, da je fake*. (UČ19) *Pa jer osoba ima jednu sliku s interneta. 6 ljudi ih prati, a oni prate 50-ak ljudi*. (UČ7) *Kad ne žele reći neke osobne podatke.* (UČ2) *Ako objave 5 slika u jednom danu..to mi je znak za fake profil.* (UČ8) Jesam *i prepoznala sam po broju pratitelja.* (UČ6)
	Rizični / neprovjereni online izvori	Pa ne znam sad. *Većinom su mi kao nesigurne. (...) ali tipa neke stranice, kada idem gledati neki film, to mi je toliko nesigurno, da ću*

		pokupiti neki virus i tako to. (UČ19) Da, *ako uđem na neku stranicu i ono piše mi error, nećemo ulaziti na te neke stranice. Sumnjičave*. (UČ9)
	Digitalni trag/otisak	*Jedan put kada nešto staviš, to je gotovo, to ostaje* (UČ18) *Iako si ti to izbrisa, to ostaje* (UČ20) *Što staviš, ostaje iako obrišeš* (UČ15) *Sve što je objavljeno na internetu ostaje trajno zapisano*. (UČ11)

Prilog 5. Pitanja za provođenje fokus grupa

Sigurnost i privatnost:

Osjećate li se sigurno na internetu?

Što za vas znači „sigurnost na internetu“?

Je li se Vama ili nekome vama poznatome dogodilo nešto što bi opisali kao manjak sigurnosti?

Što poduzimate da bi bili sigurni?

Kako bi opisali razliku između sigurnosti i privatnosti?

Je li vam važno da imate svoju privatnost?

Mogu li vam sigurnosne postavke osigurati privatnost na internetu?

Smatrate li da imate kontrolu nad sadržajima koje podijelite na internetu?

Znate li razlikovati točne i provjerene informacije od lažnih? Lažni profili?

Komunikacija na internetu:

Sadržaji na internetu podrazumijevaju komunikaciju. Kako bi opisali svoju komunikaciju na internetu?

Kako bi opisali općenito komunikaciju na internetu? Jeste li primijetili u komunikaciji drugih što vam ne odgovara?