SVEUČILIŠTE U ZAGREBU
UČITELJSKI FAKULTET
ODSJEK ZA UČITELJSKE STUDIJE

TEA MIKŠEC

DIPLOMSKI RAD

SIGURNOST I ZAŠTITA DJECE U INTERNETU

Zagreb, rujan 2019.

SVEUČILIŠTE U ZAGREBU
UČITELJSKI FAKULTET
ODSJEK ZA UČITELJSKE STUDIJE
(Zagreb)

DIPLOMSKI RAD

Ime i prezime pristupnika: Tea Mikšec
TEMA DIPLOMSKOG RADA: Sigurnost i zaštita djece u internetu

MENTOR: Doc. dr. sc. Predrag Oreški

Zagreb, rujan 2019.

SADRŽAJ

Sažetak

Život u tehnološkom dobu ima svoje prednosti i nedostatke. Svaki čovjek ima pravo na sigurnost i zaštitu te se samim time nameće i pitanje sigurnosti i zaštite na mreži, odnosno na internetu. U ovom diplomskom radu obrađuje se pregledna/teorijska tema koja se tiče sigurnosti i zaštite djece u internetu. Prvo poglavlje opisuje internet općenito kao globalnu mrežu koja pruža razne mogućnosti. Opisuje se kakav je to sadržaj na internetu primjeren i neprimjeren djeci te kako se internet može iskoristiti u nastavi u pozitivnom pogledu. Sljedeće poglavlje donosi savjete kako postići sigurnost na internetu. Objašnjena je uloga roditeljske zaštite i filtera koji se mogu postaviti i time doprinijeti sigurnosti. Osim sigurnosti, opisane su i postojeće opasnosti interneta poput malicioznih programa, krađe identiteta i ozbiljnog problema koji je sve prisutniji kod djece i mladih – elektroničkog nasilja. Poglavlje „Medijska pedagogija“ opisuje važnost te pedagogijske discipline, kao i medijske pismenosti i medijskih kompetencija koje su nužne za ”suživot“ s medijima današnjice. Sljedeće poglavlje bavi se zaštitom privatnosti u pravnom pogledu te su navedeni i kratko opisani zakoni u Republici Hrvatskoj koji se odnose na sigurnost, zaštitu, osobne podatke, elektroničke komunikacije te Kazneni zakon kojim se propisuju određene kazne za počinjene zločine. Posljednje poglavlje navodi najvažnije postojeće projekte u Republici Hrvatskoj nastalih upravo zbog tematike koja se u ovom radu obrađuje. Opisani su projekti „Sigurnih pet za sigurniji net“ i „Centar za sigurniji internet“. Također, prezentirano je istraživanje „EU Kids Online Hrvatska“ i navedeni su rezultati istraživanja relevantni za ovaj rad.

Ključne riječi: Internet, sigurnost, opasnost, zaštita, djeca

Summary

Life in the technological age has its advantages and disadvantages. Everyone has the right to security and protection and this also applies to the question of security and protection on the Internet. This thesis deals with a theoretical theme regarding the safety and protection of children in the internet. The first chapter describes the Internet in general as a global network that offers various opportunities. Also, it describes what kind of Internet content is appropriate and inappropriate for children and how the Internet can be used in education in a positive way. The next chapter provides tips on how to achieve security on the Internet. The role of parental protection and filters can be set up and thus contribute to security online. In addition to security, the existing dangers of the Internet, such as malicious programs, identity theft, and the serious problem that is increasingly present in children and youth – electronic violence are described in this thesis. The chapter "Media Pedagogy" describes the importance of this pedagogical discipline as well as media literacy and media competencies that are necessary for "coexistence" with today's media. The next chapter deals with the protection of privacy in legal terms, as well as briefly described the laws in the Republic of Croatia relating to security, protection, personal data, electronic communications and the Criminal Code of the Republic of Croatia which prescribe certain penalties for committed crimes. The last chapter lists the most important existing projects in the Republic of Croatia which have been created precisely because of the issues discussed in this thesis. "Sigurnih pet za sigurniji net" and "Centar za sigurniji internet" are described. Also, the study "EU Kids Online Croatia" was presented and the research results relevant to this paper are listed.

Key words: Internet, safety, danger, protection, children

1. UVOD

Sve što je novo i u neku ruku nepoznato, većini ljudi pobuđuje neki strah i nelagodu. Tako je i s korištenjem računala i općenito korištenjem interneta. Većini roditelja i učitelja internet predstavlja nepoznato područje s velikim mogućnosti korištenja koje se svakim danom povećavaju. Ponekad se može čuti kako netko kaže da se je dijete prije naučilo ”na računalo“ nego što je naučilo govorili ili hodati. Današnja djeca imaju veliki pristup medijima, posebice internetu. Roditelji ponekad u žurbi znaju djetetu dati pametni telefon kako bi dijete bilo okupirano nekom igrom, crtićem i slično. Najčešće se događa da djeca, kako imaju izraženu istraživačku narav, istražuju to što je pred njima i samostalnim se istraživanjem nauče služiti internetom. Iz tog razloga ne treba bježati od interneta niti odbijati naučiti osnovne stvari o njemu. Idealno bi bilo kada bi roditelji i djeca zajednički otkrivanjem učili kako internet funkcionira te što sve može ponuditi ta globalna mreža. Razgovorom i edukacijom o opasnim stvarima koje postoje na internetu, dovelo bi se do sigurnosti djece na internetu. Educirati se ne trebaju samo djeca, već i njihovi roditelji, učitelji i šira javnost. Samo se tako mogu postići željeni rezultati u vidu zaštite djece na internetu. Znanje je najbolja obrana protiv nečeg što nam može naštetiti i stoga se u ovom radu želi osvijestiti koje su to negativne stvari koje mogu ugroziti sigurnost djece na internetu te kako ih pravovremeno prepoznati i zaštiti djecu.

2. INTERNET

Kada je riječ o Internetu, postoje mnoge definicije koje ga opisuju. „Golemi sustav globalnih nezavisnih međusobno povezanih računalnih umreženja koja se koriste i komuniciraju pomoću TCP/IP protokola (*Transmission Control Protocol / Internet Protocol*) naziva se Internet.“ (Težak, 2010, str. 15). Najraširenija usluga na internetu je sveobuhvatna svjetska mreža – WWW (*World Wide Web*). Ona omogućuje pojedincu da zajednički dijeli informacije s ostalima. Često se u razgovoru o mreži može čuti pojam ”surfanje“ koji označava aktivnosti pretraživanja i navigacije internetom. „Danas se cjelokupno globalno društvo i naša civilizacija mogu smatrati internetskim društvom.“ (Težak, 2010, str. 18). Maleš i Stričević (2008) opisuju internet kao globalnu mrežu koja nam čini dostupnima bezbroj informacija i sadržaja, te omogućuje brzu komunikaciju. Upravo ta neograničena količina informacija predstavlja problem kod djece jer ona još ne znaju što sve mogu pronaći na internetu i kakve opasnosti vrebaju na njemu. „Nigdje ne postoji više *avatara*, *aliasa*, lažnih adresa i drugih oblika krivotvorenja identiteta kao na internetu.“ (Spitzer, 2018, str. 105). Kako većina djece predškolske i školske dobi, koja se koriste računalom i internetom, nisu medijski pismena ona postaju lake mete na mreži. Medijska pismenost važna je jer djeca nisu dovoljno zrela da prepoznaju opasnosti i procjene koje su informacije i sadržaji na internetu kvalitetni, a koji štetni. Djeca brzo savladaju tehniku korištenja računala kao i interneta, ali važno je i da postanu svjesna kako trebaju kritički pristupati svim informacijama i sadržajima koji se na internetu nalaze. Korisnost interneta i njegova uloga kao izvor informacija je neosporna, ali djeca (zajedno s njihovim roditeljima i učiteljima) moraju biti svjesna mogućih opasnosti koje se nalaze u ovoj globalnoj mreži.

2.1. Internet sadržaj (ne)primjeren djeci

Internet je globalna mreža u kojoj postoje beskrajni putevi u kojima bi dijete, čak i nenamjerno, moglo naići na stranice neprimjerenog sadržaja. Naravno da internet predstavlja izvor raznolikih i zanimljivih informacija, ali nažalost ima i svojih loših strana. Na internetu postoji niz agresivnih načina na koje se djecu iskorištava, od prijevara vezanih uz lažno predstavljanje, krađu identiteta pa sve do pornografskih sadržaja. Kada se postavi pitanje kako sve internet može biti opasan i štetan za dijete,

Maleš i Stričević (2008) u svojoj knjizi navode sljedeću podjelu na četiri glavne opasnosti, a to su: djeca podliježu komercijalizaciji, komunikacija postaje rizična, neistinite informacije i seksualno iskorištavanje djece. Kada je riječ o tome da djeca podliježu komercijalizaciji, misli se na to da se na neke stranice koje su namijenjene djeci ubacuju izravne veze (linkovi) koje ih vode do neprimjerenih sadržaja. Također, na takvim stranicama često se pojavljuju reklame za proizvode poput alkohola pa čak i droge, odnosno proizvoda za odrasle i one koji su zabranjeni. Komunikacija na internetu postaje rizična onda kad se djecu potiče da daju svoje osobne podatke koji će kasnije biti zlouporabljeni, poziva ih se na susrete uživo koje djeca vrlo često prešute svojim roditeljima te im se izravno nude razni sadržaji (npr. seksualni sadržaji, govor mržnje i slično) koje djeca još ni ne razumiju. Uz to, djeca često podliježu elektroničkom nasilju neovisno o tome bili oni žrtve ili napadači jer osjećaj anonimnosti, koji im pružaju stranice na internetu koje posjećuju, smanjuje njihov prag odgovornosti. Upravo zbog toga djeca misle da svašta mogu napisati, objaviti ili postaviti na mrežu i napraviti sve to bez ikakvih posljedica i kazni. Neistinite informacije i neistiniti sadržaji česta su pojava na internetu. Važno je djecu naučiti da razlikuju kvalitetne stranice koje plasiraju istinite i primjerene sadržaje te da ih razlikuju od onih koje naizgled vjerno prikazuju potpuno neistinite i izmišljene stvari i događaje. Kod vrednovanja sadržaja, važno je znati da osim interneta postoji više izvora koji mogu potvrditi istinitost neke informacije, primjerice knjige, časopisi, enciklopedije, odrasle osobe s iskustvom u vezi neke informacije i slično. Seksualno iskorištavanje djece vrlo je ozbiljna tema i predstavlja jednu od najvećih opasnosti koje vrebaju na djecu na internetu. Seksualni sadržaji su nažalost lako dostupni jer mnoge agresivne tehnologije usmjeravaju promet upravo prema njima. Djeca najčešće, ako dođu do takvih sadržaja, niti ne razumiju o čemu je riječ zbog čega lako steknu iskrivljenu sliku o spolnosti. Ponekad se u privlačenju mlađe publike koriste upravo slike djece iste dobi i na taj način djeca postanu laka meta za seksualno iskorištavanje. Maleš i Stričević iznose rezultate ispitivanja koje je 2004. godine proveo Eurobarometar (tehnički instrument Europske unije) u zemljama sjeverne Europe na uzorku djece između 9. i 16. godine. Rezultati istraživanja pokazali su kako je 44% djece koja koriste internet naletjelo na neku pornografsku stranicu, 25% njih je primilo materijale s pornografskim sadržajem, 30% njih je vidjelo stranice sa slikama nasilja, a samo je 15% njihovih roditelja izjavilo da su upoznati s aktivnostima vlastite djece. Rezultati su zabrinjavajući, ali moguće je pozitivno utjecati na njih edukacijom

roditelja, učitelja i javnosti o njima. Važno je da roditelji savladaju osnovne služenja internetom i da, ako baš ništa ne znaju o internetu, potraže pomoć stručnjaka. „Za internet se može reći da uistinu otvara vrata u svijet, no prije nego što dijete otvori ta vrata, roditelj treba znati što ga iza njih čeka!“ (Maleš i Stričević, 2008, str. 50). Svaki roditelj treba pratiti što dijete radi kad je za računalom, a posebice kada se služi internetom te znati koje internetske stranice njihova djeca posjećuju. Korištenje interneta može biti i zajednička zabavna aktivnost u kojoj će roditelji i djeca zajedno istraživati i kritički sagledati sadržaje i informacije koji su dostupni na internetu. Primjerice, pronaći nečiji broj telefona, pronaći svoju kuću ili kuću prijatelja, pronaći školu koju dijete pohađa, virtualno otputovati u neki grad, promatrati svemir, igrati edukacijske igre, pročitati neku zanimljivu i interaktivnu priču i slično. Zajedničko korištenje interneta od rane dobi dobar je temelj za kasnije razvijanje medijske pismenosti djeteta. Kod korištenja internetom, roditelji trebaju postaviti pravila u dogovoru s djetetom, ali izbjegavati stroge zabrane korištenja interneta. Maleš i Stričević naglašavaju kako roditelji zabranama ne poučavaju svoju djecu već njima potiču djecu na istraživanje zabranjenog. Dijete se uči samokontroli ako roditelji uspostave jasna pravila što je dopušteno a što nije, dok se koriste računalom i internetom, bez obzira nadgleda li ga netko ili ne. Preporučljivo je da roditelji označe stranice s primjerenim sadržajem koje su dobre za dijete. Razgovorom valja predočiti djetetu kako je internet mreža koja sadrži bezbroj korisnih i zanimljivih informacija i sadržaja, ali da isto tako postoje i neistinite i opasne informacije i sadržaji. Upravo zbog tih neistinitih i opasnih informacija i sadržaja, dijete treba znati kako se može provjeriti istinitost neke informacije koju pronađe na internetu. Također, djetetu treba objasniti opasnost davanja osobnih podataka na određenim stranicama jer ne znaju tko traži njihove podatke niti kako će se oni dalje koristiti, a često se dogodi da se takvi podaci zloupotrebe. Ako roditelji nauče dijete da im se povjeri kad god primijeti nešto loše ili strašno na internetu, onda je to veliki korak u vidu sigurnijeg korištenja internetom. Kako su roditelji uzor djetetu, tako će dijete usvojiti i navike korištenja internetom od svojih roditelja. Roditelji tada trebaju biti primjer kako se služiti internetom na koristan i zanimljiv način – pokazati djetetu koje su stranice korisne, zanimljive, ali i štetne i razgovarati s djetetom zašto je to tako.

2.2. Internet u nastavi

Računala su sveprisutna i postala su dio suvremenog života. Medijska pismenost danas predstavlja jedan od preduvjeta rada u većini zanimanja. Djeca s lakoćom i puno brže savladavaju medijsku pismenost dok roditeljima i općenito odraslima treba više vremena za to. U medijima i javnosti češće se naglašavaju negativne strane i opasnosti korištenja računala, osobito korištenja interneta. Naravno da negativnih strana trebaju biti svjesni i roditelji i učitelji pa i sama djeca, ali važno je da osvijeste kako računalo i internet imaju i brojne pozitivne strane. Pozitivne strane prevladat će samo uz dobru edukaciju i medijsko opismenjavanje. Osim što mogu pružiti zabavu, računala se mogu pretvoriti u nastavno pomagalo u obrazovanju. Učenici pretraživanjem interneta mogu steći nova znanja, istražiti nešto što ih zanima, naučiti neki strani jezik i slično. Internet se u nastavi može koristiti prilikom samostalnog, istraživačkog učenja. Učenici će naučiti raspoznati i vrednovati kvalitetne informacije od nekvalitetnih te će samim time razvijati kritičko mišljenje. Računalo, ali i internet, u nastavi pružaju velike mogućnosti korištenja. Kako bi se te mogućnosti mogle ostvariti potrebna je kvalitetna edukacija učitelja i razrađeni plan što se želi postići korištenjem računala i interneta u nastavi. „Za razliku od ljudi, računala mogu vrlo strpljivo ponavljati ono što treba naučiti. Stoga neki smatraju da je učenje uz pomoć računala vrlo pogodno za djecu, osobito mlađu i djecu s posebnim potrebama.“ (Živković, 2006, str. 16). Današnja djeca predškolske dobi provode veliku većinu vremena ili za računalom ili mobilnim telefonom. Najčešće igraju igrice, gledaju videozapise na YoutTube-u ili se koriste društvenim mrežama. Većina ih ima profil bar na jednoj društvenoj mreži, a neki koriste i nekoliko različitih društvenih mreža. Manfred Spitzer (2018) tvrdi kako život mladih ljudi danas više nije zamisliv bez društvenih mreža. Škole bi iz tog razloga trebale na pozitivan način naučiti upotrijebiti moć društvenih mreža. Primjerice, društvene mreže mogu se koristiti kao alat za učenje ili za komunikaciju s roditeljima. „Tehnologija i društvene mreže mogu poslužiti u razne pozitivne svrhe školskim ustanovama i učenicima te ne bi smjele biti ignorirane zbog straha od njihove zlouporabe.“ (Školski portal, 2014). Osim ignoriranja, trebalo bi izbjegavati i zabrane korištenja tehnologije u nastavi. Već je općepoznato i spomenuto da će djeca više htjeti nešto što im je zabranjeno. Djeci ne treba zabranjivati korištenje računala, interneta, mobilnih uređaja i svih usluga i mogućnosti koje pružaju već ih treba naučiti kako se

pravilno koristiti njima na svrhovit način te kako mogu biti korisni u svakodnevnom životu.

3. SIGURNOST NA INTERNETU

Đurđica Težak (2010) u svojoj knjizi kaže da je znanje uvijek najbolja obrana od opasnosti te ono stvara umijeće vladanja. Internet nudi bezbroj informacija i mogućnosti koje se trebaju znati koristiti na siguran i svrhovit način. Kako je internet dostupan svima, na njemu mogu djelovati i ljudi koji imaju loše namjere te se treba znati naučiti zaštititi od takvih ljudi, ali i zaštititi svoje računalo. „Bit internetske sigurnosti jest prevencija od neautoriziranoga pristupa i/ili prevencija od oštećivanja računala internetskim priključkom.“ (Težak, 2010, str. 44). Primjerice, stručnjaci mogu pomoći pri instaliranju zaštitnih filtera kako bi se izbjegli štetni sadržaji. To je u prvom redu najpotrebnije djeci predškolske dobi, a starija djeca sukladno s razvijanjem medijske pismenosti trebaju postepeno preuzimati odgovornost za sve što čine kada se koriste internetom. U Hrvatskoj se sigurnošću na internetu bavi odjel Nacionalni CERT (engl. Computer Emergency Response Team) koji je odjel Hrvatske akademske i istraživačke mreže CARNET. Kako prenosi CARNET, glavna zadaća Nacionalnog CERT-a je obrada incidenata na internetu, to jest očuvanje kibernetičke sigurnosti u Republici Hrvatskoj. Na internetskim stranicama Nacionalnog CERT-a[1] nalaze se razne brošure koje su usmjerene ka sigurnijem korištenju interneta, društvenih mreža, korištenju interneta u poslovanju, sigurnosti bežičnih mreža i slično. Također, mogu se pronaći osnovni podaci o malicioznim programima, alati za uklanjanje istih te postoje tjedni pregledi novosti o zlonamjernim sadržajima.

3.1. Zaštita djece i odraslih na internetu

Svatko tko nije svjestan nezamislivo velikog broja sadržaja i mogućnosti koje pruža internet, neovisno o tome jesu li ti sadržaji dobri ili loši, lako može postati žrtva opasnosti, bilo da je u pitanju odrasla osoba ili dijete. Upravo zato se nastoji zaštiti odrasle i djecu te općenito javnost upoznati i educirati o dobrim i lošim stranama interneta te kako se pravovremeno zaštititi od raznih opasnosti koje postoje na internetu. U jednom kliku, odnosno u jednom djeliću sekunde, pristupamo nezamislivo velikom broju sadržaja i količini informacija i stoga je važno znati kritički prosuditi koji je sadržaj kvalitetan i siguran, a koji je lažan i zlonamjeran. Uz to, važna je i svijest

[1] Nacionalni CERT – www.cert.hr

o postojanu zlonamjernog sadržaja u datotekama koje se preuzimaju s interneta. Na stranicama CERT-a u brošuri „Ne budi i ti hrvatski naivac“ (2019) opisane su glavne mjere zaštite na internetu. Najvažnije je ažurirati sve aplikacije koje su u doticaju s datotekama preuzetih s interneta, ali i ažurirati internetski preglednik koji igra važnu ulogu u zaštiti od zlonamjernog sadržaja koji pokušava dobiti pristup računalu. U brošuri piše kako bi se valjano zaštitili treba slijediti preporuke sigurnosnih stručnjaka i svakodnevno se informirati o temama iz svijeta kibernetičke sigurnosti. Na taj način će svatko biti spreman odgovoriti na napad, ako do njega dođe, i uspješno se obraniti. Neki od najvažnijih savjeta u zaštiti na internetu su: da na računalo instaliramo antivirusni program koji služi prepoznavanju i zaustavljanju malicioznih programa, da ažuriranja operacijskog sustava i aplikacija budu postavljena na automatsko ažuriranje, da lozinke budu što složenije i da izbjegavamo korištenje imena i datuma jer se takve kombinacije lako pogode, da imamo sigurnosne kopije na nekim vanjskim medijima koji nisu povezani mrežom za sve važne i povjerljive podatke koje pohranjujemo na računalu, da budemo vrlo oprezni na kojim stranicama upisujemo svoje podatke, posebice kada je riječ o korištenju kreditnih kartica prilikom internetskog plaćanja te da se informiramo o postojećim prijetnjama i općenito o novostima koje se tiču kibernetičke sigurnosti. Sve su to načini kako se zaštititi na internetu i oni se ne tiču se samo odraslih, već i djece. Roditelji možda iz navike misle da znaju više od djece o stvarima s kojima se ona susreću po prvi put u životu, ali kada je riječ o internetu i tehnologiji općenito, često je obrnuta situacija. Roditelji moraju dobro upoznati svijet tehnologije u kojem djeca odrastaju kako bi ga i sama razumjela, ali i kako bi djeci znala objasniti kako ostati siguran. Najvažnija pravila kojih se roditelji trebaju pridržavati kako bi im djeca ostala sigurna na internetu su: educirati se o servisima koje dijete koristi, postaviti pravila korištenja računala, računalo postaviti u zajedničku prostoriju na vidljivo mjesto, objasniti djetetu opasnost komunikacije s nepoznatim ljudima na internetu i posebice nalaženje s nepoznatim ljudima uživo, saznati što više o internetskim prijateljima djeteta, objasniti važnost i razliku između privatnosti i anonimnosti, pratiti aktivnosti djeteta na društvenim mrežama, koristiti roditeljsku zaštitu i filtere kako bi zaštitili dijete od neprimjerenog sadržaja i stranica te osvijestiti posljedice postavljanja sadržaja poput fotografija, videozapisa, osobnih podataka na internet („Sigurnije na internetu“, 2018).

3.1.1. Roditeljska zaštita i filteri

Važnu ulogu u zaštiti djece od opasnosti interneta ima mogućnost postavljanja roditeljske zaštite i filtera sadržaja. Laniado i Pietra (2005) navode kako su lukavosti kojima zlonamjernici pokušavaju namamiti djecu bezbrojne. Upravo iz tog razloga određeni filtri i oblici roditeljske zaštite su nužni. Roditelji mogu saznati sve o takvim vrstama zaštite na internetskim stranicama operatera ili osobno od operatera u poslovnici. Operateri pružaju mogućnosti roditeljske zaštite kojima roditelji, u dogovoru sa svojom djecom, mogu odrediti koje internetske stranice dijete smije posjećivati, s kojim kontaktima dijete smije biti u komunikaciji, pružiti djeci adekvatnu antivirusnu zaštitu te filtrirati neželjeni nasilni i/ili seksualni sadržaj. Osim raznih filtara i roditeljskih zaštita, postoje i takozvane zaštićene mreže. Laniado i Pietra opisuju zaštićene mreže kao portale stvorene upravo za djecu s ciljem da im se ponudi sigurno surfanje, daleko od stranica s neprimjerenim sadržajima. Djeca korištenjem zaštićenih mreža mogu pretraživati sadržaj koji im je primjeren. Usluga zaštićene mreže, ali i roditeljske zaštite može biti besplatna ili se plaća u nekom određenom iznosu, ovisno o operateru. U adresnoj traci web preglednika može postojati lokot ili zeleni kružić koji označava da je neka stranica sigurna. To znači da stranica nema skrivene linkove, agresivne reklame i slično. Važno je pogledati koji protokol koriste određene internetske stranice. Svaka internetska stranica na početku svoje adrese u adresnoj traci sadrži oznaku protokola. Najčešće je to HTTP[2] protokol, ali uz njega postoji i sigurniji protokol HTTPS[3]. Primjerice, ako stranica koristi HTTPS protokol i posjeduje certifikat o vlasniku te stranice, identitet vlasnika je provjerljiv i prevaranti mu nisu skloni („Sigurnije na internetu, 2018). Laniado i Pietra naglašavaju kako instalacija filtara, kao i provjera sadržaja stranica što ih dijete posjećuje, ne smije se shvatiti kao oblik kontrole zbog manjka povjerenja. Upravo suprotno, tu odluku kada roditelji odluče instalirati neki oblik roditeljske zaštite treba smatrati kao još jednu odluku u odgojnom procesu. Djeci treba postaviti jasna pravila i granice kako ne bi došlo do neželjenih posljedica. Ako usprkos svih postavljenih zaštita i dogovorenih pravila dijete ipak postane žrtva, treba nastojati izbjeći osjećaj krivnje koje dijete može

[2] HTTP (engl. HyperText Transfer Protocol)– protokol, odnosno skup pravila koja se koriste za prijenos hipertekstualnih dokumenata (web stranica) između dva računala (https://korisnik.optimahosting.hr/knowledgebase.php)

[3] HTTPS – protokol za razmjenu web sadržaja između preglednika i poslužitelja koji osigurava autentičnost, povjerljivost i neporecivost tim putem razmijenjenih podataka (https://www.cert.hr)

osjećati, a tek onda riješiti nastalu situaciju. Također, ako je riječ o uznemiravanju, svi dokazi (chat poruke, e-mail poruke, profil ili bilo koji podaci o napadaču i slično) trebaju se odnijeti u policijsku postaju radi prijave.

3.2. Opasnosti interneta

Osim svojih prednosti, internet naravno ima i svojih loših strana. Mnoge opasnosti vrebaju na internetu, pogotovo za one ljude koji se njime ne znaju služiti, a to su prvenstveno djeca. Iako su mogućnosti koje internet pruža zadivljujuće, treba biti svjestan da postoji i druga strana interneta koja nije tako ”sjajna“. Težak (2010) u svojoj knjizi kaže kako ljude moraju zanimati novi pojmovi i nove aktivnosti omogućene tajnošću, ali i lakom dostupnošću osoba i djelovanja na Internetu, internetski kriminal (*cybercrime*), zlobni kod (*malicious code*), internetski seks (*cybersex*), krađa identiteta i sigurnost umreženja. Internetski kriminal obuhvaća sve kriminalne napade koje omogućavaju komunikacijski uređaji u umreženju te svaki tip kriminala u kojemu se računala i umreženja koriste kao sredstvo, cilj i/ili mjesto kriminalne aktivnosti. Uz to, u internetski kriminal spadaju i specifični zločini čije je djelovanje olakšano uporabom računala. Primjerice, to su kriminali poput internetskih prijevara, dječje pornografije, internetske krađe i slično. Obrana od takvih opasnosti interneta, naravno, postoji. Razni sigurnosni hardveri i softveri u određenoj mjeri pružaju pomoć i sigurnost korisniku. Ali važno je naglasiti, kako i Težak kaže, da nikad neće biti rješenja koje bi potpuno zaštitilo korisnika. Sigurnosni hardveri i softveri su samo dio zaštite, ali važniju ulogu ima znanje i svjesnost korisnika o opasnostima interneta te da znanje koje posjeduju znaju i primijeniti.

3.3. Maliciozni programi

Maliciozni ili zlonamjerni program (engl. malicious software / malware) je program koji se samostalno širi putem informacijskih mreža ili interneta. Predstavlja softver koji se može instalirati s bilo kojeg medija, uključujući i internet. „Malware može imati više funkcija, od prikupljanja osjetljivih informacija, dobivanja pristupa zaraženom sustavu ili mreži, prekidu ili usporavanju računalnih operacija i komunikacija, itd.“ (CARNET, 2013). U maliciozne programe ubrajamo: viruse, crve, trojanskog konja, špijunski softver (spyware), rootkit, keylogger, dialer, URL Injector, adware,

ransomware. Težak (2010) objašnjava kako takvi maliciozni programi ne samo da inficiraju s korisnim teretom[4] ili bez njega, nego se mogu priključiti na korisnikov sustav, ukrasti lozinku ili se masovno poslati na e-adrese korisnika u adresaru. Osim što se nabrojeni maliciozni programi mogu nalaziti u programskim datotekama, datotekama dokumenata i skriptama, pojavljuju se i na internetskim stranicama. Zaštita od malicioznih programa odvija se pomoću antivirusnih softverskih programa, točnije kombinacija vatrozida i antivirusnog softvera štiti računalo i umreženje od malicioznih programa.

3.3.1. Virus

Virusi predstavljaju računalni program koji svojom reprodukcijom može zaraziti računala tako da kopira samog sebe u datotečni sustav ili memoriju računalnog sustava bez dopuštenja ili znanja korisnika („O virusima“, bez dat.). Najčešći oblik širenja virusa predstavlja širenje virusa s jednog računala na drugo u obliku izvršnog zlonamjernog koda putem interneta, privitaka u e-mail porukama ili medijima putem vanjskog tvrdog diska, USB, CD ili DVD diska. Kako bi određeni virus inficirao računalo u kojem se nalazi, korisnik mora pokrenuti zaraženi program i tada se izvršava njegov kod. Kada zarazi jedno računalo, virus može zaraziti i ostala računala koja se nalaze na istoj mreži.

3.3.2. Računalni crv

Računalni crvi su samostalni programi koji sami sebe umnožavaju i koji se šire putem računalne mreže („O crvima“, bez dat.). Širenje se odvija putem računalne mreže pomoću koje crvi s jednog računala šire zarazu na ostala računala. Način širenja računalnih crva je ili bez interakcije korisnika ili putem socijalnog inženjeringa. Širenje bez interakcije korisnika označava iskorištavanje sigurnosnih nedostataka operacijskog sustava i/ili aplikacija. Kada crv pronađe takav nedostatak, iskoristit će ga i instalirati svoju kopiju u to računalo te će tražiti druga računala koja može zaraziti preko mreže. Kako do toga ne bi došlo, redovno ažuriranje softvera je nužno. Širenje putem socijalnog inženjeringa obuhvaća interakciju sa žrtvom. Interakcija se odvija

[4] Korisni teret (engl. payload) je destruktivno djelovanje zlobnoga programa, odnosno virusa. Može biti manje ili više štetan, a nemaju ga svi virusi.

tako da autor računalnog crva prijevarom i lažima, putem e-mail poruka ili poruka na društvenim mrežama, pokušava nagovoriti žrtvu na preuzimanje i pokretanje izvršne datoteke crva. Glavnu zaštitu od računalnih crva predstavlja redovno ažuriranje softvera kako bi bilo što manje sigurnosnih nedostataka operacijskog sustava koje bi takav maliciozni program mogao iskoristiti.

3.3.3 Trojanski konj

Trojanski konj predstavlja zlonamjerni program koji se predstavlja kao neki koristan softver samo kako bi naveo korisnika na njegovu instalaciju. Na stranici CERT-a navodi se kako trojanski konj može izmijeniti operacijski sustav na zaraženom računalu kako bi on prikazivao oglase u svrhu ostvarivanja novčane koristi od strane napadača, a čak i može omogućiti napadaču potpunu kontrolu nad zaraženim računalom. Kontrolu koju napadač može imati obuhvaća korištenje memorije tvrdog diska, krađa povjerljivih informacija žrtve, praćenje pritisnutih tipki pomoću čega može saznati razne lozinke i brojeve kartica, rušenje zaraženog računala, instaliranje drugih oblika zlonamjernih programa i slične aktivnosti („O trojanskim konjima“, bez dat.). Trojanski konj može se lažno predstavljati kao neka igra ili sadržaj koji se šalje u e-mail poruci. Zaštitu od trojanskih konja pružaju razni antivirusni i *anti-malware* programi.

3.3.4. Špijunski softver (spyware)

Špijunski softver (engl. spyware) je vrsta zlonamjernog softvera čija je glavna zadaća prikupljanje informacija i preuzimanje kontrole nad računalom korisnika bez njegove dozvole i znanja. Glavna razlika između špijunskog softvera te virusa i crva je ta da se špijunski softver ne umnožava. Takav zlonamjerni softver iskorištava zaražena računala za komercijalnu dobit, za krađu osobnih podataka, za prikazivanje *pop-up* reklama ili preusmjeravanje HTTP zahtjeva na reklamne stranice. Zaraza se najčešće odvija prilikom posjete internetskih stranica s ilegalnim ili pornografskim sadržajem na kojima se zlonamjerni softver koristi sigurnosnim propustima u web pretraživačima te se instalira na računalo bez znanja korisnika. Špijunski softver opterećuje procesor, zauzima memoriju na tvrdom disku i povećava mrežnu aktivnost i zbog toga zaražena računala postaju usporena. Kako bi se uklonili ili blokirali špijunski softveri postoje takozvani *anti-spyware* alati. CERT navodi kako su najpoznatiji i najkorišteniji takvi

alati: Ad-Adware SE, Spybot-Search & Destroy i Windows Defender („O adware/spyware softveru“, bez dat.).

3.3.5. Adware

Adware predstavlja oblik špijunskog softvera koji iskorištava zaražena računala za komercijalnu dobit putem prikazivanja *pop-up* reklama („O adware/spyware softveru“, bez dat.). Dolazi od engleske riječi *Ad* koja označava reklamu te predstavlja takozvani reklamni ili oglašivački softver. Od nabrojanih malicioznih programa, adware je najmanje opasan, ali ujedno i najdosadniji jer ometa nesmetani rad na računalu.

3.3.6. Rootkit

Kao što piše na stranicama CERT-a, rootkit predstavlja najopasniju vrstu zlonamjernog programa jer je stvoren tako da je potpuno nevidljiv na računalu kojeg zarazi. Rootkit predstavlja skup alata koji omogućuju napadaču da na zaraženom računalu dobije ovlasti kao vlasnik (admin), uz prikrivanje znakova zlonamjernih aktivnosti. Rootkit nije potrebno instalirati već je dovoljno da žrtva preuzme ili kopira izvršnu datoteku na svoje računalo i pokrene ju. Današnji rootkit-ovi djeluju na razini operacijskog sustava što znači da je njihov razvoj dugotrajan i zahtjevan, ali kada zaraze računalo može proći i nekoliko mjeseci i godina prije nego budu primijećeni te stručnjaci smatraju upravo prevenciju najvećom zaštitom jer za otklanjanje tako složenih rootkit-ove savjetuju potpuno brisanje diska pa čak i ponovnu instalaciju cijelog sustava („O rootkit softveru“, bez dat.).

3.3.7. Keylogger

Keylogger je softver koji snima i prati pritisnute tipke na računalu bez znanja korisnika. Oni mogu biti i uređaji, ali prvenstveno predstavljaju softvere u užem smislu riječi. Zlonamjeran može biti kada se koristi u svrhu krađe tuđih podataka poput lozinki, brojeva bankovnih kartica, brojeva računa i slično. S druge strane, može biti korišten kod roditeljske zaštite kako bi se djeci zabranio pristup neprimjerenom sadržaju. Ostali oblici zlonamjernih softvera mogu sadržavati keylogger softver te

snimati pritisnute tipke na zaraženom računalu i podatke slati napadaču bez korisnikova znanja (primjerice, trojanski konj). Keylogger softveri šire se putem e-mail poruka, web preglednika ili putem nekog drugog zlonamjernog softvera s mogućnošću preuzimanja s mreže. Kada je riječ o zaštiti, kao i kod ostalih zlonamjernih softvera i kod keylogger softvera važno je imati antivirusnu zaštitu s trenutnim ažuriranjima. Još jedan važan korak u zaštiti je korištenje jednokratnih lozinki ili prilikom unošenja lozinke koristiti dvostruku autentifikaciju („O keylogger softveru“, bez dat.).

3.3.8. Ransomware

Jedan od opasnijih oblika malicioznih programa svakako je ransomware. Ransomware zapravo predstavlja skup malicioznih programa i specifičan je po tome da nakon što zarazi računalo, sve datoteke na računalu šifrira (kriptira) i čini ih neupotrebljivima, a od korisnika traži otkupninu kako bi vratio šifrirane datoteke. Iako se mnogi podvrgnu plaćanju otkupnine, u velikom broju slučajeva su datoteke zauvijek izgubljene i niti jedan iznos koji napadač ponudi žrtvi i kojeg žrtva plati neće vratiti datoteke. Iz tog razloga stručnjaci ne preporučuju plaćanje otkupnine jer tako žrtve zapravo financiraju kriminalce. Obrana od ovakvog oblika malicioznog programa je redovno stvaranje sigurnosnih kopija svih datoteka i podataka koje pohranjujemo na računalu. Također, kao i kod ostalih malicioznih programa, zaštiti od ransomware-a pridonosi antivirusni program s redovnim ažuriranjem, izbjegavanje otvaranja sumnjivih poveznica iz sumnjivih izvora koje su pristigle na e-mail, izbjegavanje otvaranja raznih reklama na internetskim portalima i najvažnije, redovno ažuriranje operacijskog sustava i aplikacija na računalu. Na internetskim stranicama CERT-a nalaze se detaljne upute što učiniti ako se računalo zarazi ransomware-om, odnosno ako postane neupotrebljivo dok se ne plati neka određena svota novca. Primjerice, objašnjeno je kako se mogu spasiti već šifrirane datoteke ili vratiti datoteke pomoću programa za vraćanje izbrisanih datoteka, kako stvoriti sigurnosnu kopiju datoteka (engl. Backup) ili sigurnosnu kopiju sustava (engl. System Backup) te kako vratiti datoteke ili sustav pomoću stvorene sigurnosne kopije („Ransomware“, bez dat.).

3.4. Krađa identiteta

Agencija za zaštitu osobnih podataka krađu identiteta opisuje kao radnju kojom netko koristi (prikuplja obrađuje) tuđe osobne podatke (fizičkih osoba) protivno zakonu. Krađe identiteta ne događaju se samo na mreži – u virtualnom svijetu, nego i u stvarnom životu. Nažalost, *online* krađe identiteta vrlo su česta pojava. Razni maliciozni programi poput trojana, špijunskog softvera, kradljivaca lozinki i sličnih oblika internetskih zločina, mogu služiti napadaču u krađi nečijeg identiteta. U krađu identiteta ubraja se: otvaranje lažnog profila na nekoj društvenoj mreži, lažno predstavljanje, zlouporaba tuđih osobnih podataka u svrhu počinjenja kaznenih djela (primjerice, u svrhu sklapanja lažnih ugovora). Krađa identiteta kazneno je djelo za koje je, prema Članku 146. Kaznenog zakona (2011), predviđena kazna zatvora do godinu dana. Osim što krađa identiteta predstavlja kazneno djelo, također predstavlja i povredu Zakona o zaštiti osobnih podataka. U slučaju krađe identiteta ili zlouporabe osobnih podataka važno je odmah reagirati – prijaviti slučaj policiji uz navođenje svih dokaza, te podnijeti zahtjev za zaštitu prava Agenciji za zaštitu osobnih podataka. U slučaju sklopljenog lažnog ugovora treba kontaktirati pravnu osobu s kojom je ugovor sklopljen. Neki od savjeta kako zaštititi svoj identitet na mreži su da se ista lozinka ne koristi na mnogim mjestima, kod online kupovine treba izbjegavati nepoznata e-komercijalna mjesta, paziti kada se pojavi neka neočekivana obavijest da je računalo zaraženo ili treba popravak, istražiti malo o načinima internetskih prijevara i znati prepoznati maliciozne programe te održavati računalo sigurnim tako da je antivirusni program ažuran, a vatrozid djelotvoran. Uvijek treba s oprezom i svjesno postupati osobnim podacima, voditi računa o tome na kojim stranicama ih dijelimo i kome te gdje ih ostavljamo vidljivima.

3.5. Cyberbullying – elektroničko nasilje

Problem nasilja nikada nije bio toliko prisutan kao u današnje vrijeme kada se susrećemo sa sve češćim prijetnjama u stvarnom i virtualnom svijetu. „Nasilje je postalo sastavni dio našega svakodnevnog života i činjenica je da se pojavljuje u sasvim neočekivanim okolnostima i oblicima.“ (Težak, 2010, str. 84). Nemoguće je poznavati sve uzroke i posljedice nasilja, ali treba biti svjestan da nasilje postoji i da se u nekoj mjeri može prevenirati. Cyberbullying predstavlja oblik nasilja koji se

odvija ”na mreži“, odnosno predstavlja elektroničko (virtualno) nasilje. „Elektroničkim nasiljem smatra se svaki oblik nasilja koji podrazumijeva slanje neprimjerenih i uvredljivih tekstualnih, vizualnih i audiovizualnih poruka, a može uključivati i prijetnje i druge oblike narušavanja privatnosti pojedinca.“ (Ciboci, Kanižaj, Labaš, Osmančević, 2018, str. 70). Glavna karakteristika ovakvog oblika nasilja je da ono nije ograničen niti vremenom niti lokacijom odvijanja. Ovaj oblik nasilja utječe na velik broj mladih ljudi i rastući je trend zbog sve veće uporabe mobilnih uređaja među mladim ljudima, već od primarnog obrazovanja. MacEachern (2012), objašnjava što sve uključuje elektroničko nasilje, bilo da se događa putem e-maila, SMS-a, chata, bloga ili web stranice. Navodi najčešće odlike nasilnika elektroničkog nasilja, a to su: nazivanje pogrdnim imenima, širenje glasina i mržnje, razne prijetnje, utjecanje na ljude da budu posli prema drugima i da ih izbjegavaju, procjenjivanje koliko je netko ružan ili glup, nagovaranje nekoga da da nešto svoje, okrivljavanje ljudi za nešto što nisu učinili, ucjenjivanje drugih. Školski portal donosi nekoliko savjeta što škole mogu učiniti kako bi spriječile cyberbullying (Cyberbullying – kako ga spriječiti i savjeti za škole“, 2014):

- Škole bi trebale aktivno promicati svijest o kaznama za cyberbullying;
- Prijavljivanje cyberbullyinga bi trebalo uvelike olakšati. Trebalo bi angažirati i učenike u mehanizam prijavljivanja zlostavljanja;
- Nove tehnologije razvijaju se konstantno, zbog čega bi škole trebale uvijek biti informirane o upotrebama tehnologije kod mladih ljudi;
- Učenike bi trebalo podsjećati na potrebu za uključivanjem u odgovorno online ponašanje;
- Djeci i mladima treba pomoći da shvate što je zapravo bullying u njegovim raznim oblicima, te upozoriti na njegov utjecaj kroz sastanke i radionice. Djeci bi trebalo dati savjete o tome kako reagirati i informirati ih kome se mogu obratiti za pomoć;
- Za učitelje, ne-učiteljsko osoblje i roditelje trebali bi postojati regulirani anti-bullying informativni treninzi. Jedna osoba, obično školski ravnatelj, trebala bi preuzeti vodstvo u razvoju anti-bullying mjera.

Osim savjeta što bi škole trebale učiniti, postoji i nekoliko savjeta što bi učenici mogli učiniti. Primjerice, na društvenim mrežama ostaviti svoj profil privatnim ili bar

osigurati da objave vide samo prijatelji koje stvarno poznaju. Kod postavljanja osobnih podataka, slika ili bilo čega drugog na internet treba biti oprezan kako se nešto ne bi moglo zlouporabiti ili iskoristiti na manipulativan način. Također, dobro je biti upoznat sa sigurnosnim mjerama koje pružaju društvene mreže. Roditelji koji opuštaju djeci boravak na društvenim mrežama trebali bi znati kako je minimalna dob za registraciju veća nego što zapravo misle. Primjerice, za korištenje usluga informacijskog društva na društvenim mrežama kao što su Instagram, Snapchat, Twitter, Facebook, YouTube i WhatsApp, minimalna dob za registraciju je 16 godina. Djeca nažalost već i prije navršenih 16 godina imaju profile na nekoliko društvenih mreža i njima se koriste svakodnevno, vrlo često bez znanja njihovih roditelja. Iz tog razloga su vrlo ranjiva jer iz svog neznanja objavljuju razne sadržaje koje netko može zlouporabiti, objavljuju svoju lokaciju, dijele svoje osobne podatke s nepoznatim osobama i slično. Doza anonimnosti koji društvene mreže nude, djecu može lako očarati i lako mogu postati nasilnici na mreži, a još lakše i žrtve. Ako učenici postanu žrtve cyberbullyinga ni pod koju cijenu to ne smiju prešutjeti, već se trebaju povjeriti nekome kome mogu vjerovati i ispričati sve što se dogodilo. Sve dokaze koji upućuju na nasilje trebaju zadržati kako bi zlostavljači mogli odgovarati za svoja djela.

4. MEDIJSKA PEDAGOGIJA

Medijska pedagogija je pedagogijska disciplina. Miliša, Tolić i Vertovšek (2009) opisuju medijsku pedagogiju kao disciplinu koja sadrži sociopedagoške, sociopolitičke i sociokulturne analize u ponudama medija za djecu, mlade i ljudi treće dobi, te njihove kulturne interese u odrastanju, radu, slobodnom vremenu i obiteljskom životu. To je disciplina koja omogućuje nove koncepte i vizije, otvara nove mogućnosti komunikacije, mobilnosti i pronalaženja informacija. Medijska pedagogija sadrži sljedeće poddiscipline: medijski odgoj, medijsko obrazovanje, medijsku didaktiku, medijsku civilizaciju i medijsko znanstveno istraživanje. Što su ljudi više medijski obrazovani, time se pospješuje razvoj komunikacija. Kada govorimo o ulozi medijske pedagogije, prvenstveno treba shvatiti njezinu važnost. Miliša i sur. objašnjavaju kako se medijska pedagogija ne odnosi samo na temeljne zahtjeve odrastanja djeteta i mladih u svijetu medija i informacijsko-komunikacijskih tehnika, nego i na mogućnost korištenja informacija, na šanse obrazovanja, na razvijanje kompetencija i kritike nasuprot medijima koji su preuzeli manipulacijsku ulogu. U današnje vrijeme, tehnološki napredak uvelike olakšava i pruža mogućnosti pristupa informacijama iz medija, ali i manipulaciju s medijima. U suvremenim komunikacijama, odnosno u digitalnim medijima postoji šest funkcija medija (Miliša i sur., 2009, str. 115):

1. organizacija razmjene komunikacije;
2. razumljivost informacija;
3. socijalna organizacija društva;
4. kulturalna reprodukcija;
5. transfer komunikacije;
6. demokratizacija obrazovanja i interkulturalna funkcija.

Dvije osnovne značajke medijske pedagogije su komunikacija i komunikacijski mediji. Miliša i sur. navode (raz)otkrivanje skrivenih simbola kao temeljnu ulogu medijske pedagogije. Drugim riječima, mediji su nositelji poruka, a uloga medijske pedagogije je dešifriranje tih istih poruka. Iz tog razloga je važno da pojedinac, osim upotrebljavanja sadržaja medija, zna imaju li ti sadržaji odgojno-obrazovnu ili manipulativnu ulogu. Medijski odgoj mora voditi razvoju medijske kulture te stoga Miliša i sur. sugeriraju kako kolegij Medijska kultura treba razvijati u Hrvatskoj na

nastavnim sveučilištima kako bi se izvršili odgojno-obrazovni zadatci u sklopu suvremenog medijskog okruženja za nadolazeće generacije.

4.1. Medijska pismenost

Medijski odgoj, kao poddisciplina medijske pedagogije, bavi se usvajanjem medijske pismenosti i ovladavanju medijskih kompetencija. Glavna zadaća medijskog odgoja jest razgradnja sadržaja medija, odnosno prepoznavanje medijskog djelovanja i stjecanje medijskih kompetencija. To podrazumijeva sljedeće: analiza i procjena medijskih sadržaja, prepoznavanje funkcije medijskih sadržaja, razlikovanje stvarnosti od ”nerealnosti“ te prepoznati imaju li mediji manipulativno ili odgojno djelovanje. Prema Miliši, Tolić i Vertovšeku (2009), pojam medijske pismenosti odnosi se na sposobnost pristupa, analize, vrednovanja i odašiljanja poruka posredstvom medija. Također, Miliša i sur. spominju kako ona treba sadržavati funkcionalnu pismenost, vizualnu pismenost i računalnu pismenost. Funkcionalna pismenost podrazumijeva sposobnost razumijevanja onog što je napisano, vizualna pismenost podrazumijeva sposobnost razumijevanja vizualnih detalja, a računalna pismenost podrazumijeva korištenje računala, interneta i slično. Ciboci, Kanižaj i Labaš (2011) opisali su kako korištenje interneta predstavlja takozvanu ulaznicu u potpuni život, a tko nije medijski pismen u opasnosti je da ostane isključen iz života na različitim razinama. „Medijski pismena osoba je ona osoba koja je dobro informirana o temama koje se kreću u medijima, svjesna je svog svakodnevnog kontakta s njima i shvaća njihov utjecaj u obrazovnom ciklusu.“ (Miliša i sur., 2009, str. 169). Navedene komponente razvijaju se samo pod pretpostavkom da nastavnik ima razvijene medijske kompetencije. Kako bi se stekle medijske kompetencije i ostvario glavni cilj medijskog odgoja, važna je medijska pismenost koja predstavlja prvi korak u stjecanju medijskih kompetencija.

4.2. Medijska kompetencija

Pojam medijske kompetencije vrlo je važan pojam u medijskoj pedagogiji i, prema Miliši, Tolić i Vertovšeku (2009), ona omogućuje simbiozu znanja, sposobnosti i vještina u suživotu s medijima. Opisuju kako ona podrazumijevaju znanje, sposobnosti i vještine komuniciranja s medijima. Drugim riječima, medijska kompetencija

obuhvaća sposobnosti koje pojedinac mora usvojiti, a koje se odnose na izgradnju i razvoj kritičke interpretacije. Medijska kompetencija sadrži sljedeće čimbenike (Miliša i sur., 2009, str. 123-124):

a) individualna i demokratska orijentacija primatelja;
b) dekodiranje medijskih simbola;
c) aktivno korištenje medija: informacijska funkcija;
d) kritička refleksija;
e) razvitak kritičkog medijskog okruženja;
f) emancipiranost i motiviranost medijskog korisnika;
g) svjesnost pojedinca.

Kako bi se razvile pojedinačne medijske kompetencije postoje dva temeljna pojma: znati i moći. Pojam znati podrazumijeva znanje, a pojam moći podrazumijeva djelovanje. Isti pojmovi su važni i za provedbu pet osnovnih medijskih kompetencija. Miliša i sur. opisuju pet osnovnih dimenzija medijske kompetencije u medijskoj pedagogiji, a to su: kognitivna dimenzija, moralna dimenzija, socijalna dimenzija, estetska dimenzija i dimenzija djelovanja. Kognitivna dimenzija obuhvaća znanje, razumijevanje i analizu sadržaja u medijima. Moralna dimenzija temelji se na dva pojma: interakcija i osobnost pojedinca. Zagovara tezu da se mediji trebaju promatrati s etičkog stajališta. Sljedeća je socijalna dimenzija koja obuhvaća prava, medijsku politiku i socijalna djelovanja. Estetska dimenzija ukazuje na to da su mediji nositelji izražaja i informacijskih poruka. Medijski manipulatori najčešće koriste ovu dimenziju zato što estetski sadržaji pobuđuju emocionalne učinke koje mediji imaju na korisnike, neovisno kojoj dobnoj skupini pripadaju. Posljednja dimenzija je dimenzija djelovanja. Pomoću medija, korisnici se izražavaju i informiraju. Dimenzija djelovanja teži razvoju sposobnosti korisnika, ne samo da medije zna konzumirati, već i da se aktivno uključi u interpretaciju sadržaja medija. Drugim riječima, od pasivnog korisnika, stvoriti aktivnog. Miliša i sur. smatraju kako je proces kompetencije uspješan ako se u pojedinca razviju svih pet navedenih dimenzija.

4.3. Računalna i informatička pismenost

Računalna pismenost temelji se na deklarativnom i proceduralnom znanju o korištenju računala i poznavanju računala općenito (poznavati njegovu namjenu i slično). Temelji informacijske pismenosti predstavljaju prepoznavanje, traženje i vrednovanje kvalitete informacija. Ono što je zajedničko informacijskoj i računalnoj pismenosti je primanje, procesiranje i prenošenje informacija. „Računalna i informacijska pismenost je sposobnost pojedinca da koristi računala kako bi istraživao, stvarao i komunicirao radi učinkovitog sudjelovanja kod kuće, u školi, na radnome mjestu i u društvu.“ (Braš Roth i sur., 2013, str. 21). Braš Roth, Markočić Dekanić i Ružić (2013) objašnjavaju kako računalna i informacijska pismenost istovremeno predstavljaju i cilj i sredstvo obrazovanja jer učenici u školi uče koristiti informacijsko i komunikacijsku tehnologiju (IKT)[5], ali ju koriste i prilikom učenja. Iz toga proizlazi glavna zadaća razvijanja računalne i informacijske pismenosti, a to je da učenici razviju vještine i znanja vezana uz IKT te da razumiju ulogu IKT-a u obrazovanju i svakodnevnom životu, odnosno društvu. „Da bi ljudi mogli koristiti informacijsku pismenost u društvu znanja jednako im je potreban i pristup informacijama i sposobnost korištenja IKT-a“ (Braš Roth i sur., 2013, str. 21). Braš Roth i sur. opisuju kako se i medijska i informacijska pismenost odnose na sposobnost pristupanja informacijama i na sposobnost analiziranja i vrednovanja tih informacija te komuniciranja. Kao glavnu razliku navode to što medijska pismenost stavlja naglasak na izravno ispitivanje razumijevanja informacija i na oblike u kojima su informacije prikazane, dok informacijska pismenost stavlja naglasak na procese upravljanja informacijama i usredotočena je na statične tekstove, bili oni elektronički ili tiskani.

[5] Informacijska i komunikacijska tehnologija, IKT (engl. Information and Comunication Technology, ICT) – djelatnost i oprema koja čini tehničku osnovu za sustavno prikupljanje, pohranjivanje, obradu, širenje i razmjenu informacija različita oblika, tj. znakova, teksta, zvuka i slike. (http://www.enciklopedija.hr/natuknica.aspx?id=27406)

5. ZAŠTITA PRIVATNOSTI

Opća deklaracija o ljudskim pravima koja je proglašena na Općoj skupštini Ujedinjenih naroda 1948. godine predstavlja temeljni dokument za ljudska prava. Sastoji se od 30 članaka i njima se naglašava da svi ljudi trebaju imati ista prava te da se ne smiju diskriminirati bilo po spolu, rodu, rasi, vjeroispovijesti i slično. Članak 3. Opće deklaracije o ljudskim pravima (2009) navodi da svaki čovjek ima pravo na život, slobodu i osobnu sigurnost. Članak 7. navodi da svaki čovjek ima pravo na jednaku pravnu zaštitu, bez ikakve diskriminacije. Osim Opće deklaracije o ljudskim pravima, postoji i Deklaracija o pravima djeteta iz 1959. godine koja je usmjerena na sveobuhvatnu zaštitu dječjih prava i interesa. Deklaraciju o pravima djeteta (1959) usvojila je Generalna skupština Ujedinjenih Naroda, a trideset godina poslije, usvojila je i Konvenciju o pravima djeteta (1989). Konvencija o pravima djeteta predstavlja međunarodni dokument usvojen 1989. godine kojim se štite prava djece. UNICEF prenosi da je glavna razlika Deklaracije o pravima djeteta i Konvencije o pravima djeteta ta što Deklaracija ima moralnu snagu, dok Konvencija predstavlja pravni akt koji ima snagu zakona i obvezuje stranke na pridržavanje njezinih odredaba te uključuje pravo nadziranja primjene u državama koje su ju prihvatile i ratificirale (UNICEF, 2017). „Konvencija je jedinstvena po tome jer na sveobuhvatan način osigurava djeci građanska, politička, ekonomska, socijalna i kulturna prava; univerzalna je jer se primjenjuje na svu djecu, u svim situacijama, u gotovo cijeloj zajednici naroda; bezuvjetna je jer zahtijeva od svih država, neovisno o njihovom bogatstvu, da poduzmu aktivnosti vezane uz zaštitu prava djeteta; holistička jer zagovara gledište da su sva prava temeljna, nedjeljiva, međusobno ovisna i jednako važna.“ (Ajduković, Habar, 2016, str. 28).

5.1. Zakonska regulativa Republike Hrvatske

U Republici Hrvatskoj postoji nekoliko zakona koji se tiču sigurnosti, osobnih podataka i elektroničkih komunikacija. To su sljedeći zakoni: Zakon o informacijskoj sigurnosti (2007), Zakon o zaštiti osobnih podataka (2012) i Zakon o elektroničkim komunikacijama (2017). Zakon o informacijskoj sigurnosti određuje pojam informacijske sigurnosti, mjere, standarde i područja informacijske sigurnosti te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske

sigurnosti. Zakon o zaštiti osobnih podataka bio je na snazi do 2018. godine, ali sada je na snazi Opća uredba o zaštiti podataka[6] (2016) i Zakon o provedbi Opće uredbe o zaštiti podataka (2018). Opća uredba o zaštiti podataka Člankom 16. utvrđuje da svatko ima pravo na zaštitu svojih osobnih podataka s obzirom na njihovu obradu i kretanje tih podataka. Agencija za zaštitu osobnih podataka obavlja nadzor nad provedbom Zakona o provedbi Opće uredbe o zaštiti podataka. Zakon o elektroničkim komunikacijama (2017) obuhvaća korištenje elektroničkih komunikacijskih mreža i pružanje elektroničkih komunikacijskih usluga, pružanje univerzalnih usluga te zaštita prava korisnika usluga, zaštita podataka, sigurnost i cjelovitost elektroničkih komunikacijskih mreža i usluga i drugo. U Kaznenom zakonu (2011) Republike Hrvatske, 2002. godine propisano je novo kazneno djelo o dječjoj pornografiji. Članak 163. Kaznenog zakona opisuje kako će osoba koja iskorištava dijete za pornografiju na način da ga namamljuje, vrbuje ili potiče na sudjelovanje ili ga silom, obmanom, prijevarom prisili i navede na snimanje dječje pornografije, biti kažnjena zatvorskom kaznom. Zatvorska kazna može biti u trajanju od minimalno jedne do maksimalno dvanaest godina zatvora, ovisno o težini počinjenog zločina. Članak 164. navodi kako će osoba koja namamljuje, vrbuje ili potiče djecu ili ih silom i prijevarom prisili ili navede na sudjelovanje u pornografskoj predstavi, biti kažnjena zatvorskom kaznom u trajanju od minimalno jedne do maksimalno 12 godina, kao i u prethodnom članku. Također, zatvorskom kaznom kaznit će se i osobe koje gledaju pornografsku predstavu ako su znali ili su morali i mogli znati da u njoj sudjeluje dijete. Članak 165. propisuje kazne od šest mjeseci do pet godina zatvora osobama koje upoznaju djecu s pornografijom i pornografskim sadržajima. To podrazumijeva osobu koja djetetu mlađem od petnaest godina proda, pokloni, prikaže posredstvom računalnog sustava, mreže, medija ili na drugi način učini pristupačnim slike, audiovizualne sadržaje ili druge predmete pornografskog sadržaja.

5.1.1. Opća uredba o zaštiti podataka

U Republici Hrvatskoj Opća uredba o zaštiti podataka (GDPR) izravno se primjenjuje od 25. svibnja 2018. godine. Tehnološki razvoj bio je glavni pokretač donošenja takve

[6] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)

uredbe kojom se nastoje zaštititi prava pojedinaca u vezi s njihovim osobnim podacima i obradom tih istih podataka. Uredba se primjenjuje na sve tvrtke bez iznimaka, na pojedince koji obavljaju određenu profesionalnu aktivnost, udruge, bolnice, klubove, na fizičke osobe kada obrađuju osobne podatke izvan okvira potreba kućanstva (primjerice postavljanje video nadzora ispred ulaznih vrata kuće ili stana) te na sve državne institucije koje su dužne obrađivati osobne podatke u okviru odredaba, osim u slučajevima kaznenopravnih aktivnosti („Vodič kroz Opću uredbu o zaštiti podataka“, 2018). Kada se govori o osobnim podacima tada je riječ o svim podacima koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Drugim riječima, u Općoj uredbi o zaštitit podataka (2018) stoji kako su osobni podaci ime i prezime, identifikacijski broj, slika, glas, adresa, broj telefona, IP adresa, povijest bolesti, popis najdraže literature ili pjesama, odnosno svi podaci koji mogu dovesti do izravnog ili neizravnog identificiranja pojedinca. Kod prikupljanja osobnih podataka, u bilo kojem obliku, strana koja prikuplja podatke mora dati informaciju u koju svrhu se podaci prikupljaju, na temelju koje pravne osnove, tko sve može vidjeti te podatke te kako pojedinac može pristupiti svojim podacima, izmijeniti ih ili obrisati. Primjerice, škole i fakulteti prikupljaju podatke svojih učenika i studenata na on-line platformama za učenje. Svatko to je administrator takvih stranica mora napisati koji su nužni podaci koji se prikupljaju, koja je svrha prikupljenih podataka, kome se osoba može javiti ako ima bilo kakva pitanja u vezi svojih korisničkih podataka, navesti do kada se čuvaju prikupljeni podaci te kako se do njih može pristupiti, kako se mogu izmijeniti ili obrisati. Također, poželjno je navesti i prava korisnika prema Općoj uredbi o zaštiti osobnih podataka. Ako dođe do povrede osobnih podataka, tada znači da je došlo do slučajnog ili nezakonitog uništenja, gubitka, izmjene ili neovlaštenog pristupa nečijim osobnim podacima koji su bili obrađeni. Obrada podataka podrazumijeva sve radnje, od prikupljanja i bilježenja, do čuvanja, prenošenja i uništavanja. Podaci koji se obrađuju su osobni podaci zaposlenika, učenika, studenata, klijenata, pacijenata, članova udruga, korisnika društvenih mreža i slično. Prilikom obrade podataka važno je da je sve napravljeno po zakonu te da je pojedinac upoznat s postupkom i svrhom obrade, a da mu strana koja obrađuje podatke pruži sve dodatne informacije o sigurnosti osobnih podataka. Također, važno je da su nečiji osobni podaci točni i ažurni te da su čuvani samo onoliko koliko je potrebno u svrhu njihove obrade. Osoba koja obrađuje podatke, takozvani voditelj obrade, dužan je upoznati

pojedinca s njegovim pravima, a to su („Vodič kroz Opću uredbu o zaštitit podataka“, 2018):

- Pravo na informacije u sažetom, razumljivom i lako dostupnom obliku;
- Pravo pristupa do osobnih podataka;
- Pravo na ispravak osobnih podataka;
- Pravo na brisanje osobnih podataka;
- Pravo na ograničenje obrade osobnih podataka;
- Pravo na prenosivost podataka;
- Pravo na upućivanje prigovora.

U slučaju kršenja Opće uredbe o zaštiti osobnih podataka, odnosno u slučaju povrede osobnih podataka, sankcija uključuje novčanu upravnu kaznu. Prvo se utvrđuje postoji li kršenje i ako postoji, koje je težine, a nakon toga će se odrediti novčana kazna. Kod određivanja novčanog iznosa kazne u obzir se uzimaju kriteriji kao što su trajanje i težina kršenja, prijašnja kršenja, priroda kršenja, tehničke i organizacijske mjere primijenjene u obradi podataka, mjere ublažavanja štete, vrsta krivnje i slično („Vodič kroz Opću uredbu o zaštitit podataka“, 2018). Kod povrede osobnih podataka, voditelj obrade mora najkasnije 72 sata nakon saznanja o povredi izvijestiti nadzorno tijelo, odnosno Agenciju za zaštitu osobnih podataka, o istoj.

5.2. Povelja o sigurnosti djece na Internetu

Dan sigurnijeg interneta obilježava se 6. veljače. Godine 2018. na taj je dan potpisana prva Povelja o sigurnosti djece na Internetu u Hrvatskoj. Povelju o sigurnosti djece na Internetu (2018) potpisali su tri mobilna operatera (Hrvatski Telekom, Vipnet, Tele2), Hrvatska regulatorna agencija za mrežne djelatnosti HAKOM, Centar za nestalu i zlostavljanu djecu te Centar za sigurniji Internet uz podršku Ureda pravobraniteljice za djecu. Povelja je potpisana u cilju promicanja boljeg i sigurnijeg interneta i njegovog korištenja među djecom i mladima. Javno je potpisana kako bi se osvijestilo roditelje i javnost na važnost teme sigurnosti i zaštite djece i mladih na internetu, ali i stvaranje sigurnog okruženja za njih.

6. POSTOJEĆI PROJEKTI

U Republici Hrvatskoj postoji nekoliko projekata koji se bave problematikom sigurnosti djece i mladih na internetu. Ciljevi projekata i raznih istraživanja na tu tematiku uglavnom se podudaraju. Ističe se važnost sigurnosti djece na internetu, njihova zaštita od mogućih napada, prijevara, elektroničkog nasilja i slično, ali i edukacija koja će učiniti djecu, njihove roditelje i učitelje savjesnim korisnicima interneta na svrhovit način.

6.1. Sigurnih pet za sigurniji net

Projekt „Sigurnih pet za sigurniji net“ je projekt koji se provodio od kolovoza 2013. godine do prosinca 2014. godine. U projektu su sudjelovali učenici starosti od 7 do 10 godina, njihovi roditelji i učitelji iz pet osnovnih škola: OŠ Veliki Bukovec, OŠ ”Mato Lovrak“ Nova Gradiška, OŠ Popovača, OŠ ”Gripe“ Split i OŠ ”Mladost“ Osijek. Suradnici na projektu bili su Agencija za odgoj i obrazovanje, Hrvatska akademska i istraživačka mreža CARNET, Agencija za zaštitu osobnih podataka, Udruga ”Suradnici u učenju“, Općine Veliki i Mali Bukovec, Brodsko-posavska županija, Gradska i sveučilišna knjižnica Osijek, grad Nova Gradiška i Turistička zajednica Nove Gradiške. Za potrebe projekta stvoren je školski kurikulum „Sigurnost djece na internetu“ čiji se sadržaj razmatrao kao i rezultati njegova pilot testiranja na učenicima navedenih osnovnih škola. Također, stvoreni su i obrazovni sadržaji: udžbenici, priručnici, interaktivna multimedija, e-knjige. Svi stvoreni sadržaji za učenje i poučavanje objavljeni su online i dostupni su za korištenje na stranici „Sigurnih pet za sigurniji net“[7]. Ciljevi projekta bili su (Kralj, 2016, str. 61-62):

- Razviti i implementirati dio školskog kurikuluma o sigurnosti djece na internetu;
- Osvijestiti učenike, nastavnike, roditelje i širu javnost na razumijevanje problema vezanih uz sigurnost djece na internetu u sinergiji s politikama Europske Unije;
- Razviti područje školskog kurikuluma temeljenog na ishodima učenja o sigurnosti djece na internetu;

[7] Sigurnih pet za sigurniji net – http://www.petzanet.hr/

- Razviti i primijeniti popratni pedagoški model za učenje usmjereno na učenika;
- Unaprijediti digitalne kompetencije učenika i razviti kritički odnos prema odgovornom korištenju informacijsko komunikacijske tehnologije.

Rezultati istraživanja kojeg je provela Lidija Kralj (2016) na temu „E-sigurnost i digitalne vještine kao dio školskog kurikuluma“, a koji se odnose na rezultate pilot testiranja projekta Sigurnih pet za sigurniji net, pokazali su kako je stvoreni kurikulum ispunio očekivanja učenika te da su suvremene nastavne metode uspješno primijenjene. Rezultati i obrazovni sadržaji poslužili su kao pozitivno uporište u prijedlogu novog nacionalnog kurikuluma za međupredmetnu temu „Uporaba informacijske i komunikacijske tehnologije (IKT)“, ali i za predmet Informatika u osnovnim i srednjim školama.

6.2. Centar za sigurniji Internet

Centar za sigurniji Internet, kao što i samo ime kaže, predstavlja hrvatski nacionalni centar za sigurnost djece na internetu. Centar je osnovan 2012. godine u Zagrebu, a zajednički su ga osnovali: Hrvatska akademska i istraživačka mreža CARNET, Tehničko veleučilište u Zagrebu, Ministarstvo unutarnjih poslova, Ministarstvo uprave, Poliklinika za zaštitu djece grada Zagreba, Agencija za zaštitu osobnih podataka i Udruga ”Suradnici u učenju“. Osim osnivača, strateški partneri Centra za sigurniji Internet su: Agencija za odgoj i obrazovanje, Hrvatska regulatorna agencija za mrežne djelatnosti HAKOM, Ministarstvo socijalne politike mladih, Ministarstvo znanosti i obrazovanja, OŠ Veliki Bukovec, Učenički dom ”Hrvatskoga radiše“ Osijek i XV. gimnazija Zagreb. Kako piše na internetskim stranicama Centra za sigurniji Internet, aktivnosti centra baziraju se na rizicima i opasnostima kojima su izloženi svi koji su povezani na mrežu (odrasli, ali i djeca) te se tom problematikom bave iz različitih aspekata: psiholoških, pedagoških, informacijskih, zakonodavnih i sociooloških. Na svojoj internet stranici žele omogućiti roditeljima, nastavnicima i djeci da na jednom mjestu mogu pronaći informacije i obrazovne sadržaje koji pokrivaju sve aspekte koji se tiču sigurnosti djece na internetu. Stranica djeci, roditeljima te učiteljima i nastavnicima nudi razne priručnike, odgovore na razna pitanja, obrazovne igre, vodiče i brošure, kratke savjete, pojmovnik te aktualna događanja Centra. Glavna misija Centra za sigurniji Internet je postojanje referentnog centra znanja i vještina koji

postavlja standarde u sigurnosti korištenja interneta te promicanje vrijednosti internetskih tehnologija na dobrobit šire društvene zajednice (CSI, 2016). Također, Centar želi osvijestiti djecu, njihove roditelje i učitelje o pozitivnim i negativnim stranama interneta, mogućnostima korištenja interneta za istraživanje i učenje te ih osposobiti za primjereno i sigurno korištenje interneta.

6.3. Istraživanje EU Kids Online Hrvatska

Agencija za elektroničke medije zajedno s Unicefom svake godine u travnju organizira Dane medijske pismenosti kojima se promiče medijsko opismenjavanje djece u školama diljem Hrvatske. Na internet stranici Medijska pismenost[8] mogu se pronaći nastavni materijali za osnovne škole za učenike od 5. do 8. razreda pod nazivom „Sigurnost djece na internetu i elektroničko nasilje“ (Ciboci, Kanižaj, Labaš, 2018) koji su nastali u sklopu obilježavanja Dana medijske pismenosti. Materijali omogućuju da učitelji zajedno s učenicima analiziraju i vrednuju medijske sadržaje, bar na jednom nastavnom satu, te da tako postanu odgovorni korisnici medija. Također, na stranici Medijska pismenost mogu se pronaći i podaci o istraživanju „EU Kids Online Hrvatska“ iz 2018. godine. To istraživanje je prvo nacionalno reprezentativno istraživanje u Hrvatskoj o sigurnosti djece na internetu i internetskim navikama djece. U istraživanju je sudjelovalo 1017 djece u dobi od devet do sedamnaest godina i njihovi roditelji. Istraživanje je pokazalo kako djeca svakodnevno koriste internet i to najčešće preko mobilnog uređaja. Rezultati istraživanja dostupni su na internetskoj stranici HR Kids Online[9], a ovo su neki od izdvojenih rezultata koji bi trebali biti zabrinjavajući („EU Kids Online Hrvatska“, 2018):

- Gotovo svako dijete u dobi od 9 do 11 godina uvijek ima roditeljsko dopuštenje posjećivati društvene mreže (npr. Facebook, Snapchat, Instagram) iako je dobna granica za pristupanje većini društvenih mreža 16 godina;
- Svako osmo dijete u dobi od 12 do 14 i svako četvrto dijete u dobi od 15 do 17 godina u posljednjih se godinu dana susrelo uživo s osobom koju su upoznali na internetu;

[8] Medijska pismenost – https://www.medijskapismenost.hr/
[9] HR Kids Online – http://hrkids.online/

- Preko dvije trećine djece u dobi od 9 do 17 godina na internetu je u proteklih godinu dana vidjelo seksualne fotografije ili film gole osobe, a da im nije bila namjera vidjeti ih;
- Kada ih je zadnji put na internetu nešto uznemirilo ili zasmetalo, tek je svako deseto dijete u dobi od 9 do 11 godina tražilo pomoć od druge osobe (roditelja, učitelja ili prijatelja).

7. ZAKLJUČAK

Mnogi roditelji, zbog svog neznanja o medijima ili straha što bi djeca mogla raditi s medijima podliježu kaznama i zabranama. Kreću s pretpostavkom kako su djeca kompetentnija u korištenju interneta i ne preostaje im ništa drugo nego uskratiti djeci korištenje. To naravno može proizvesti kontraefekt jer će djeca možda baš iz inata poželjeti koristiti internet još više ili će ga koristiti u tajnosti, skrivajući to od svojih roditelja. Ako se djeca koriste internetom u tajnosti ili bez znanja roditelja, kada naiđu na neki neželjeni sadržaj velika je vjerojatnost da će to prešutjeti. Iz tog su razloga rezultati istraživanja zabrinjavajući jer su djeca već u osnovnoškolskoj dobi izložena seksualnim scenama, nasilnim scenama, nalaze se s nepoznatim osobama koje su upoznali na internetu, a sve to narušava njihov pravilan razvoj i ugrožava njihovu sigurnost. Većina djece koja naiđu na neki eksplicitni sadržaj ne znaju kako reagirati, prešućuju to roditeljima i u većini slučajeva se osjećaju neugodno, prestrašeno ili zbunjeno. To može narušiti njihov psihički razvoj i zato je važno educirati i djecu i roditelje na vrijeme kako djeca ne bi stekla neka traumatska iskustva koristeći se internetom. Roditelji trebaju biti svjesni da je internet dio svakodnevnog života njihove djece, ali i dio društvene kulture u kojoj žive te da se učestalim korištenjem javljaju određeni problemi na koje pedagozi i odgojitelji pokušavaju naći rješenja. U svemu treba biti umjeren, pa tako i u korištenju interneta, ali važno je znati koristiti se njime i kritički vrednovati dostupne sadržaje.

LITERATURA

Ajduković, M.; Habar, D. (ur.) (2016). *Prava djece – multidisciplinirani pristup*. Zagreb: Pravni fakultet Sveučilišta.

Braš Roth, M.; Markočić Dekanić, A.; Ružić, D. (2014). *ICILS 2013 – Priprema za život u digitalnom dobu*. Zagreb: Nacionalni centar za vanjsko vrednovanje obrazovanja – PISA centar.

Ciboci, L., Kanižaj, I., Labaš, D. (ur.) (2011). *Djeca medija – od marginalizacije do senzacije*. Zagreb: Matica hrvatska.

Ciboci, L.; Kanižaj, I.; Labaš, D. (2018). *Sigurnost djece na internetu i elektroničko nasilje. Nastavni materijali za osnovne škole za učenike od 5. do 8. razreda.* Zagreb: Agencija za elektroničke medije i Unicef.

Ciboci, L.; Kanižaj, I.; Labaš, D.; Osmančević, L. (2018.). *Obitelj i izazovi novih medija. Priručnik s radnim listićima za roditelje, nastavnike i stručne suradnike (treće dopunjeno izdanje).* Zagreb: Društvo za komunikacijsku i medijsku kulturu.Ž

Kralj, L. (2016). E-sigurnost i digitalne vještine kao dio školskog kurikuluma. *Medijske studije,* 7 (13), 59-74.

Laniado, N.; Pietra, G., prev. Modrić Tićak, N. (2005). *Naše dijete, videoigre, Internet i televizija: što učiniti ako ga hipnotiziraju?*. Rijeka: Studio TiM.

MacEachern, R., prev. Starc, B. (2012). *Cyberbullying: učini nešto – prekini lanac elektroničkog nasilja*. Zagreb: Mosta Viridis.

Maleš, D., Stričević, I. (2008). *Moje sigurno dijete*. Zagreb: Udruženje Djeca prva.

Miliša, Z., Tolić, M., Vertovšek, N. (2009). *Mediji i mladi: prevencija ovisnosti o medijskoj manipulaciji*. Zagreb: Sveučilišna knjižara.

Spitzer, M. (2018). *Digitalna demencija: kako mi i naša djeca silazimo s uma.* Zagreb: Naklada Ljevak.

Težak, Đ. (2010). *Internet – poslije oduševljenja*. Zagreb: Hrvatska sveučilišna naklada.

Živković, Ž. (2006). *Dijete, računalo i Internet*. Đakovo: Tempo.

Internetski izvori:

Centar za sigurniji Internet – CSI. (24.06.2016). *O nama*. Preuzeto s https://www.csi.hr/. Pristupljeno 13. lipnja 2019.

„Cyberbullying – kako ga spriječiti i savjeti za škole“. (06.02.2014). Preuzeto s https://www.skolskiportal.hr/clanak/213-cyberbullying-kako-ga-sprijeciti-i-savjeti-za-skole/. Pristupljeno 5. lipnja 2019.

Hrvatska akademska i istraživačka mreža – CARNET. (2018). *Sigurnije na Internetu*. Preuzeto s https://www.cert.hr/wp-content/uploads/2018/02/Sigurnije_na_internetu.pdf. Pristupljeno 15. srpnja 2019.

Hrvatska akademska i istraživačka mreža – CARNET. (2019). *Ne budi i ti hrvatski naivac*. Preuzeto s https://www.cert.hr/wp-content/uploads/2019/03/cert_naivci_brosura_web-1.pdf. Pristupljeno 15. srpnja 2019.

Hrvatska enciklopedija. (bez dat.). *Informacijska i komunikacijska tehnologija*. Preuzeto s http://www.enciklopedija.hr/natuknica.aspx?id=27406. Pristupljeno 13. srpnja 2019.

Hrvatska regulatorna agencija za mrežne djelatnosti – HAKOM. (2018). *Povelja o sigurnosti djece na Internetu*. Preuzeto s

https://www.hakom.hr/UserDocsImages/2018/dokumenti/Press%20release%20Potpisivanje%20Povelje%20o%20sigurnosti%20djece%20na%20internetu.pdf.
Pristupljeno 10. lipnja 2019.

Hrvatski Telekom. (bez dat.). *Što je roditeljska zaštita?*. Preuzeto s https://faq.hrvatskitelekom.hr/pages/category.xhtml?question=17391257.
Pristupljeno 5. lipnja 2019.

Narodne novine. (2009). *Opća deklaracija o ljudskim pravima* (NN 12/2009). Preuzeto s https://narodne-novine.nn.hr/clanci/medunarodni/2009_11_12_143.html.
Pristupljeno 12. lipnja 2019.

„O adware/spyware softveru“. (bez dat.). Preuzeto s https://www.cert.hr/adware/.
Pristupljeno 30. kolovoza 2019.

„O crvima“. (bez dat.). Preuzeto s https://www.cert.hr/crvi/. Pristupljeno 30. kolovoza 2019.

„O keylogger softveru“. (bez dat.). Preuzeto s https://www.cert.hr/keyloggeri/.
Pristupljeno 27. kolovoza 2019.

„O rootkit softveru“. (bez dat.). Preuzeto s https://www.cert.hr/rootkitovi/.
Pristupljeno 30. kolovoza 2019.

„O trojanskim konjima“. (bez dat.). Preuzeto s https://www.cert.hr/trojanski_konji/.
Pristupljeno 27. kolovoza 2019.

„O virusima“. (bez dat.). Preuzeto s https://www.cert.hr/virusi/. Pristupljeno 27. kolovoza 2019.

„Predstavljanje rezultata o izloženosti djece novijim oblicima rizičnog ponašanja u virtualnom svijetu“. (15.02.2018). Preuzeto s http://hrkids.online/. Pristupljeno 14. lipnja 2019.

„Ransomware“. (bez dat.). Preuzeto s https://www.cert.hr/19795-2/ransomware/>. Pristupljeno 30. kolovoza 2019.

Sigurnih pet za sigurniji net. (bez dat.). *Osnovne informacije o projektu*. Preuzeto s http://www.petzanet.hr/. Pristupljeno 11. lipnja 2019.

„Što je HTTP?“. (bez dat.). Preuzeto s https://korisnik.optimahosting.hr/knowledgebase/104/Sto-je-HTTP.html. Pristupljeno 20. srpnja 20019.

„Što je krađa identiteta?“. (31.08.2015). Preuzeto s http://azop.hr/aktualno/detaljnije/krada-identiteta-i-kako-se-zastititi. Pristupljeno 5. lipnja 2019.

Unicef Hrvatska. (2017). *Konvencija o pravima djeteta*. Preuzeto s https://www.unicef.hr/wp-content/uploads/2017/05/Konvencija_20o_20pravima_20djeteta_full.pdf. Pristupljeno 10. lipnja 2019.

„Vodič kroz Opću uredbu o zaštiti podataka“. (2018). Preuzeto s https://azop.hr/info-servis/detaljnije/vodic-kroz-opcu-uredbu-o-zastiti-podataka. Pristupljeno 22. srpnja 2019.

ZAKON HR. (2011). *Kazneni zakon*. Preuzeto s https://www.zakon.hr/z/98/Kazneni-zakon. Pristupljeno 12. lipnja 2019.

ZAKON HR. (2012). *Zakon o zaštiti osobnih podataka*. Preuzeto s https://www.zakon.hr/z/220/Zakon-o-zaštiti-osobnih-podataka. Pristupljeno 12. lipnja 2019.

ZAKON HR. (2016). *Opća uredba o zaštiti podataka*. Preuzeto s https://www.zakon.hr/z/1021/Op%C4%87a-uredba-o-za%C5%A1titi-podataka---Uredba-%28EU%29-2016-679. Pristupljeno 12. lipnja 2019.

ZAKON HR. (2017). *Zakon o elektroničkim komunikacijama*. Preuzeto s https://www.zakon.hr/z/182/Zakon-o-elektroničkim-komunikacijama. Pristupljeno 12. lipnja 2019.

ZAKON HR. (2017). *Zakon o informacijskoj sigurnosti*. Preuzeto s https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti. Pristupljeno 12. lipnja 2019.

ZAKON HR. (2018). *Zakon o provedbi Opće uredbe o zaštiti podataka*. Preuzeto s https://www.zakon.hr/z/1023/Zakon-o-provedbi-Op%C4%87e-uredbe-o-za%C5%A1titi-podataka. Pristupljeno 12. lipnja 2019.

PRILOZI

Izjava o samostalnoj izradi rada

Izjava kojom ja, Tea Mikšec, studentica Učiteljskog fakulteta Sveučilišta u Zagrebu, kao autorica diplomskog rada s naslovom „Sigurnost i zaštita djece u internetu“ izjavljujem da sam diplomski rad izradila samostalno pod mentorstvom doc. dr. sc. Predraga Oreškog. U radu sam primijenila preglednu/teorijsku temu i koristila se navedenom literaturom.