Zaštita podataka u virtualnom okruženju

Antolović, Vanesa

Sveučilište Jurja Dobrile u Puli
Fakultet za odgojne i obrazovne znanosti

VANESA ANTOLOVIĆ

ZAŠTITA PODATAKA U VIRTUALNOM OKRUŽENJU

Diplomski rad

Pula, veljača 2025.

Sveučilište Jurja Dobrile u Puli
Fakultet za odgojne i obrazovne znanosti

VANESA ANTOLOVIĆ

ZAŠTITA PODATAKA U VIRTUALNOM OKRUŽENJU

Diplomski rad

JMBAG: 0303089041, redovita studentica
Studijski smjer: Integrirani prijediplomski i diplomski Učiteljski studij
Predmet: Uporaba ICT u odgoju i obrazovanju
Znanstveno područje: Društvene znanosti
Znanstveno polje: informacijske znanosti

Mentorica: prof. dr. sc. Maja Ružić

Pula, veljača 2025.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisana Vanesa Antolović, kandidat za magistru primarnog obrazovanja ovime izjavljujem da je ovaj Diplomski rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Diplomskog rada nije napisan na nedozvoljeni način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, 20. veljače 2025.

IZJAVA O KORIŠTENJU AUTORSKOGA DJELA

Ja, Vanesa Antolović, dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj diplomski rad pod nazivom „Zaštita podataka u virtualnom okruženju“ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu sa Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, 20. veljače 2025.

Potpis

_____

Sadržaj

1. Uvod

Širok pojam zaštita podataka omogućuje fizičkim i pravnim osobama jednako koliko i korisnicima internetskih usluga pravo na zaštitu osobnih podataka. Korisnici virtualnog svijeta nesvjesno učestalo koriste svoje osobne podatke kada to ponekad dovodi do krađe istih. Zaštititi svoje podatke u virtualnom svijetu postaje sve teže jer su internetske prijevare dostigle potpuno novu razinu. Nikada nije bilo riskantno toliko izlagati svoje osobne podatke i informacije drugim ljudima, poduzećima, tvrtkama, zajednicama i slično. Nažalost, današnjica od nas zahtijeva da prije nego što se odlučimo upustiti u bilo kakvu vrstu razmjene podataka ili davanja podataka zbog osobnih potreba budemo kompletno sigurni u naše radnje i postupke. Metode kojima se koriste prevaranti kako bi otuđili podatke i zlouporabili iste postale su učinkovite, brze i nažalost u nekim slučajevima nepovratne. Sve češće svjedočimo raznim prijevarama putem interneta, a osim tehnoloških trikova, osobni podaci mogu nestati prilikom nepažnje. Posebno je važno naglasiti kako tehnologija svakim danom sve više napreduje i razvija se, a svijest o nesigurnosti i mogućim virtualnim napadima raste nekontrolirano.

Tehnologija i njene sposobnosti u usporedbi prije dvadesetak godina odnosno prilikom početka 21. stoljeća i sada je vidljiv nevjerojatno veliki i nagli preokret na tom području. Stvari kao što su zloupotreba osobnih podataka nismo u stanju predvidjeti. Ako se u kojem slučaju nalazimo u manjoj sredini, ne previše napućenoj i naseljenoj onda je naravno manja mogućnost da će se naši podaci iskoristiti protiv nas samih. Takve šanse uvijek su male u tim okolnostima, ali ako živimo u gradu koji raspolaže sa više od milijun stanovnika onda se šanse za pronevjeru podataka povećavaju.

Kao najranjivija skupina spomenute teme trenutno su to najmlađe dobne skupine odnosno sama djeca. Koračajući ka budućnosti djeca su podvrgnuta raznim rizicima u virtualnom svijetu te je ključno da se što prije educiraju o mogućim prijetnjama i opasnostima koje vrebaju na tom području. Djeca većinom svojom znatiželjom i znatnim nedostatkom iskustva povećavaju rizik od virtualnih opasnosti. Zato je potrebno držati na oprezu maloljetne skupine prilikom susreta s virtualnim svijetom kako bi se izbjegle moguće negativne posljedice.

Virtualnost pruža aktivno djelovanje, no ne nužno i javno djelovanje. Naime, riječ je o pojmu anonimnosti. Anonimnost kao takva i internet koji ju omogućava gotovo

uvijek, nažalost predstavlja srž problema. Akcije koje su skrivene sa korisnikove strane odnosno anonimne akcije predstavljaju veliki alat onih koji virtualni svijet koriste kao mjesto za zloupotrebu podataka. Zapravo se većina protuzakonitih radnji odvija anonimnim putem te je na taj način počinitelju teže uči u bilo kakav trag.

Kako bi se barem malo zaštitili od takve sudbine onda možemo računati na zakon i njegove opće odredbe. Uoči velike učestalosti krađe osobnih podataka zakon je proširio svoje uredbe i nadogradio iste. Postoji više zakona o očuvanju i zaštiti osobnih podataka zbog toga jer je Republika Hrvatska članica i pripadnica Europske Unije.

Naši osobni podaci nikada nisu bili na sigurnom mjestu niti će ikada biti, sami ćemo teško nadmudriti ljude koji se cijeli život bave krađom identiteta i osobnih podataka. Ljudi u većoj količini počinju shvaćati kakve bi to probleme moglo donijeti pa se tako i sve više njih osigurava na razne načine te štiti svoje podatke. Ovim diplomskim radom nastoje se istražiti ključni aspekti zaštite podataka u virtualnom svijetu, s posebnim naglaskom na zaštitu najranjivijih korisnika poput djece, ali i svih drugih skupina izloženih sveprisutnim rizicima modernog virtualnog svijeta. Rad je fokusiran na glavne prijetnje kojima su korisnici svakodnevno izloženi poput digitalnog nasilja, uključujući krađu identiteta, osobnih podataka i drugih sličnih kriminalnih radnji. Istovremeno rad je popraćen analizom uloge zakonodavnog okvira. „Opreza nikad dosta“ jedna je od značajnih poruka koje bismo se trebali držati prilikom zadiranja u virtualno područje i iskušavanja svega što ono nudi.

1.1. Opće činjenice o zaštiti podataka

Tema rada ujedno i ograničena posebnim provedbenim zakonom svake države koja je članica Europske unije jest zaštita osobnih podataka. Osobni podaci su oni koji pokazuju na identitet osobe koji se može utvrditi njima. Bilo to ime i prezime, adresa stanovanja, boravište, broj osobne iskaznice ili putovnice, kulturni profil, adresa internetskog protokola odnosno IP adresa ili podaci koje su u posjedu liječnika ili bolnice koji njime raspolaže, ali izrazito samo u zdravstvene svrhe. Osoba koja posjeduje podatke i ima svoj vlastiti identitet naziva se ispitanikom. Osobni podaci koji se ne mogu obrađivati su nečiji spol, rasno podrijetlo, politička uvjerenja i zastupanja,

vjera, kazneni postupci i ostalo. Osobne podatke može obrađivati samo voditelj obrade podataka koji odlučuje o svrsi i načinu upotrebljavanja podataka i izvršitelju obrade podataka je dopušteno čuvati i skrbiti o podacima te koristiti se njima umjesto voditelja.

Obrada podataka je dopuštena kada imate privolu pojedinca, ako su vam potrebni podaci za ispunjavanje ugovorne ili zakonske obveze, obrađivanje podataka u svrhu javnog, legitimnog ili životnog interesa. Ako vi obrađujete spomenute dokumente odnosno podatke onda pojedincima morate odmah dati do znanja tko ste, zašto to radite i u koju svrhu te tko će sve imati pristup tim navedenim podacima. Ako koristite bilo kakve podatke nasumičnog djeteta primjerice izrađivanje korisničkog računa na internetu onda je nužno kontaktirati roditelje i zamoliti iste za privolu korištenja djetetovih osobnih podataka. Ako se dogodi neusklađenost prema Općoj uredbi o zaštiti podataka onda za takve pronevjere može doći do izrazito velikih novčanih kazni u iznosu do 20 milijuna eura ili u postotku prometa vašeg globalnog poduzeća koji iznosi četiri posto. (Your Europe, 2021) Radi li se o podacima vezanim za radno mjesto, odnosima s javnošću, zdravstveni osobni podaci, korištenju internetskih platformi i stranica, kupnji materijalnih stvari i slično, uvijek može doći do zloupotrebe osobnih podataka.

Najveći sustav koji donosi takve zakone i odrednice naziva se Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda. Europska konvencija ima puno veći status nego što je pokazano, nadalje pomoću nje smo na neki način osigurani i sigurni te slobodni činiti određene stvari. Radi se o tome da svatko ima ljudsko pravo na privatan život pa tako i podatke odnosno informacije te privatne stvari unutar njega. Neovisno o društvenim mrežama koje posjedujemo, poslu koji radimo, hobijima kojima se bavimo i ostalim aktivnostima. Čovjek mora imati svoju slobodu i svoj mir do nekakvih granica.

Zbog kompletnog razvitka i napredovanja društvenih mreža te ostalih platforma koje su dio cijele zajednice dolazi do velikog problema pri potpuno osiguranoj zaštiti podataka. Usprkos svim visokim provjerama i povjerljivim stvarima koje su iznesene kao bitne lako su dohvatljive i pristupačne. Zarazne i pomalo neizbježne tehnologije koje su danas ovladale svijetom poput Instagrama, Twittera, one virtualne primjerice Skype, Zoom, Google Meet i Facebook ponajviše imaju veoma visoku razinu pristupačnosti dotične osobe odnosno mete, a željene informacije nije teško pridobiti

uz današnju zaštitu podataka. Hakeri te općenito ljudi koji nemaju poveznice s pravnim i državnim tijelima dolaze do stvari koje su im potrebne na najlakši mogući način pa tako i uz kršenje više određenih zakona. (Klarić, 2016)

S druge strane Zakon o zaštiti podataka na području Republike Hrvatske određuje kako je u nekim uvjetima dopušteno obrađivanje podataka ovisno zbog koje je to svrhe i namjene.

Virtualni svijet je preplavljen mrežnim stranicama kojima vjerujemo, ali jesu li to uistinu vjerodostojne mrežne stranice? Možemo li se pouzdano i sigurno koristiti mrežnim sjedištima misleći da su naši osobni podaci sigurni? Kada je riječ o stvarnom životu, ako postoji bilo kakva sumnja o određenom poslovanju ili tvrtki, to možemo provjeriti odlaskom na samu adresu navedenu u sklopu tog istog poslovanja. Što se tiče mrežnih stranica i provjere njihove legitimnosti korisnici su prisiljeni osloniti se na informacije koje mrežna stranica pruža, a te iste informacije ne moraju uvijek biti točne iako se čine takvima. Internet je zona dostupna apsolutno svima pa tako i informacije koje nalazimo na spomenutom. Kako bi sigurno zaštitili podatke preporuča se pažljivo čitanje pravila privatnosti i uvjeta korištenja s kojima se slažemo. (Aftab, 2003)

2.1. Počeci (ne)sigurnosti u virtualnom svijetu

Virtualni svijet nije mjesto već mnogo mjesta. Karakter tih mnogobrojnih mjesta nije istovjetan, a upravo te razlike proizlaze iz razlika u ljudima koji nastanjuju ta mjesta. (Lessig, 2004)

Primjerice, određene mrežne stranice isključivo su odgojno-obrazovne tematike poput sveučilišnih stranica ili e-knjižnica dok istovremeno postoje mjesta posvećena zabavi, društvenim interakcijama ili pak poslovnom umrežavanju. Vratimo li se na sam početak interneta, uvidjet ćemo da prethodno navedene mrežne stranice nisu postojala oduvijek.

Nekada nije bilo jednako lako biti dio virtualnog svijeta kao što to je danas. U davnim počecima interneta, pristup mreži bio je ograničen te je tada bila vještina znati koristiti se internetom. Povezanost nije bila toliko snažna kao u današnje doba, ali uspostavili su se odlični temelji za napredak. Tada je bilo omogućeno komuniciranje

isključivo pomoću elektroničke pošte odnosno u tekstualnom obliku, a sada je to moguće putem raznih društvenih mreža, aplikacija, programa i ostalih sličnih. Nakon poslužitelja elektroničke pošte, stvoren je protokol za prijenos hiperteksta što je omogućilo izgradnju velikog broja preglednika. Nakon nastanka preglednika, korisnici su počeli izrađivati mrežne stranice i međusobno ih povezivati s drugima.

Rast interneta kao takvog prouzročilo je i rast u pogledu prijetnji te rast nesigurnosti prilikom korištenja istog. Korisnici su često nepromišljeno provodili transakcijske procese preko internetskih trgovina te tako u više slučajeva ostali bez resursa na računu ili pak bili prevareni. S vremenom došlo je do programa koji su osmišljeni za identificiranje pronevjere te enkripcija koja je kreirana kako nepoznate osobe ne mogu dešifrirati podatke koji ne prepadaju njima.

U prošlosti samog interneta zaštite podataka nisu postojale te su se zakoni godinama gradili kako bi korisnici na neki način bili zaštićeni. Nakon učestalih prijava, sigurnosne provjere su se povećale te dostigle najstrožu razinu, a prijevare u virtualnom svijetu su se znatno smanjile. Zahvaljujući novonastalim protokolima i zakonima, kao što su GDPR (eng. General Dana Protection Regulation) to jest Opća uredba o zaštiti podataka, koja štiti privatnost korisnika, osigurava se bolja zaštita osobnih podataka. (Lessig, 2004)

3.1. Virtualni svijet i njegov značaj u suvremenom društvu

Da internet i njegove usluge još uvijek ne postoje u današnje vrijeme, mnogo toga bilo bi značajno drugačije. U smislu brzine širenja podataka, uspostavljanja komunikacije s drugim ljudima, otežan rad gotovo u svakom sektoru. Posao bi zapravo najviše bio u problemu jer bi sve spalo na fizički rad. Općenito poslovanje bilo bi veoma ograničeno, online sastanci ne bi postojali, a osvrnemo li se na globalnu povezanost, vjerojatno bi i taj proces bio otežan jednako koliko i suradnja u poslovnom smislu. Život bez pristupa internetu trenutno je nezamisliv, no u prošlosti život bez interneta nije se činio toliko otežan.

Ljudi bez pristupa internetu postoje i danas, bilo zbog financijskih razloga, geografske nepristupačnosti ili su to strogi osobni razlozi, ali i dalje je moguće biti dio zajednice, a s druge strane ne biti uključen u virtualni svijet. Međutim, ljudi koji su

svjesno ili nesvjesno u nikakvom doticaju virtualnog svijeta, nažalost su sigurno zakinuti aspektima poput loših društvenih veza ili lošeg obrazovanja, a ponekad se to odražava i na zdravstvenu zakinutost. Unatoč tomu, takvi ljudi vjerojatno svakodnevno imaju prouzročenu količinu stresa, žive mirniji život i opušteniji su. Nisu obasipani svakakvim informacijama na svakom kutku i većinom se to odražava na kompletan način života pa je poznato da inače takvi ljudi žive manje užurbanije i smirenije. (Brljafa, 2022)

Postoje i klasifikacije sadržaja odnosno medija koje korisnici svakodnevno konzumiraju. Dijele se na tradicionalne medije, konvergirane medije, nove medije i najnovije medije. Tradicionalni mediji prepoznaju se prema informacijama koje se distribuiraju iz jednog izvora za heterogenu publiku dok se konvergirani mediji održavaju putem komunikacije prema mnogima te sadrže značajke masovnih medija. Novi mediji odnose se na komunikaciju jedan prema jednome te je riječ o izravnoj komunikaciji sa svakim korisnikom što danas nazivamo e-poštom, videoigrama, blog i mrežnim sjedištima. Karakteristična komunikacija za virtualno područje najnovijih medija jest upravo ona gdje mnogi komuniciraju s mnogima. Takvu vrstu najnovijih medija i sadržaj svakodnevno pronalazimo na platformama poput Youtube-a, Twitter-a, Wikipedije i slično. (Zgrabljić Rotar, 2017)

Novi se mediji karakteriziraju podjelom na nekoliko značajki među kojima su – virtualnost, mobilnost, interaktivnost, konvergencija, digitalizacija i nova publika. Virtualnost je simulacija tehnologije na računalu koja je usko povezana s pojmom mobilnosti koji označava termine poput pokretljivosti i promjenjivosti. Interakcijom sam korisnik može utjecati na promjenu sadržaja ili unos istog, a od koje se sastoji cjelokupna virtualnost. Uz konvergenciju ističu se pojmovi poput radija, televizije ili primjerice različite platforme koje se međusobno spajaju. Digitalizacija obuhvaća proces pretvaranja i prevođenja analognih informacija i zapisa u digitalni oblik. Nova publika podrazumijeva participaciju u tehnologiji te kolaboraciju i suradništvo prilikom interaktivnosti. (Bilić, 2020)

3.1.1. Aktivni korisnici

Biti korisnik virtualnog svijeta gotovo je neizbježno, a trenutno se dijeli na dvije vrste korisnika odnosno pasivne i aktivne. Aktivni korisnici su osobe koje se aktivno gotovo svakodnevno uključuju u digitalne aktivnosti, često objavljuju putem

društvenih mreža ili foruma, dio su raznih online zajednica pa čak su i njihovi videozapisi dostupni na određenim platformama namijenjenim za iste. Biti aktivan član online zajednice nekima doprinosi u financijskom smislu pa tako neki korisnici u doslovnom smislu preživljavaju putem društvenih mreža, online poslovanja i slično. Međutim s aktivnom izloženošću virtualnom svijetu dolazi i do veće izloženosti potencijalnih rizika. Aktivni korisnici često dijele informacije iz privatnog života, bilo kroz sadržaj koji objavljuju ili kroz interakcije s drugim korisnicima.

3.1.2. Pasivni korisnici

Dok s druge strane pasivni korisnici uključuju one korisnike koji se koriste virtualnim svijetom pa gotovo i istom mjerom kao i aktivni, ali je razlika u tome što njihovi postupci i radnje ostaju gotovo neprimjetne ili minimalne. Takvi korisnici uglavnom promatraju sadržaj, ali pretežito se ne upuštaju u sudjelovanje online interakcija. Oprezniji su i paze na svoje osobne podatke u posebnoj mjeri, ne pretražuju često informacije, ne objavljuju sadržaj i ne ostavljaju trag na internetu kao što to aktivni korisnici učestalo rade. Bez obzira što ovakva skupina korisnika ne djeluje aktivno putem virtualnog svijeta i svega što ono sadrži, isti ti korisnici doprinose prometu na mrežnim stranicama kojima se koriste te podižu popularnost sadržaju kojeg prate. Popularnost je stvar korisnikova odabira, što više klikova to će popularnost biti veća. Pasivni korisnici, iako ne koriste virtualni svijet na način na koji to čine aktivni korisnici, doprinose povećanju broja pregleda i posjećenosti sadržaja. Te aktivnosti imaju značajan utjecaj na statističke pokazatelje, koji su od velike važnosti za kreatore sadržaja i aktivne korisnike društvenih mreža te za sve one koji intenzivno koriste internet. (Tandara, 2020)

4.1. Sigurnost na internetu

Prema Težak (2010) bit internetske sigurnosti jest upravo prevencija od neautoriziranoga pristupa i/ili prevencija od mogućeg oštećivanja računala internetskim priključkom.

Iz prijašnjih spomenutih činjenica kako ljudi nesvjesno razmjenjuju informacije preko računala, mreže, mobilnih uređaja pa čak i televizije. Bilo kakve informacije koje

nisu na domak ruke mogu biti ukradene sa strane profesionalaca. Porastom tehnologije takve informacije i podaci mogu biti ukradeni bez izvršavanja fizičke krađe računala ili mobilnog uređaja već prespajanjem na žrtvino računalo. Prilikom enormne krađe prijenosnih računala tokom presjedanja u hotelu, čekanja vlaka ili same vožnje do grada možemo u sekundi postati žrtva. Ako se želimo spasiti od gubljenja bitnih podataka i informacija važno ih je zaštiti na pravi način pa tako podatke nećemo nositi sa sobom i izlagati ih rizičnom transportu nego ćemo upravo te podatke spremiti odnosno kopirati na disk ili hardver jer zapravo nigdje nisu sigurni. Podaci i informacije koje se vežu uz nas mogu biti u svakom trenutku ukradene pomoću raznih aktualnih tehnologija. Filtri za ekran računala su jedni od njih pa tako bilo tko može očitati i spremiti osobne podatke koje se nalaze na osobnom računalu. Najveći rizik pružaju društvene mreže i samo uključivanje na njih te korištenje istih može naškoditi u izuzetno velikoj i nenadanoj mjeri. Na internetu dok surfamo se svakodnevno pojavljuju prozorčići za koje većinom mislimo da su virusi, ali ponekad nas samo jedan klik dijeli do nesvjesnog gubitka novca. Iz tog razloga korisnik mora jako dobro biti upućen u sadržaj prikazan na zaslonu kako bi bio siguran da mu klik na prikazanu ikonu „yes“ neće naškoditi novčano, fizički ili psihički. Takve su podvale česte i svakako treba pripaziti na njih, dolaze u svakakvim mogućim oblicima prevare. Jedne od njih su primjerice rasprodaja mobitela ili računala po skroz niskim cijenama ili izreka „obogatite se brzo“, rad kod kuće za kojeg je vrlo mala vjerojatnost da se pojavi u obliku reklamnog prozorčića na računalu pa se pitamo koliko je to zapravo istinito i ostale lažne podvale. (Marjanović i sur., 2008)

Naša sigurnost na internetu jednako je ugrožena kao i u realnom svijetu, jedina razlika jest ta da u realnom svijetu postoji nada da počinitelj odgovara za svoje posljedice. Postoji mnogo savjeta kako očuvati svoju sigurnost, a neki od najpoznatijih su korištenje jakih lozinki, izbjegavanje dijeljenja osobnih podataka i korištenje sigurnim i provjerenim alatima.

Sada je dostupna i identifikacija koristeći se dvaju faktorima te je trenutno najučinkovitija metoda zaštite korisničkih računa. Glavna svrha takve identifikacije je pružiti korisnicima dodatnu sigurnost odnosno dodatan sloj autentifikacije prilikom prijavljivanja na korisnički račun. Microsoft Security (2025) definira dvostruku provjeru autentičnosti kao sigurnosnu metodu upravljanja identitetima. Takva potvrda se odvija pristupom, a potrebna su dva oblika potvrde identiteta kako bi korisnik mogao pristupiti

resursima i potrebnim podacima. Dvostruka provjera autentičnosti služi tvrtkama te im omogućuje nadzor i zaštitu od najranjivijih podataka koji se nalaze u bazama i mreža. Postupak dvostruke provjere identiteta je brz i jednostavan, a učinkovito štiti podatke. Postoje razni načini kojima se provjera odvija, a pod to spadaju i provjera valjanosti SMS notifikacijama, glasovna provjera i provjera automatskim obavijestima. Korištenjem ove autentifikacije, čak i ako se slučajno dogodi da korisnik bude žrtva prijevare i lozinka bude ukradena, napadač bez druge sigurnosne provjere neće moći pristupiti podacima. (Microsoft Security, 2025)

Nadalje, korisnici bi trebali biti „izbirljivi“ kada je riječ o aplikacijama koje dovode u pitanje njihovu sigurnost. Prije samog pristupa određenoj mrežnoj stranici i dijeljenja osobnih podataka potrebno je dobro informirati se o određenom mrežnom sjedištu te proučiti recenzije drugih korisnika i provjeriti njenu vjerodostojnost. Informiranje o sigurnosti mrežne stranice uključuje i provjeru certifikata sigurnosti, zatim provjera HTTPS protokola i dobro čitanje uvjeta koji se tiču korištenja same mrežne stranice. Općenito je svaki oblik komunikacije koja se oslanja na mobitele i računala generalno nesiguran. Stoga se preporuča komunikacija na zaštićenijim Wi-Fi mrežama, a ne mobilnim podacima. (Vukoje, 2022) Uvjeti korištenja obično sadrže informacije kako se prikupljaju i obrađuju podaci koje korisnik pritom korištenja stranice svjesno unosi. Sadrži i informacije o pravima korisnika te pravilima ponašanja kao i mogućim posljedicama vezanima za kršenje tih istih pravila.

Važno je prepoznati legitimnost stranica. Uostalom, korisnik bi odmah trebao biti alarmiran ako u slučaju korištenja mrežne stranice primijeti da ista od njega traži nekakve potrebne informacije koje nisu nužne za njezino funkcioniranje.

Jedan od značajnijih timova odgovoran za sigurnosne incidente jest upravo CERT tim odnosno punog naziva: Computer Emergency Response Team. CERT tim kontinuirano prati promet unutar mreže kako bi prepoznao potencijalne prijetnje te obranio korisnike od istih. Kada se dogodi incident, cilj je zaustaviti napad te poduzeti mjere vezane uz smanjenje štete i rad na sprječavanju ponavljanja. Također, tim nudi i tehničku pomoć te sanacije prilikom posljedica napada. Kao podršku korisnicima nude i raznolike edukacije o sigurnosnim alatima. Kako bi poboljšali svoj rad ujedno i surađuju s nacionalnim i međunarodnim organizacijama. (CARNET, 2018)

4.2. Privatnost

Privatnost kao takva u virtualnom svijetu izaziva veliku moć. Upravo ta moć koja se postiže privatnošću stvara probleme kojima se virtualni svijet suočava svakodnevno. Prikriveni identitet oduvijek je davao značaj pravu na mišljenje i slobodi govora pa tako i danas, ali u realnom svijetu. Privatnost je jedno od osnovnih ljudskih prava vezano za identitet osobe i predmete koji su neposredno vezani za nju. Ovim pravom usko vežemo i komunikacijsku privatnost kojom podrazumijevamo osobne zapise poput primjerice, dopisivanja ili nekog drugog oblika komuniciranja. Temelji spomenute komunikacijske privatnosti i njene zaštite proizlaze iz Ustava Republike Hrvatske prema kojima su sloboda dopisivanja i njena tajnost nepovredivi. Pa je tako zakonom zabranjeno prikupljanje, korištenje i obrađivanje osobnih podataka u bez dopuštenja korisnika. (Boban, 2012)

Činjenica jest da sadržaj objavljen u virtualnom svijetu može ostati tamo duže vremensko razdoblje ako ne i zauvijek. Vezano za zakonodavni okvir prema članku 12. Opće deklaracije o ljudskim pravima „Nitko ne smije biti podvrgnut samovoljnom miješanju u njegov privatni život, obitelj, dom ili dopisivanje, niti napadima na njegovu čast i ugled. Svatko ima pravo na zakonsku zaštitu protiv takvog miješanja ili napada.“ (Narodne novine, 2009.)

Pravo na privatnost imaju i djeca gdje se Člankom 16. Konvencije o pravima djeteta to i zagovara, a glasi „Ni jedno dijete ili mlada osoba ne smije biti izloženo samovoljnom ili nezakonitom miješanju u njegov privatni život, obitelj, prepisku, niti smije biti izloženo napadima na njegovu čast i ugled. U slučaju takva miješanja ili napada dijete ima pravo na pravnu zaštitu.“ (Maleš i Stričević, 2005)

U realnom svijetu svakodnevno obavljamo radnje koje netko može promatrati pa je na taj način i to moguće ako smo dio virtualnog svijeta. Taj se dio može pretraživati, a u to spada zapis odnosno trag koji ostavljamo u virtualnom svijetu. Razlika između motrenja i pretraživanja jest upravo ta da motrenje možemo kontrolirati. To možemo učiniti na način da se sklonimo u svoju privatnost, podalje od svih. Pretraživanje nikada ne možemo kontrolirati jer ne znamo koliko daleko je dospio naš zapis i tko sve ima pristup istom. Na neki način, pretraživanje korisnicima ponekad narušava privatnost.

Razni sustavi koje koristimo prikupljaju podatke o tome što pretražujemo, koje poveznice slijedimo pa čak i kako se ponašamo na internetu. Korisnici nisu potpuno svjesni koliko se podataka prikuplja o njima te kako ti podaci mogu biti upotrijebljeni bez njihovog znanja. Primjerice, zapis o našoj elektroničkoj pošti smatramo sasvim bezopasnim, ali trebali bi obratiti pozornost kakav sadržaj primamo, a kakav šaljemo. Elektronička poruka sadrži slične vrijednosti kao na primjer pismo gdje dolazi neplanirano, ali sadržaj koji smo primili putem pisma se ne pohranjuje dok za elektroničku poruku ne vrijedi isto. Kada se jednom pohrani, e-poruku se može pretraživati ili arhivirati. Mobilni telefoni narušavaju privatnost prilikom upotrebe lokacije. Lokacija može biti stalno dostupna te na taj način pohranjivati informacije o kretanju. (Lessig, 2004)

Poznato je kako većina internetskih preglednika koje korisnici posjećuju zadržava tu evidenciju u svojoj bazi posjeta. Mnogi korisnici koriste se i incognito opcijom koja definira značajku privatnog pretraživanja. Što bi značilo da ako privatno pretražujemo informacije na mrežnom pregledniku te aktivnosti neće biti zabilježene ili pod sustavom praćenja.

To funkcionira na način da unutar običnog mrežnog preglednika otvorimo novu karticu koja je zasnovana na privremenoj sesiji te upravo ta sesija nije ista kao i kod običnog pretraživanja. Ova značajka postoji još od 2005. godine zahvaljujući tvrtki Apple, a prepoznatljiva je po tome što internet preglednik ne sprema lozinke ili prijave koje korisnik zabilježi tokom svog pretraživanja. U tom slučaju povijest se automatski ne može pregledati, a ukoliko se takav način rada upotrebljava u nekakvoj firmi, onda ista može zadržati te informacije. Primjerice, djeca ponekad ne žele da im roditelji saznaju što su pretraživali pa se koriste takvom vrstom pretraživanja. Neki se zlonamjerno koriste ovakvim tipom pretraživanja dok drugi ne. Glavno pitanje jest upravo koliko je takvo pretraživanje konkretno u anonimnom načinu rada uistinu privatno?

Kada korisnici pretražuju bilo kakav sadržaj na internetu koristeći se anonimnim načinom ne znači da su njihove kretnje nezabilježene. Primjerice, ako na tabletu ili prijenosnom računalu korisnik sa svojim korisničkim računom pretražuje pomoću anonimnog načina onda te radnje neće biti zabilježene na njegovom računu, odnosno povijesti gledanja. Konkretno aktivnosti gledanja neće biti dostupne ostalim osobama

koje se koriste tim tabletom ili prijenosnim računalom. Dok će na tim internetskim stranicama koje je korisnik posjetio biti zabilježen njegov posjet. Ako na primjer korisnik želi te podatke kojim je stranicama pristupio, kada i što je pretraživao – moguće je dobiti ih upitom direktno na samu mrežnu stranicu.

Zato je važno prisjetiti se upravo te činjenice da informacije koje pretražujemo nikada ne nestaju i uvijek su negdje zabilježene. U virtualnom svijetu uvijek ostaje digitalni otisak koji sadrži svu bazu podataka aktivnosti. (Centar za sigurniji internet, 2024)

2. Zaštita podataka na temelju Opće uredbe o zaštiti podataka

Pravni okvir za osobnu zaštitu podataka na području Europske unije jest Direktiva Europskog parlamenta i Europskog vijeća. Takav okvir je stvoren kako bi podaci mogli nesmetano prijeći iz jedne u drugu država koja se nalazi na području same Europske unije odnosno ta država je članica iste. Uz to bi se osobni podaci koji bi bili preneseni ujedno sačuvali te pojedinac ne bi izgubio pravo na vlastitu zaštitu podataka.

Države koje su članice Europske unije i samog postupka prijenosa osobnih podataka bi trebale osigurati da se ti podaci prenesu zakonski i pošteno. Na punu snagu od 25. svibnja 2018. godine stupila je EU Opća uredba koja sadrži zakone o ljudskim pravima te slobodi kretanja. Takva uredba napisana je kako bi što više modernizirala i pogurala napredovanje na području zaštite osobnih podataka. Korisnicima se na lakši i bolji način predočuje njihovo upotrebljavanje osobnih podataka usprkos svim današnjih vrstama komunikacije, medijima i široko obuhvaćenim društvenim mrežama prema Radelić i suradnicima (2017).

Jedne od najvažnijih odredbi su da svaka osoba odnosno svaki korisnik ima pravo na zaštitu podataka te se jamči pravna sigurnost i transparentnost. Uredba uvodi sasvim nove načine za pohranu podataka, a kao primjer možemo protumačiti pseudominizaciju. Ovaj postupak sadrži potpuno novu metodu pohrane podataka na način da se više ne mogu izravno povezati s određenom osobom koja je vlasnik tih podataka bez korištenja dodatnih informacija. Podrazumijeva se da privola koju potpisujemo kad to želimo odnosno kad je to potrebno onda svjesno i dobro informirano te dobrovoljno to radimo. (Zakon.hr, 2018)

Osoba mora biti svjesna da se njeni podaci automatizirano cijelo vrijeme obrađuju. Ovakva zaštita podataka nastala je upravo iz razloga kako bi državama koje su članice Europske Unije omogućila osiguranje osobnih podataka. Nadzornik ih mora zaštititi od gubitka koji može biti nezakonit ili nenamjeran odnosno slučajan, neovlaštenog ili zabranjenog pristupa. (Klarić, 2016)

Pravo na privatnost ujedno je jedno od najvažnijih i temeljnih ljudskih prava. (Krbavac, 2023.) No, isto tako postoji i Zakon o pravu na pristup informacijama koji se nalazi unutar Opće uredbe o zaštiti podataka. Taj pristup informacijama imaju

dozvoljene samo javne vlasti koje propisuju načela, ograničenja, djelokrug, način rada i između ostalog inspekcijski nadzor nad provedbom ovog Zakona. Prema samoj Općoj uredbi u nastavku je navedeno nekoliko Zakona koji se strogo vežu za zaštitu podataka pojedinca.

(1) Članak 5. – Načela obrade podataka

- Osobni podaci moraju se obrađivati zakonito, pošteno i transparentno.
- Podaci se prikupljaju u jasno definirane i legitimne svrhe.
- Mora se osigurati minimalizacija podataka, točnost i ograničenje čuvanja.

(2) Članak 12. Informiranje ispitanika o obradi mora biti transparentno.

(3) Članak 13./14.Pravo na obavijest; ispitanici moraju biti informirani o prikupljanju i obradi njihovih podataka.

(4) Članak 17. – Pravo na brisanje

- Ispitanik ima pravo zahtijevati brisanje njegovih osobnih podataka ako više nisu potrebni, ako je privola povučena ili ako se podaci obrađuju nezakonito.

Dakle, Opća uredba o zaštiti podataka (GDPR – eng. General Data Protection Regulation) predstavlja jedan od najbitnijih Zakona privatnosti i zaštiti podataka pojedinca. S ciljem pružanja sveobuhvatnog okvira, dobro je koncipirana jer pokriva širok raspon mogućnosti. Uredba je uređena tako da pruža zaštitu u cijelom životnom ciklusu podataka – od prikupljanja i obrade do pohrane podataka i brisanja istih. Neke od ključnih prednosti GDPR-a su upravo globalna primjena te fleksibilnost podložna mogućim tehnološkim promjenama. (Barjaktar i Ivanović, 2019)

2.1. Zakonska regulativa zaštite podataka u Republici Hrvatskoj

Pitanje zaštite podataka u Hrvatskoj je na ustavnoj razini te se radi o sustavu Zakon o zaštiti podataka. Napismeno se može uvidjeti u Ustavu Republike Hrvatske u trećem poglavlju pod nazivom *Zaštita ljudskih prava i temeljnih sloboda* koje vodi na drugo potpoglavlje pod nazivom *Osobne i političke slobode i prava* u članku 39. se navodi sljedeće: „Svakome se jamči sigurnost i tajnost osobnih podataka. Bez privole

ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Zakonom se uređuje zaštita podataka te nadzor nad djelovanjem informatičkih sustava u državi. Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihovog prikupljanja“. Ovim riječima jasno je kako se takvo pravo i sam zakon odražava na svaku fizičku osobu diljem cijele Republike Hrvatske.

Ključne točke zakona navode prava građana u vezi s obradom osobnih podataka, obveze tijela javne vlasti i drugih subjekata koji obrađuju osobne podatke te postupanje s podacima u skladu s propisima. (Narodne novine, 2012)

3. Zaštita računala u virtualnom svijetu

Zaštita računala u virtualnom svijetu nije pitanje izbora već nužnosti. U vremenu kada se većina radnji odvija u virtualnom svijetu uključujući svakodnevne aktivnosti poput internet kupovine, plaćanje računa, razvijanje i održavanje komunikacije, sigurnost korisnika postaje glavna zadaća. Nažalost, što više tehnologija napreduje to je i sve veći rizik od prijetnji koje se odvijaju putem računala. Računalo je podložno različitim vrstama prijetnji primjerice zlonamjernom softveru, socijalnom inženjeringu, krađi identiteta, mnogim hakerskim napadima te *phishing* napadima. U nastavku rada te su prijetnje pomno sagledane i analizirane.

3.1. Zaštita računala od hakera

Pojam *haker* ima puno definicija koje ga opisuju, no najpoznatija je ona koja ga opisuje kao osobu koja se bavi računalima i njihovim sustavima te programira, a istovremeno je ekspert za pronalaženje slabosti u računalnim programima, softverima i mrežama. Haker ne mora nužno biti vezan uz negativno značenje, ali većinom se spominje upravo u takvom smislu.

Većinom hakeri napadaju svoje mete zbog određenih motiva, a nekada je to i zbog informacija koje su nedostupne. Većinom do napada dolazi zbog želje za određenim informacijama i podacima. Hakeri su počeli djelovati vrlo rano obzirom na svojevrsnu tehnologiju pa ih tako raspodjeljujemo na tri vrste: crne, bijele i sive hakere. Crne hakere klasificiramo kao one koji su poznati po svojim zlim namjerama kao na primjer oni koji kradu osobne podatke i informacije koje bi mogle oštetiti pojedinca na neki način. Takvi hakeri su većinom profesionalci koji jako dobro poznaju sustav i njegove slabosti. Većinom isti žive od hakerstva i bave se tim ozbiljno, ali ilegalno. Sivi hakeri nisu nužno oni koji dođu do informacija kao crni nego oni uzimaju informacije od crnih hakera koje su već ukradene. Dok se bijeli hakeri koriste svojim znanjem kako bi poboljšali mreže, sustave i softvere. Bijeli hakeri većinom su obrazovani programeri koji su zaposleni u raznim tvrtkama ili institucijama i koriste iste metode crnih hakera, ali u dobre svrhe.

Svima je opće poznato da hakeri ulaze u željene sustave tako da dešifriraju šifru. Tu dolazimo do bitne grane koja godinama služi za zaštitu podataka –

kriptografija. Kriptografija sakriva poruke pomoću enkripcije – šifre. Zahvaljujući enkripciji, podaci ostaju skriveni, a s druge strane zaštićeni od napada hakera.

Ciljevi hakerskog napada pretežito su raznovrsni, te se isti planiraju danima, mjesecima, a oni zahtjevniji nekada i godinama. Većinom taj plan izgleda kao nekakvo otkrivanje lozinki, probijanje sigurnosnih zidova i šifri, a ispitivanje je većinom pogađanje lozinki dok se ista ne otkrije raznim generiranjem mogućih lozinki. (Vrančić, 2019)

3.2. Zaštita računala od virusa

Prema CERT-u, računalni virus čini računalni program koji je u stanju zaraziti računala svojom reprodukcijom tako da postupke bez dopuštenja korisnika kopira u samog sebe odnosno u svoju memoriju kojom se koristi. Često se i pojam virus povezuje s programima za oglašavanje i programima za prikupljanje podataka. Virus dospije do računala tako da se širi s jednog na drugog u obliku nekakvog zlonamjernog koda. Takav kod može se nalaziti dok se korisnik koristi internetom i njegovim uslugama ili se kod nalazi u raznim privicima koji se prenose elektroničkom poštom. Virus se može širiti i upotrebom hard diska ili USB diska, a da korisnik nije ni svjestan. Prilikom prebacivanja podataka na vlastite spremnike memorije potrebno je dobro sagledati o kakvim se podacima radi i s kojeg mjesta su dospjeli na naše računalo. Virus se također može brže i efikasnije širiti ako se datoteke zaražene virusom nalaze na mrežnom poslužitelju koji istovremeno koristi više korisnika. Virus i njegovo djelovanje veoma je opasne naravi tako da korisnici trebaju biti što oprezniji prilikom širenja podataka i primanju istih.

Sama vjerojatnost da će virus dospjeti na vaše računalo prilikom pretraživanja informacija na internetu je znatno mala, ali kada se to dogodi oporavak je podosta dugotrajan, a ponekad zna zahtijevati i tehničku podršku pa tako kompletno čišćenje računala nije na odmet u tom slučaju. Naravno, podrazumijeva se da se računalo ne može zaraziti samo ako se određene mrežne stranice posjećuju već ako korisnik dovede virus na računalo. Virus sam po sebi nije teško otkloniti te za to služi antivirusni program koji se preporuča korisnicima da preuzmu na računalo kako bi spriječili širenje virusa. No, ako je računalo već zaraženo, antivirusni program neće djelovati jer on primarno služi za prevenciju, a ne onda kad virus već zarazi računalo. (Aftab, 2003)

Program za antivirusno djelovanje funkcionira na način da cijelo vrijeme skenira uređaj, u ovom slučaju računalo te neprestano prati sve datoteke, programe i aplikacije odnosno sve zapise kako bi osigurao računalo od potencijalnih prijetnji i zaštitio isto. Zbog toga kada antivirusni program bude naišao na jedan od virusa, na ekranu će se pojaviti obavijest koja će jasno korisniku dati do znanja sve informacije o zaraženoj datoteci. Pri samoj instalaciji antivirusnog programa, ono od korisnika traži da odabere razinu zaštite kojom se žele koristiti. Najniži stupanj zaštite pokreće samo korisnik te se takva razina smatra podosta nesigurnom upravo zbog toga jer se zna dogoditi da korisnik zaboravi samostalno provjeriti opasnost od virusa. Dok najviši stupanj zaštite podrazumijeva automatiziran nadzor svih mogućih zapisa koji dospijevaju na računalo. (Kušer, 2016)

Osim računalnog virusa postoje i ostali oblici koji djeluju slično virusu, ali ih pronalazimo djelovanjem kroz druge načine, a navedeni su jedni od najčešćih i najrasprostranjenijih:

- Crv nazivamo računalnim kodom koji se ne mora nužno širiti uspostavom korisničke interakcije pa su tako većinski oblici crva rasprostranjeni putem elektroničke pošte koja će zaraziti računalo nakon otvaranja. Virus crva traži zaražene datoteke kao što su primjerice adresari te kasnije oponaša ili lažira adrese pošiljatelja kako bi korisnik mislio da su od nekoga koga poznaje.
- Trojanac se prepoznaje kao zlonamjerni softverski program koji se ujedno i krije unutar drugih programa. Takav program dolazi na računalo sasvim normalnim putem legitimnog programa, ali nakon ulaska u računalo, ono umeće kod u operacijski sustav, što će naravno hakerima omogućiti pristup računalu koje je zaraženo. Ovakvi programi nisu poznati po tome da se samostalno šire već to rade putem virusa, crva ili nekakvog preuzetog softvera. (Microsoft Support, 2025)

3.3. Zaštita računala od prijevara

Svjesni smo da se s porastom digitalizacije pojačala i opreznost prema ekranima pogotovo zbog internetskih prijevara. Internetske prijevare svakim danom su

raznovrsnijeg karaktera i oblika pa tako žrtve nasjednu na jednu od prijevara ne znajući pritom da postaju subjekt kaznenog djela. Najčešći razlog prijevara jest upravo vezan za financijska sredstva korisnika. Kriminalci igraju na nepažnju i povjerenje korisnika, a korisnici nisu ni svjesni što se zapravo zbiva.

Zbog manjka socijalne izolacije, starijim je ljudima lakše manipulirati, u ovom slučaju ljudi starije životne dobi postaju najdraža meta internetskih prijevara. Skupina takvih ljudi općenito je manje tehnološki nastrojena nego što su to primjerice osobe srednje dobi kojima je tehnologija ipak malo bliža u smislu baratanja istom. Nadasve, stariji ljudi smatraju se i imućnijima pa tako isto spadaju u ranjivu skupinu. Osobe starije životne dobi nisu tehnološki sposobne za prepoznavanje „dobrih“ od „loših“ mrežnih stranica pa tim putem nasjedaju na razne prijevare. Ne prepoznaju zlonamjerne kodove, virusne datoteke ili pak lažne identitete. Zaštita starijih osoba može se povećati na taj način da ih osvijestimo te educiramo o mogućim opasnostima te pružimo pomoć ako je potrebna u situacijama koje slute na prijevaru. (Stanković, 2024)

Napadi koji se dogode i oštete korisnika u financijskom smislu ili pak nekom drugom većinom ostaju nekažnjeni zbog nemogućeg pronalaska počinitelja. Počinitelj može djelovati iz bilo kojeg dijela svijeta te policija jednostavno postaje ograničena kada je riječ o internetskoj prijevari. Žrtve spomenutih računalnih prijevara nasjedaju na svakakve ponude s druge strane ekrana koje se čine primamljivima i sigurnima te na kraju obećavanje velikih nagrada za malu uloženu svotu novca postaje prava noćna mora. Naime, žrtve su u tom trenutku jako sklone donositi impulzivne odluke, pogotovo mete za koje počinitelji znaju da im je potreban novac. Počinitelji sve pomno planiraju te taktički spremaju napad kako žrtva ne bi ni posumnjala da je riječ o prijevari. Također, isti se veoma služe žrtvinim slabostima koje su prije samog napada pomno proučili. Kada je riječ o novcu koji s realnog gledišta pokreće svijet, svaki korisnik kojemu je novac slaba točka, pronaći će cijenu koju je spreman platiti da postane „milijarder“ preko noći.

Također, sve su češće prijevare putem internetskih oglasa, a prijevare se pojavljuju u obliku reklama. Reklamiraju se skupocjeni automobili, odjeća i obuća poznatih marki, mobiteli i slično. Prevaranti od žrtava traže uplatu, a zatim žrtve prilikom dostave shvate da su nasjeli na jednu od prijevara jer ne stigne ono što su naručili već prazna kutija ili nasumični predmeti koji su iznimno male novčane

vrijednosti. Teško je identificirati počinitelja ovakvog tipa prijevare jer nakon što uplata bude izvršena i proknjižena, briše se svaki trag identiteta istog. U trenutku kada se gubi svaki trag počinitelju, nažalost postaje gotovo pa nemoguće da isti kazneno odgovara za svoje posljedice.

Jedna od najčešćih vrsta napada je upravo ona ljubavne naravi, a obično se naziva takozvanom romantičnom prijevarom. Namijenjena je za osobe ženskog spola, a koje su većinom udovice ili nesretno rastavljene pa čak to ponekad budu i osobe u nesretnom braku. Romantična prijevara je ona koja uspijeva korisnike okrenuti same protiv sebe koristeći se upravo njihovim najvećim slabostima – emocijama. Prevaranti često nazivani i romantični prevaranti koriste se pretežito društvenim mrežama, aplikacijama za upoznavanje i drugim digitalnim platformama kako bi upoznali svoju „ljubav“. Dok s druge strane žrtva ne sluti kako će biti dio iskorištavanja u financijskom smislu. Prevaranti kada pronađu ciljanu osobu mogu i mjesecima planirati rasplet okolnosti. Planiraju napad tako da druga strana nikad ni ne nasluti na prijevaru. Sve zvuči veoma istinito i realno da se čak i koriste fotografijama prilikom dopisivanja kako žrtva ne bi ni u kojem slučaju posumnjala. A neki se koriste raznim programima i efektima kojim kreiraju identitet kojim će se koristiti putem video poziva pa tako još manje izazivaju sumnju. Počinitelji izmišljaju priče koristeći se lažnim identitetima kako bi zvučali i izgledali kao idealni partner. Žrtva tada ne razbire lažno od stvarnosti te pada na emocije koje presuđuju neočekivan splet okolnosti. Pobuđivanjem najdubljih ljudskih osjećaja žrtve se ulove u zamku pa su tako u začaranom krugu svakodnevnih manipulacija, spletkarenja i iskorištavanja. Mnoge žene bile su prevarene te su neke čak i ostale bez svega u materijalnom smislu te bile primorane početi život iznova. Na tu temu donedavno je nastao velik broj filmova i članaka koji upućuju na oprez prilikom upuštanja u svakojake odnose preko društvenih mreža.

Isprve je tu bio minimalan broj žrtava te je podjednako bilo ženskih i muških, a sada se broj takvih prijevara pretežito povećao te su žene te koje su većinskim djelom žrtve. (Goljački, 2022)

Među opasnim prijevarama smatra se i ona pod nazivom *Direktorska prijevara*. Direktorska prijevara funkcionira na način da se varalice prave kao šefovi od žrtve koji na taj način žele izvući novac i prevariti korisnika. Primjerice lažira se elektronička pošta od direktora te se zatim imitira način komunikacije, a ciljana publika jesu upravo

radnici u administrativnom djelu ili računovodstvenom gdje se od njih traži da izvrše hitnu uplatu. Radnici odnosno žrtve u ovom slučaju većinom postupe kako im je rečeno zbog povjerenja koje imaju prema svojim šefovima te su skloni slijediti upute osoba koje se nalaze na visokom položaju. Većinom je taj zahtjev od počinitelja hitan pa tako dodatno stvaraju pritisak i stres žrtvama. (Ministarstvo unutarnjih poslova, 2025)

Prema Ministarstvu unutarnjih poslova (2025) najučinkovitija obrana jest upravo obrazovanje žrtava koje su potencijalne prijetnjama. MUP navodi kako to može biti svatko od nas te je važno podizati svijest o ovakvim problemima u društvu.

3. 4. *Cyber* napadi

Ovisno o tome u kojem obliku se izvodi – licem u lice, putem elektroničke pošte ili SMS-a, chata, bloga, oglasne ploče ili mrežne stranice nasilništvo uključuje sljedeće: nazivanje svakakvim pogrdnim imenima, širenje mržnje i neistinitih glasina, bilo kakav oblik prijetnje i slično. Zlostavljanje u virtualnom svijetu nije protuzakonito te se zakonski može kažnjavati. *Cyber* napadi nekad znaju biti i najgora opcija bilo kakvih internetskih napada obzirom da veoma negativno utječu na korisnika u emocionalnom smislu. *Cyber* napadi se još i nazivaju suvremenim oblikom nasilja u virtualnom svijetu, a meta može postati svatko te ne mora postojati određeni razlog zašto je ista žrtva nasilja. Većinom su ovakvi oblici nasilja najviše raširenji kod mlađih uzrasta gdje roditelji i skrbnici nemaju potpuno kontrolu nad djecom. Prema Li (2010) postoji osam metoda internetskog nasilja:

1. Grubo online sukobljavanje – kratkotrajna rasprava koja se većinom odvija između dvije ili više osoba te koju karakterizira grub ili agresivan govor.
2. Uznemiravanje – slanje okrutnih, uvredljivih i neprijateljski nastrojenih poruka k pojedincu ili prema grupi.
3. Ogovaranje i klevetanje – navođenje netočnih informacija o žrtvi te njihovo dalje dijeljenje s ostalim korisnicima. Cilj ove radnje je uništavanje reputacije i odnosa s drugima.
4. Lažno predstavljanje – korištenje tuđeg identiteta za slanje poruka i sadržaja u nečije ime s ciljem uništavanja ugleda i međuljudskih odnosa.

5. Iznuđivanje i širenje povjerljivih informacija – javno objavljivanje fotografija koje je žrtva poslala nasilniku.
6. Socijalno isključivanje – događa se istom mjerom putem interneta kao i u realnom svijetu te je žrtvama onemogućen ulaz u određene virtualne chatove ili su isključeni iz grupnih poruka.
7. Prijetnje i uhođenje – oblici nasilja koji se odnose na prijeteće poruke te pokušavanja uspostavljanja neželjenog kontakta.
8. Snimanje videozapisa za koji žrtva nije suglasna za snimanje. (Mamula i Mihaljević, 2019)

Nasilnici se koriste internetom jer takve stvari nisu u stanju napraviti ili izreći uživo, a na ovaj način su prikriveni i imaju veću slobodu. Nekada vrše internetsko nasilje kako bi namjerno povrijedili žrtvu, a nekada jer želi ispasti bolji i zabavniji u društvu. Mete mogu biti svakakve, a najčešće su to popularna i sretna djeca većinom jer su ostali ljubomorni na njihov uspjeh. Svađe na ovakvu temu mogu jako brzo eskalirati i izmaknuti svakoj kontroli. Mlađi uzrasti često koriste računala za dopisivanje s prijateljima, komuniciranje putem društvenih mreža i objavljivanje objava na istim servisima. No ponekad su u neposrednoj blizini nasilja, a da to nisu ni svjesni. Sam utjecaja jedni na druge da budu podli prema ostalim korisnicima već je jedan od tipova nasilja na internetu. Okrivljavanje korisnika nešto što nisu učinili isto može biti razlog nasilja preko interneta ili pak uvjeravanje korisnika da je netko ružan i glup. Nasilnici u virtualnom svijetu će sve poduzeti kako bi zahuktali problem pa će tako i poduzeti sve što mogu da nanesu što veću štetu svojoj odabranoj žrtvi. (Šostar i sur., 2006)

Primjerice, ako se zamjere određenoj osobi, *cyber* napadači spremni su ići toliko daleko sa nasiljem da se dovode u napast kreiranja mrežnih stranica koje šire svakakve netočne glasine i mržnju prema žrtvi. To izgleda da preuzmu žrtvine slike te ih preurede koristeći se raznim alatima za obradu fotografija. Ta ista slika nakon preuređivanja većinom bude oslovljena nekakvim pogrdnim nazivima te napadnim filterima koji unakaze žrtvin pravi izgled. Promjene na fotografiji koje nekoga posramljuju i zlonamjerne su, predstavljaju zlostavljanje. Takvi nasilnici često provaljuju lozinke pa koriste tuđe elektroničke adrese kako bi nekog uznemirili. Nagovaraju druge korisnike da nekoga izbrišu s liste prijatelja ili blokiraju s određene društvene mreže, sve kako bi stvorili negativan ugled te osobe. Također, šalju datoteke koje mogu zaraziti računalo virusima. Kao jedan od oblika zlostavljanja jest i

ismijavanje zbog izgleda ili načina koji se netko oblači, čak i kada izgleda kao šala, može povrijediti korisnika s druge strane ekrana. I žrtva se ponekad prikriva smijanjem na ovakav tip zlostavljanja, ali to ne znači da se ne osjeća povrijeđeno. Bitno je kada su ovakve situacije u toku pokušati sačuvati sve primljene sadržaje, poruke i druge relevantne dokaze. Vlasti će kasnije pomoću tih istih lakše pronaći zlostavljača. (Komljenović i Mihaljević, 2017)

Prema navedenim primjerima, nasilništvo u stvarnosti nije daleko od nasilništva na internetu jer oba oblika kasnije dolaze do ozbiljnih sukoba i posljedica. Ponekad zlostavljanje u virtualnom svijetu može snositi puno teže posljedice nego što to jesu u realnom svijetu. Teško je kad nasilništvo pristiže sa svih strana. Važno je u takvim trenucima ostati pribran i ne se dalje suprotstavljati jer nekad internetski nasilnici samo to i čekaju kako bi dalje nastavili s uznemiravanjem. Najteže je mlađim osobama biti žrtva grupe jer se tako svi korisnici okome na žrtvu. Za sve postoji rješenje, a komunikacija je gotovo uvijek najispravniji mogući način. (MacEachern, 2012) Pokazuje se da je ignoriranje očito najučinkovitiji način da zlostavljanje prestane pa tako na kraju i mnogi postupe. Na raspolaganju za rješavanje takvih problema postoje raznorazne stranice koje šalju elektroničku poštu pošiljatelju umjesto vas pa tako uznemiravanje isto brzo prestane. Isto tako postoje različiti mrežni servisi kojima se može poslati elektroničku adresu koja vrši uznemiravanje u virtualnom svijetu te će se taj isti servis pobrinuti da taj račun postane neaktivan ili ga potpuno deaktivirati. (Aftab, 2003)

Postoje različite teorije zašto uopće dolazi do nasilja u virtualnom svijetu, a jedna od najpoznatijih je teorija o socijalnom učenju koja govori da promatranje sadržaja koji su nasilni može osobu potaknuti na imitaciju. Prilikom imitiranja, osoba će izgubiti zauzete stavove i norme ponašanja na internetu. Ciboci i suradnici (2011) naglašavaju kako je znanstvenik Albert Bandura uspio pokazati da promatranjem tuđeg agresivnog ponašanja dolazi do agresivnog ponašanja promatrača. Također spominju i kako su stotine znanstvenih studija pokazale da izloženom medijskom nasilju povećava agresiju. Učinci se dijele na kratkoročne i dugoročne gdje kratkoročni budu oni koji se pojavljuju odmah nakon kontakta s medijskim sadržajima, a oni dugoročni nakon nekoliko tjedana ili čak mjeseci. O učincima također ovise trenutne okolnosti i težine slučaja kao i pojedini slučaj. Obzirom da su većini nasilja u virtualnom svijetu izložena djeca, važno je naglasiti kako nasilni sadržaji imaju znatno veći utjecaj

na mlađu djecu koja ne mogu razborito pratiti razvoj radnje prilikom korištenja internetom zbog kognitivnih sposobnosti koje su još uvijek u samom razvoju. Njihovu pozornost konkretno privlače scene u kojima se događa nešto zanimljivo, dinamično i zabavno, a često je to i sam oblik nasilja. Mnogi ističu poveznicu na nasilje ako gledanje filmova, serija i programa na televiziji kao izvor nasilja. Pa tako osjećaji ljutnje, agresije i frustracije daju veću mogućnost od samog imitiranja ovakvih ponašanja. Još jedan način kojim možemo biti dio nasilja jest upravo preko videoigra. Neposrednim igranjem ili gledanjem video igara dokazano je kako izazivaju agresivnost i štetne učinke na funkcije mozga i pamćenje. Istraživanja su pokazala kako gotovo sve videoigre imaju nasilne sadržaje, dok je samo mali dio njih vezan za edukativan sadržaj. (Ciboci i sur., 2011)

Ono što u ovom slučaju zabrinjava stručnjake osobito kod komunikacije pomoću moderne tehnologije jest javno objavljivanje privatnih podataka poput: imena, prezimena, adrese, škole koju pohađaju i sama mjesta na koja izlaze. Takve stavke kod prevaranata često mogu otkriti točnu lokaciju žrtve pa i tu dolazi do velikog problema. Žrtve objavljivanje takvih osobnih podataka stavlja u rizik kojeg često nisu niti svjesni. Osim toga, nesvjesno dijeljenje takvih informacija na društvenim mrežama i drugim javnim platformama može pružiti prevarantima i zlonamjernim osobama dodatne prilike za manipulaciju i iskorištavanje žrtava. (Bilić i sur., 2012) Prevaranti se takvim informacijama koriste kako bi stvorili lažne profile, čime povećavaju svoju vjerodostojnost u očima potencijalne žrtve i tim putem olakšavaju manipulaciju. Još jedan problem leži u činjenici da jednom objavljene informacije na internetu često ostaju trajno dostupne, čak i ako ih korisnik kasnije odluči izbrisati. Time se dodatno povećava rizik od njihove zloupotrebe u budućnosti. Primjerice, informacije poput adrese ili mjesta kretanja mogu olakšati fizički pristup žrtvi, čime se narušava njezina osobna sigurnost i privatnost.

3.4.1 Socijalni inženjering

U virtualnom svijetu kad je riječ o socijalnom inženjeringu misli se na manipulaciju pojedinim žrtvama kako bi izvršile određene radnje u svrhu otkrivanja informacija. Kao takav socijalni inženjering navodno ne zahtjeva veliko znanje u smislu tehnologije već se napadač koristi uobičajenim principima sociologije i psihologije poput znatiželje, lakovjernosti, nepromišljenosti, straha i ostalih sličnih primjera.

Napadači saznaju na slabosti koje ljudi imaju te ih iskoriste protiv njih samih. Te slabosti koriste kako bi dobili lozinku, brojeve bankovnih kartica i osobnih podataka. Većinom se oslanjaju na sposobnost manipulacije i uvjeravanja. Napadači se koriste dvaju mogućim tipovima za napad, a uključuju fizički i psihološki. Fizički sadrži nekakve pristupe žrtve gdje napadač želi prikupiti podatke o žrtvi – radno mjesto; napadač će ušetati na područje žrtvinog radnog mjesta te se praviti da je netko drugi kako bi prikupio što više informacija. Ili će jednostavno nazvati određenu tvrtku i metodom uvjeravanja postići željeno. Socijalni inženjering vrsta je *cyber* napada, a najčešći oblik ovakvih obmana su upravo krađa podataka koji se nalaze na bankovnim karticama. (Kelam, 2018)

Prijevare koje se događaju isključivo kako bi se žrtva financijski oštetila većinom su dobro isplanirane sa strane napadača. Postoji nekoliko vrsta financijskih prijevara, a jedna od je upravo ona gdje se prevaranti pretvaraju da su klijenti, dobavljači ili partneri žrtava, šaljući lažne račune te tjerajući žrtvu da uplati novac na bankovni račun koji pritom kontroliraju. Napadači koriste skoro pa identične adrese poznatih klijenata žrtvi pa je tako teško shvatiti da se radi o prijevari – primjerice, mijenjaju jedno slovo u domeni elektroničke pošte kako bi izgledali legitimno. U nekim slučajevima čak i presreću stvarnu komunikaciju između žrtve i njihovih poslovnih partnera te onda mijenjaju podatke na fakturama. Kada se radi o ovakvoj vrsti prijevare, prepoznat ćemo je po tome jesu li postupci koji klijenti traže od žrtve žurni ili ne. Ako se od žrtve zahtijeva brz postupak uplate onda se većinom radi o prijevari. Slična ovoj vrsti prijevare jest ona gdje prevaranti kod online kupovine kreiraju lažne internetske trgovine, oglase ili ponude koje na prvi pogled izgledaju autentično i zaista uvjerljivo. Domena mrežne stranice izgleda legitimno, a oglašavanje je napravljeno u svrhu kako bi privukli kupce. Takve ćemo lažne online trgovine prepoznati kao one koje imaju velike popuste na marke ili popularne proizvode. Ako naletimo na mrežnu stranicu koja se ne čini pouzdana lako možemo provjeriti je li zapravo original provjerom na uvjete poslovanja ili pronalaskom sigurnosnog certifikata. Takve stranice ne pružaju povrat novca i plaćanje je obavezno unaprijed, prije samog primitka paketa što ukazuje na prijevaru.

Danas na svakom kutku možemo naići na prijevare putem nagradnih igara. Takva prijevara djeluje primamljivo i zaista istinito, no jedna je od najopasnijih. Sve se odvija tako da osoba dobije elektroničku poštu u kojoj ju obavještavaju o velikom

novčanom dobitku na nekoj od nagradnih igara ili na primjer iznenadnom osvajanju luksuznog putovanja. Iako se korisnik nikad nije prijavio za takvu vrstu igre, napadači imaju pomno osmišljen plan kojim nagovaraju žrtvu da sve izgleda vjerodostojno i potpuno sigurno. No, sve se zakomplicira kada osoba mora ispuniti određene zahtjeve prilikom preuzimanja svoje nagrade. Neki od tih zahtjeva uključuju: plaćanje administrativnih troškova, poreza ili naknade za transfer novca, a zapravo sve se odvija preko napadača gdje oni žele izvući što više novaca od žrtve. Ovakav tip prijevare uključuje dostavljanje osobnih podataka, a neki od njih su broj bankovnog računa, adresu stanovanja te identifikacijske dokumente. Nakon što žrtva obavi sve potrebno za uplatu novčanog iznosa koji je „osvojila“, prevaranti nestaju, ostavljajući žrtvu bez novca i nagrade. Osobni podaci žrtve upotrebljavaju se u svrhu krađe identiteta ili pristup njezinim financijskim računima. (Stanković, 2024.) Sprječavanje ovakvih načina prijevare je dobra provjera koliko je zapravo istinit. To korisnik može napraviti kontaktiranjem odgovornih osoba za nagradnu igru. (Goljački, 2022)

3.4.2. Phishing

Porijeklo pojma „phishing“ dolazi od engleske riječi „fishing“ koja metaforički opisuje postupak neovlaštenih korisnika koji privlače korisnike interneta kako bi im otkrili svoje osobne podatke. (Goljački, 2022) Napadač u ovom slučaju radi sve kako bi potpuno pridobio korisnikovo povjerenje pa tako i lažira određena mrežna sjedišta poput bankovnih mrežnih stranica. Ovakve stranice mogu se prepoznati upravo preko URL putanje odnosno domene cjelokupne mrežne stranice. Ponekad je dovoljno da korisnik samo slijedi poveznicu koju mu napadač pošalje kako bi isti prikupio neke informacije o osobnim podacima koje se nalaze primjerice na računalu s kojeg žrtva slijedi tu poveznicu. Postoje različite mogućnosti koje nalazimo u imenima domene, te već u samom nazivu domene možemo otkriti radi li se o prijevari. Većinom i same banke na taj način ne komuniciraju sa svojim klijentima već ih kontaktiraju telefonskim putem ili pošalju poštanskim putem ono što trebaju pa se prijevara u ovom slučaju lako prepoznaje.

U zadnje vrijeme česta je pojava ovakve *cyber* prijevare preko poruka koje stignu na mobitel žrtve u obliku tekstualne poruke glaseći „Ime banke: Plaćanje je uspješno izvršeno s Vaše kartice. Link na poveznicu“ ili „Ime banke: Imate novu transakciju, koristite dostavljenu poveznicu za povrat: link na poveznicu“. Većina

korisnika koja je tada zbunjena klikne na poveznicu jer misle da će tamo dobiti nekakve informacije, a otvara se skočni prozor koji izgleda identično kao i kod žrtvine vlastite banke. Upravo phishing prijevare funkcioniraju na temelju socijalnog inženjeringa – strategije koja iskorištava ljudsku psihologiju kako bi prevarant naveo žrtvu da povjeruje u autentičnost dobivene tekstualne poruke. Prevaranti smišljaju svakakve moguće vrste tekstualnih poruka kako bi bili uvjerljivi i naveli žrtvu da klikne na poveznicu.

Prema Agenciji za zaštitu osobnih podataka (2025), napadači se u današnje vrijeme sve češće predstavljaju i kao tijela javne vlasti poput elektroničkih poruka koje se odnose na Poreznu upravu gdje žrtve dobije obavijest kako im je odobren povrat poreza, a kako bi im isti bio isplaćen moraju kliknuti na poveznicu ili skenirati QR kod. Također, preko Porezne uprave od žrtve se može tražiti da uplati dug koji je namijenjen porezu, a još nije podmiren. Elektroničke poruke od primjerice od Hrvatskog zavoda za zdravstveno osiguranje, Ministarstva i slično u kojima obavještavaju žrtve da imaju pravo na isplatu pomoći ili povrat troškova određenog iznosa isto tako slijedeći poveznicu ili skenirajući QR kod. Korisnicima može biti poslana i poruka sa strane Policijske uprave u kojoj ih navedena obavještava da su optuženi za nekakvo kazneno djelo koje na primjer nisu počinili. Žrtve koje prije nisu upozorene za ovakav slučaj prijevare mogu naivno slijediti poveznicu koja će tražiti od njih osobne podatke, a koje nadležna tijela nemaju pravo zahtijevati od pojedinaca na ovakav način. Automatski se može procijeniti da se radi o prijevari. Jedna od aktualnih prijevara jest isto lažna e-poruka, ali odnosi se na poštanske i dostavne usluge. Žrtve mogu primiti elektroničku poruku u kojoj ih pošiljatelj obavještava kako paket čeka na isporuku, a kako bi isti mogao biti isporučen, potrebno je plaćanje naknade za dostavu od svega nekoliko centi putem naravno, poveznice. Samim klikom na poveznicu, otvoriti će se lažna stranica osmišljena za upravo ovakve prijevare. Tako žrtve svakodnevno dobivaju ovakav tip poruka, a slabo educirani mogu biti dio iste prijevare.

Kako bi se izbjegao ovakav tip poruka bitno je dobro provjeriti pošiljatelja i službenu e-mail adresu. Ukoliko se od žrtve traži da upiše podatke s bankovnih kartica ili osobne podatke, preporuča se zatvaranje takve stranice i brisanje e-poruke. Također, u današnje vrijeme poznato je da postoje razne vrste prijevara te je preporučljivo strogo čuvanja svojih osobnih podataka i ne dijeljenje istih, pogotovo u virtualnom svijetu!

Posebna vrsta kojom se žrtve danas suočavaju uključuje vrstu investicijskih prijevara odnosno kriptovalute. Obzirom da transakcije kojima trguju korisnici kriptovaluta ne uključuju tradicionalni bankovni sustav koji omogućuje povrat sredstava tada postaju velika meta za prevarante. Prva kriptovaluta stvorena je 2008. godine pod nazivom „Bitcoin“, a danas postoji nekoliko tisuća različitih valuta. Phishing napadi usmjereni su na korisnike aplikacija za kriptovalute te su osmišljeni na način da napadači dopru do vjerodajnica za prijavu, lozinka ili drugih osjetljivih informacija koje omogućuju pristup sredstvima. Prevaranti često kreiraju lažne mrežne stranice koje izgledaju gotovo identično onim originalnim. Primjerice, phishing e-poruka može sadržavati obavijest o navodnom sigurnosnom problemu na korisničkom računu gdje se od korisnika traži da se prijavi putem lažne poveznice. Osmišljeni su i lažni kripto-novčanici preko kojih prodavači uspiju pokrasti male količine novca, zatim lažne mjenjačnice koje ne prikazuju istinite informacije o kriptovalutnom tržištu. Lažne kampanje koje se bave donacijama ciljaju na humanitarne ljude, a zatim uzmu sva sakupljena sredstva i nestanu sa istima. (Goljački, 2022)

Kako bi navedene žrtve znale postupati s određenim obavijestima koje svakodnevno pristižu putem e-poruka, mail poruka ili sličnih trebaju biti sumnjičavi ukoliko netko stvara hitnost ili traži pristup informacijama koje uključuju osobne podatke. (Kelam, 2018)

4. Djeca u virtualnom okruženju

Kada se spomenu djeca i pojam virtualnog okruženja, svakakve mogućnosti pristižu kao misao. Sve takve misli većinom se sve svode na varijaciju istih. Djecu u relaciji s virtualnim svijetom dijelimo na dva moguća ishoda koji se smatraju pozitivnim ili negativnim. Svakim danom sve teže je biti u korak s digitalnim dobom, a pogotovo sa svime onime što ono nosi. Neizbježno je nadodati da tehnologija djeci i mladima postaje važna za svakodnevno funkcioniranje.

Računalo im postaje najbolji prijatelj u kojega imaju povjerenja već od mlađe dobi pa nekima čak i u dobi od četvrtog mjeseca života. Iako se govori kako djeci nije preporučljivo davati ekrane u ruke prije no što kognitivno sazriju. Time, govore stručnjaci, unazađujemo njihov rast, koliko fizički toliko i psihički. Danas djeca u jako ranoj dobi dolaze u doticaj s računalima, mobilnim telefonima i ostalom tehnologijom. Do problema dolazi jer upravo tako rana dob onemogućuje djeci da se educiraju o mogućim rizicima koristeći se virtualnim svijetom. Igrice i crtići zamjenjuju računalom na kojemu ako nemaju dogovoreno vrijeme s roditeljima ili skrbnicima, provode znatno više vremena nego što bi trebali. Nedavno je i takva generacija djece dobila naziv net-generacija uzimajući u obzir kako je ta generacija djece rođena u doba gdje odrastaju djeca koja su izravno povezana s internetom i ne poznaju svijet bez računala. Obzirom da je kreiran i vlastiti naziv za takvu djecu rođenu u pripadajućoj generaciji onda postoji i podjela takve generacije. Naime, proučavanjem djece rođene u razdoblju koje ulazi u net-generaciju, stručnjaci razbiru pozitivne od negativnih osobina. Kao pozitivne ističu brzinu koja se razvija prilikom stjecanja digitalnih vještina i primjenjivanja istih. Brzo se prilagođavaju modernom svijetu i utjecaju tehnologije što doprinosi njihovim tehnološkim vještinama. Takva djeca većinom su optimističnija i više samopouzdanija no inače. Velika pozitivna karakteristika je otvorenost kojom barataju, no neka djeca znaju biti ranjivi odnoseći se na takve stvari. Svojom otvorenošću otvaraju mnoga vrata no isto tako dolazi do velikog rizika prekomjernog dijeljenja osobnih informacija prilikom zaviranja u virtualni svijet. Djeca odrasla u net-generaciji lakše se uklapaju u virtualnost pa im tako komunikacija ne predstavlja problem. Pragmatičnost je jedna od ključnih karakteristika takve generacije budući da su odrasli u okruženju punom informacija te su skloni praktičnom pristupu problemima. Dok je ambicioznost sastavni dio njihovih vidika i budućnosti. Djeca net-generacije sklona su prilagođavanju i konstantnoj suradnji kako bi se povezali jedni s drugima. Bitno je naglasiti kako

virtualno okruženje daje veoma pozitivan utjecaj na djecu što se tiče kreativnosti i izražavanja ideja te mišljenja. Djeca su spremna na prihvaćanje novih izazova, znanja i tehnologija koje buduće vrijeme donosi.

Nažalost, uz pozitivne osobine gotovo uvijek se vežu i one negativne. Pa tako uz sve dobre karakteristike koje djeca snose koračajući kroz virtualni svijet, one negativne ipak ponekad više prevladaju. Obzirom na stalnu izloženost i povezanost s virtualnošću, djeca nisu ni svjesna koliko to utječe na njihovo cjelokupno zdravlje. Najviše to utječe na vid, kasniji problemi koji se javljaju u vezi bolova kralježnice i slično. Obzirom na puno vremena provedenog za računalom, djeca su ometena u obavljanju svakodnevnih zadataka koji su ključni za razvoj određenih navika. Činjenica jest da su djeca net-generacije previše obasuta informacijama čiji protok jednostavno ne mogu kontrolirati. Zasićenost informacijama dovodi do manjka pozornosti što je zaista zabrinjavajuće u tako ranoj dobi djeteta. Informacije su danas brze i dostupne u svakom trenutku, ponekad i toliko brze da djeca ne stignu razabrati dobro od lošega ili primjereno od neprimjerenoga. Brzi protok informacija ne dozvoljava djeci da racionalno razmišljaju prilikom donošenja određenih odluka već im upravo takav način širenja informacija onemogućava donošenje ispravnih odluka u vlastitu korist. Primjerice, ne razbiru štetnu informaciju pa ju tako nekad nesvjesno prošire ili ne posavjetuju se s odraslima prilikom dopisivanja s nepoznatom osobom koja ima loše namjere. Djeca net-generacije skloniji su stvaranju lažnih identiteta nego što su to primjerice starije generacije. Danas stvoriti lažni identitet dostupno je u svega par klikova te se radi na način da se kreira korisnički profil koristeći pritom lažne slike, informacije i ostalo. Na internetu je lako kreirati različite verzije sebe te to rade upravo osobe koje nisu dobro povezane sa realnim svijetom, pate od manjka socijalizacije ili se osjećaju izolirano. Takve osobe lakše će kreirati lažni identitet putem na primjer društvene mreže nego se sprijateljiti s jednim od svojih vršnjaka. Lažni identitet će tada osobi pružiti nekakvu razinu komfora i bijeg od stvarnosti gdje mogu biti tkogod požele bez osuđivanja ili ograničenja. Djeca internet generacije često sami sebe idealiziraju te su fokusirani na materijalnu vrijednost stvari i osobni uspjeh. Upravo te značajke smatraju ključnim temeljima za sreću i uspješan status.

Djeca općenito virtualni svijet vide kao pomoć da otkriju nove stvari, interese, informacije, prijatelje i mnoge druge stvari. Manjina djece pronalazi virtualni svijet i kao idealno mjesto za učenje i prikupljanje zanimljivih i korisnih informacija. Rješavaju

probleme i doziraju svoju upotrebu računala. Dok s druge strane, velik dio djece ne prepoznaje koliko virtualni svijet nekada može biti rizičan i predstavljati opasnost. (Bilić, 2020)

4.1. Djeca i internet

Sveprisutnost medija počinju od praktički prvog dana djetetova života. Od televizije do radija pa kasnije i susret s računalima, tabletima i mobitelima. Net-generacija koristi se tehnološkim uređajima kao da im je baratanje istima urođeno, a neophodno je spomenuti kako to utječe na njihov cjelokupni razvoj. Djeca virtualni svijet koriste selektivno pa tako odabiru sadržaj prema interesu, potrebama ili željama. Zbog širokog spektra kojim se svakodnevno susreću, odabiru ono što im najviše pobuđuje interes, bilo da je riječ o igrama, video sadržajima, društvenim mrežama ili edukativnim stranicama. Dokazano je kako se djeca nižeg školskog uspjeha koriste računalima više nego ona koja ima veći prosjek. Djeca se većinom koriste internetom zbog zabave te im virtualni svijet na taj način privlači puno pažnje. (Ilišin i sur., 2001)

Prilikom korištenja računalom i komunikacija istim, javlja se neravnoteža između komunikacije u virtualnom svijetu i osobne komunikacije. Tim načinom djeca često ne mogu doživjeti emocije koje dolaze primjerice; govorom tijela, tonom glasa i ostalim neverbalnim signalima koji su važni za uspostavljanje interakcije. (Ciboci i sur. 2011)

Kada je riječ o predstavljanju na internetu, utvrđeno je kako se djevojčice drukčije ponašaju nego dječaci. Djevojkama služi internet kao mjesto za upoznavanje, jačanje sadašnjih prijateljstava i uspostavljanje novih prijateljstava dok dječaci gledaju povezivanje prema zajedničkim interesima. Djevojke biraju estetski lijepe fotografije koje objavljuju kako bi izgledale privlačno i zavodljivo, a mladići se u sadržajima koje objavljuju često oslanjanju na teme poput sporta, tehnologije i humora. Velike su tu razlike te isto tako različiti načini privlačenja pažnje koji su usmjereni više ka djevojčicama od strane nepoznatih korisnika i/ili onih koji nemaju dobre namjere. Djevojčicama je bitnija online ličnost zbog toga jer u virtualnom svijetu općenito mogu više privlačiti pozornost nego što to mogu u realnom svijetu. Često se koriste programima za uređivanje fotografija kako bi izgledale bolje i na taj način povećale popularnost. Uglavnom se korisnički profil koji posjeduje djevojčica prikazuje kao profil koji sadrži objave vezane za lijepu okolinu, važne trenutke i obuhvaća samorefleksiju

odnosno fotografije koje opisuju njihov način života i ono što one pronalaze važnim. S druge strane, profil jednog mladića prikazuje dominaciju. Dječaci vole pojam moći i primijećenosti pa se tako i predstavljaju. Vole isticati informacije koje ne moraju biti nužno točne, ali ih svejedno spomenu kako bi ih to učinilo popularnijima pred virtualnom publikom. (Bilić, 2020)

Kada vežemo pojam interneta s djecom često se spominju negativni utjecaji, no internet je mjesto jako korisnih informacija koje mogu poslužiti djeci. U korist djece edukativni portali mogu znatno olakšati djeci prilikom učenja ili istraživanja novih informacija. (Žderić, 2009)

4.2. Roditeljski nadzor kao pomoć u zaštiti podataka

No od svega navedenog, zabrinjavajući su ipak postotci maloljetne djece koja se koriste virtualnim svijetom bez nadzora roditelja ili skrbnika. Većina roditelja djecu prepuštaju virtualnosti bez obzira jesu li educirana o mogućim rizicima i posljedicama. Naime, veoma je bitno pratiti kojim se vrstama internet stranicama ili aplikacijama odnosno platformama djeca koriste te ih usmjeravati prema onim edukativnim i poučnim. Potrebno je osvijestiti se koliko je dovoljno provoditi vrijeme pred ekranom pa i na taj način upravljati time kao roditelj. Prema Radolović i Renić (2024) ključ je u uspostavljanju pravila koja se moraju poštovati kako bi se uravnotežilo korištenje virtualnim svijetom. Dijete mora biti svjesno koliko dijeli svoje osobne podatke kako bi što više uspjelo zaštititi svoju privatnost. Važna je svjesnost kreiranja jakih zaporki i postupanja s istima te snalaženje u različitim vrstama *cyber* napada u slučaju da se isti dogodi. Maloljetna djeca koja učestalo imaju kontakt s virtualnim svijetom moraju biti oprezna obzirom na moguće rizike od anonimnih i nepoznatih korisnika. Također, svjesna o trajnosti objavljenog sadržaja te posljedice koje mogu imati te iste objave u stvarnom životu. Dijete koje posjeduje određene vještine kao na primjer ove navedene, smatra se djetetom koje je educirano i spremno za virtualni svijet i sve što ono nosi.

Kako bi roditelji imali pod kontrolom posjećene stranice svoje djece, postoje razni alati kojima se mogu poslužiti. Primjerice, alati poput Google Family Link ili Norton Family koji omogućuju nadzor aplikacija. Takvi alati omogućuju roditeljima praćenje, filtriranje i kontroliranje sadržaja. Djeca su često na internetu te je tako njihova sloboda upitna, a kako više ne bi bila važno je odabrati alate koji pokrivaju sve za vlastite

potrebe. Naravno, postoje i one vrste alata koje zahtijevaju dodatan trošak, ali nisu nužne kako bi roditelji očuvali sigurnost djeteta. Postavljanje granica je bitno od samog početka poput blokiranja određenih chat soba ili primjerice onemogućavanje gledanje sadržaja specifičnih aplikacija. Roditelji moraju biti svjesni kako uvijek postoji način za izbjeći takva pravila i dogovore nekakvim alternativnim rješenjima stoga je bitno razgovarati s djecom o aktivnostima koje provode na internetu. Jedna od najvažnijih stvari prilikom osiguravanja sigurnosti je blokiranje neprimjerenih sadržaja. Većinom internetske stranice na kojima nalazimo neprimjereni sadržaj mogu voditi ka sumnjivim stranicama koje znatno mogu narušiti djetetovu sigurnost. Praćenjem online interakcija, softver za roditeljski nadzor može biti ključan u sprječavanju nasilja preko interneta, a roditelji imaju priliku brzo reagirati ako dođe do navedenog. Aplikacije koje su ujedno i alati za roditeljski nadzor djece omogućuju i postavljanje vremenskih ograničenja.

Takve vrste nadzora dijele se na aktivan i pasivan nadzor. Aktivan nadzor podrazumijeva onaj koji se odnosi na svakodnevno promatranje i praćenje dječjih aktivnosti od strane roditelja. Na taj način roditelji pravovremeno prepoznaju moguće probleme i opasnosti te mogu pružati djetetu potrebnu zaštitu. Dok se pasivan nadzor odnosi na onaj neizravan bez stalnog roditeljskog praćenja. Takav nadzor djetetu omogućuje veću slobodu uz prethodno postavljene smjernice i pravila. Roditelji prate djetetove aktivnosti, ali mu omogućuju razinu privatnosti i samostalnosti. Primjerice, roditelji kada prakticiraju pasivan nadzor budu u istoj prostoriji s djetetom dok ono koristi internet. Kada roditelji uspostave određenu vrstu nadzora onda mogu zadržati sigurnost djeteta na visokoj razini. (Centar za sigurniji internet, 2023)

Zbrajanjem svih navedenih pozitivnih stvari koje donose alati za roditeljski nadzor tako izdvajamo i one negativne. Stalnim praćenjem djetetovih aktivnosti postoji velika mogućnost od narušavanja njegove privatnosti što može dovesti do nepovjerenja i ograničiti djetetovu samostalnost. Tako da korištenjem tih alata isto tako treba oprezno postupati kako roditelji ne bi pretjerali. Online platforme i aplikacije u konačnici imaju veliku odgovornost i sam utjecaj na online sigurnost svih, a ne samo maloljetne djece. Tim putem Centar za sigurniji internet (2024) ističe kako je važno komunicirati o sigurnosti na internetu i odgovornom ponašanju.

Prema nedavnom istraživanju Kamar i suradnika (2022) ističe se kako je nadzor roditelja ključan u održavanju virtualne sigurnosti djece i mladih. Istraživalo se koliko utjecaj roditelja ima smisla i kakve posljedice donosi. Rezultatima se utvrdilo kako je utjecaj i veći no što je bila glavna pretpostavka.

4.3. Opasnosti interneta

Internet je itekako u današnje vrijeme rizično koristiti. Teško je objasniti mlađim uzrastima koji su još uvijek naivni te žele ili moraju sve vidjeti i isprobati. Prvenstveno je bitno da znamo kako sam internet nije kriv za silna događanja, zločine, krađe i slične stvari nego su krivi upravo oni korisnici koji ga koriste na bezobziran način, kršeći zakone i namjerno nanose štetu drugima. Rizici prepuštanja interneta djeci su razni, a najčešće opasnosti su one koje narušavaju djetetovu sigurnost i privatnost.

Dijete može poslužiti kao posrednik dijeljenja osobnih podataka nesvjesnim radnjama. Tako će na primjer dijete zbog zanimanja za neki proizvod ili oglas odmah nasjesti. Opreznosti nikad dovoljno što se tiče osobnih podataka ili važnih dokumenata kao što su kreditne kartice ili pak lozinke koje djeca mogu odati na internetu i nesvjesno napraviti veliku pogrešku. Postoje internetski imenici koji sadrže sve prikupljene podatke o osobama pa tako i o samoj djeci. Stvar je u tome da dijete ne treba napisati direktno svoje podatke i informacije jer će internet u trenutku sve uneseno povezati te doći do djetetovog mobilnog uređaja pa ga je u mogućnosti i čak locirati. Takvi se podaci nalaze u mnogobrojnim internetskim katalozima takozvanim mrežnim sjedištima gdje je dovoljno upisati broj telefona i sve ostale informacije će se ispisati same od sebe.

Među svim rizicima kojima bi dijete moglo biti izloženo „surfajući“ internetom dolazimo do prevara. Primjerice, popunjavanjem obrasca dijete bi moglo dospjeti u ruke marketinških stručnjaka kojima je cilj skupiti osobne podatke i tako nedopuštenim tehnikama upravljati njima. Djeca mogu postati žrtve prijevara i tako može doći do ostalih sličnih stvari koje krše zakon i nedopustive su.

Nažalost, ne možemo znati da su mrežne stranice uistinu onakve kakve jesu. Mrežne stranice koje posjećujemo se možda čine pouzdanima i sigurnima, ali to nije uvijek slučaj. Podaci mogu biti prikupljeni da ih mi upišemo ili automatski uz pomoć

kolačića (eng. Cookies) i slične tehnologije. Kolačići su tekstualne datoteke koje sadrže informacije te pomoću njih operator može uvidjeti koje ste mrežne stranice prije posjetili te tako sakupiti vaše osobne podatke. Stoga je važno da budemo oprezni u svojim odlukama pogotovo na internetu, društvenim mrežama i mrežnim stranicama. (Aftab, 2003)

Internet itekako može biti opasan za djecu što se tiče ovisnosti. Ovisnost najčešće prevladava kada je riječ o igranju video igrica i posjetu raznim društvenim mrežama. Ovisnost svrstavamo u skupinu ponašajnih ili bihevioralnih ovisnosti. To znači da djeca koja su stekla ovisnost nad internetom postaju vezana za korištenje istog. Postoje i simptomi, a mnogi se svode na neprekidno otvaranje elektroničke pošte, neprekidnom željom za spajanje na internet, pregledavanju objava na društvenim mrežama i slično. Djeca koja su korisnici interneta nepoznatim ljudima povjeravaju osobne stvari koje ne bi trebali. Štoviše, društvene mreže postale su temelj za elektroničko nasilje osnovnoškolskoj i srednjoškolskoj djeci gdje koriste svoje korisničke profile kao izvor za maltretiranje, uznemiravanje i ponižavanje drugih žrtvi.

Virtualni svijet također ponekad sadrži jako opasne informacije koje se smatraju neprikladnima za djecu no moguće je da djeca lako naiđu na njih. Ako ne razmišljaju razumno i odluče iskoristiti te iste informacije, postoji velika vjerojatnost da će posljedice biti negativne. Primjerice, mnogo djece internet iskorištava kako bi preko takozvanog „dark weba“ naručili ilegalne stvari. Dark web ima općenito lošu namjenu te se većinom koristi u svrhu kupnje i prodaje. Centar je za mnoga crna tržišta koja mogu sadržavati prodaju ukradenih podataka, lažnih dokumenata, ilegalnih supstanci pa čak i oružja. Sadrži usluge poput hakerstva, prijevara te svakakve moguće ilegalne aktivnosti. (Ružić, 2011)

Uz pristup „dark webu“ djeca imaju i pristup pornografiji te mnogim drugim neprimjerenim informacijama. Mlađim dobnim skupinama prijete i opasnosti poput prikupljanja podataka sa marketinškim strategijama. Djeca ne razbiru što je stvarno, a što je prijevara pa tako nasjedaju na različite rizike koje naposljetku zaraze računalo i sa virusima. (Aftab, 2003)

4.3.1. Rizične aktivnosti djece na internetu

U današnje digitalno doba internet je mjesto brojnih mogućnosti, a učenje, zabava i komunikacije spadaju u iste. Međutim, uz sve prednosti koje donosi, djeca su itekako svakodnevno izložena raznim rizicima i rizičnim aktivnostima. U neke od tih spada i neoprezno dijeljenje informacija pa tako dolazi do loše zaštite podataka što može uzrokovati posljedice poput povrede dječjih prava, privatnosti ili pak onog najvažnijeg – sigurnosti.

Današnjica je poznata po društvenim mrežama te silno dijeljenje javnog života koje je postalo trend u maloljetnoj dobi. Djeca sve češće dijele svoje svakodnevni životni stil putem fotografija, objava pritom ne pazeći da zaštite svoje osobne podatke primjerice – lokaciju. Lokacija je alat koji je pogodan za mnogo stvari, no nekada ga dijelimo previše nepromišljeno i olako. Svi ju na svom pametnom telefonu koriste u različite svrhe, a njeno korištenje može poslužiti za očitavanje vremenske prognoze, GPS-a odnosno karti, može koristiti za lakše pronalaženje mobitela u slučaju gubitka ili krađe. Lokacija kao takva ima mnogo namjena te većina korisnika poput djece dozvoljava stalno praćenje. Poznato je kako gotovo sve aplikacije traže dozvolu od pristupa lokaciji kako bi se mogli koristiti istima. Takva se radnja naziva geo lociranje, a spada u praćenje putem društvenih mreža ili aplikacija kada ih korisnik aktivno koristi. Objavljivanje lokacija ulazi pod rizične radnje na internetu jer ugrožava sigurnost djece u tom trenutku kada je objava objavljena na društvenoj mreži. Primjerice, mnoga djeca vole koristiti lokaciju kako bi s vršnjacima podijelili svoje zanimljive aktivnosti, putovanja ili trenutne kretnje no to maksimalno može ugroziti njihovu sigurnost. Djeca nesvjesnim dijeljenjem svoje lokacije stvaraju određene rizike među koje spada:

- pružanje pristupa osobnim podacima nepoznatim osobama
- omogućavanje da nepoznate osobe prate njihovo kretanje
- otkrivanje detalja iz svog privatnog života.

Činjenica da bilo tko može znati gdje se određeno dijete nalazi u bilo kojem trenutku samo zato jer ima upaljenu lokaciju i dijeli je s ostalima veoma je opasno. Preporuča se da lokacijska usluga bude uključena samo onda kada je prijeko potrebna za potrebe funkcioniranja aplikacija na kojima je to nužno. U suprotnom, svakog trenutka djeca riskiraju na svoju sigurnost i sigurnost njihovih bližnjih. (Centar za sigurniji internet, 2023)

Dosad najriskantniji oblik ponašanja koji može utjecati negativnim posljedicama na djecu pripisuje se zlostavljanju. Zlostavljanje može nanijeti štetu žrtvi u obliku povrede osobnih podataka. Naime, puno internetskih napadača koriste se upravo osobnim podacima koje saznaju tokom komunikacije sa žrtvom. Tim se podacima koriste na taj način da ih upotrijebe protiv žrtve kako ih ne bi odala ili prijavila nadležnim institucijama. Napadači se ne čine kao opasni ili zlonamjerni pri samom početku, ali djeca nekada ne uspiju prepoznati njihove skrivene namjere. Često se prevaranti isprve predstavljaju kao prijateljski nastrojene osobe, koristeći se laskavim vokabularom kako bi uspješno namamili žrtvu. Postupno, kroz duže razdoblje komunikacije, nonšalantno počinju tražiti osobne informacije od žrtve primjerice fotografije ili videozapise koji kasnije mogu poslužiti za ucjenu ili zlouporabu. Dijete u tom trenutku ne shvaća opasnost i bezobzirno dijeli te podatke s napadačem. Napadači se često prepoznaju kao anonimni što im znatno olakšava u slučaju da se pokrene kazneni postupak protiv istih. U trenutku kada napadač prikupi dovoljno materijala počinje manipulacija. Tada dijete pod prisilom ili zbog straha može nastaviti komunikaciju.

Djeca ponekad i nesvjesno uključe roditelje ili korisnika čiji je korisnički račun korišten u trenutku. Radi se o ugovornim pravima i obvezama na koje korisnički račun pristaje prilikom sklapanja ugovora internetskog priključka. Djeca često izvode štetne radnje koristeći se rizičnim mrežnim stranicama koje dovode roditeljski korisnički račun u opasnost. Primjerice, maltretiranje preko roditeljskog korisničkog računa može krenuti u sasvim krivom smjeru pa tako može doći i do prijave korisničkog računa. Zbog navedenih mogućih situacija preporučljivo je ne koristiti istu privatnu i poslovnu elektroničku adresu. Poslodavci su u trenutku terećenja poslovnog korisničkog računa jednog od radnika u nezgodnoj situaciji. Razlog tome može rezultirati povredi ljudskih prava, kršenju poslovne tajne, dijeljenje povjerljivih podataka i slično.

Djeca ponekad svjesno riskiraju sigurnost upisujući tako podatke s bankovnih kartica roditelja bez njihova znanja na neprovjerene internetske stranice. Tim načinom uplaćuju novac za kupnju video igrica, gledanje neprimjerenih sadržaja i slično. Mrežne stranice potom nisu provjerene od strane roditelja, a djeca nemaju potrebno znanje da bi provjerili je li stranica sigurna. Često putem ovakvih sličnih situacija dolazi do prijevara ili krađe podataka.

Podaci koji se prikupljaju u slučaju da ih djeca upišu bez roditeljskog nadzora, a sa njihovih korisničkih računa mogu se prikupljati u svrhu demografskih podataka. Tada primjerice, internetske stranice traže od korisnika da unesu podatke poput dobi, spola, lokacije, obrazovanja ili interesa na temelju čega analiziraju sklonosti svih posjetitelja. Često su na internetu vidljive razne reklame koje su zapravo mamci djeci na temelju njihovih odabranih interesa i stvari koje vole. Ti podaci se prikupljaju već ranije spomenutim takozvanim „kolačićima“ (eng. Cookies). Prikupljaju se na način da operatori mrežnih sjedišta prilikom posjete istih koriste upisane informacije koje su djeca unijela uključujući osobne podatke ili posjećene stranice u svrhu reklama. (Aftab, 2003)

Kako bi prevenirali navedene rizike koji su najpoznatiji bitno je pravovremeno educirati mlađe uzraste o mogućim dešavanjima. Dati im do znanja kako nisu potpuno sami u takvim situacijama i ponuditi im se za potrebnu podršku te pomoć. Komunikacija je ključna te je važno naglasiti djeci koliko god se nepoznate osobe činile zanimljivima i dobronamjernima to i dalje ne znači da im se može vjerovati. (Centar za sigurniji internet, 2022)

4.3.2. Zakon i propusti zaštite podataka djece na internetu

Postoje zakonske regulative kako bi se adekvatno zaštitila djeca konkretno govoreći na internetu suočavajući se s prijetnjama, online zlostavljanjima, krađi podataka i nasilju. Pravni okvir pod nazivom „Zakon o elektroničkim medijima“ sadrži glavne odrednice prema kojima djeca imaju puno pravo zaštite. Kada je riječ o zaštiti podataka i svemu što ono obuhvaća tada zakon o elektroničkim medijima, objavljen u narodnim novinama člankom 24. stavkom 5. jasno definira sljedeće tvrdnje: „Nije dopušteno objavljivanje informacije kojom se otkriva identitet djeteta do 18. godine života uključenog u slučajeve bilo kojeg oblika nasilja, bez obzira je li svjedok, žrtva ili počinitelj ili je dijete pokušalo ili izvršilo samoubojstvo, a niti iznositi pojedinosti iz djetetovih obiteljskih odnosa i privatnog života.“ Navedeno pravilo je jasno definirano te ne postoji niti jedan izuzetak referirajući se na članak. (Narodne novine, 2021)

Sve internetske stranice, forumi, blogovi i drugi oblici medija na neki način ugrožavaju privatnost i sigurnost djeci. Istraživanja su pokazala kako je nastupila velika razlika u prošlosti i sadašnjosti vezana za djecu i korištenje interneta.

Prava djece nastupaju u raznim aktima kao što je *Ustav Republike Hrvatske* ili *Opća deklaracija o pravima čovjeka*. Među tim navedenim dokumentima teži se ka očuvanju čovjekove intime, no za djecu jedan možda od najvažnijih dokumenata jest *Konvencija Ujedinjenih naroda o pravima djeteta.* Spomenuta konvencija o pravima djeteta jamči za zaštitu djeteta sa dodatnim protokolima koji proširuju mjere zaštite. Usprkos svim navedenim zakonima, *Kazneni zakon* čl. 201. propisuje kako će biti kažnjen novčanom ili zatvorskom kaznom upravo onaj tko iznese nešto iz osobnog života drugoga. Često se dogodi da novinari objave djetetov identitet sasvim slučajno bez ičije dozvole pa tako ugroze dječja prava. Identitet se može otkriti objavom fotografije ili čak objavom inicijala, podacima o obiteljskim prilikama i slično. Ovakvi zakoni stekli su uspješnu provedbu kada je riječ o neovlaštenom korištenju osobnih podataka. (Jelavić i sur., 2009)

Sam zakon koji se odnosi na zaštitu podataka djece ima i nekoliko propusta pravnog okvira. Unatoč tome što zakon jasno propisuje zakone određenim stavcima, vidno nedostaje nekoliko odrednica koje nisu definirane. Iako „Opća uredba o zaštiti podataka“ zahtjeva da se za djecu mlađu od 18 godina traži roditeljski ili pristanak skrbnika, ne poštuju sve internetske stranice tu stavku. Mnoge poznate platforme i aplikacije ne primjenjuju mjere dovoljno strogo, dopuštajući maloljetnoj djeci registriranje i korištenje usluga. To omogućava djeci da nesmetano dijele osobne podatke čime se povećava rizik od zloupotrebe tih istih podataka. Mnogi roditelji i skrbnici nisu u potpunosti svjesni svojih zakonskih prava pa se tako i teže učinkovito zaštititi u virtualnom svijetu.

Jedan od problema je taj što mnoge aplikacije i platforme kojima se djeca u današnjem virtualnom svijetu koriste, nisu smještene unutar Republike Hrvatske ili Europske unije. Što itekako stvara prepreke u primjeni lokalnih zakona. Obzirom da određena internetska sjedišta još uvijek nisu usklađena sa uredbom o zaštiti podataka to čini težu provedbu zakona. Iako postoje međusobne suradnje zakonodavnih tijela za zaštitu podataka, provedba zakona ostaje izazov zbog nesuglasica u zakonodavstvu različitih država. (Centar za sigurniji internet, 2025)

4.3.3. Europska strategija za bolji internet za djecu

U suvremenom virtualnom svijetu mlađi uzrasti provode vremena najviše, koristeći ga u razne svrhe. Kako bi se osigurala još veća sigurnost predstavljena je „Europska strategija za bolji internet za djecu“ – Better Internet for Kids (BIK). Prvi puta je predstavljena 2012. godine, a ažurirana je kasnije u 2022. godini kako bi se prilagodila novim izazovima virtualnog svijeta. Europska strategija za bolji internet za djecu temelji se na četiri glavna cilja:

1. Stvaranje digitalnog sadržaja i usluga prilagođenih djeci
   - digitalne platforme su organizirane i dizajnirane tako da omogućuju sigurno iskustvo za djecu, bez izloženosti štetnom sadržaju,
   - potiče se razvoj mrežnih stranica koje pružaju edukativne i interaktivne sadržaje.
2. Osnaživanje djece za odgovorno i sigurno korištenje interneta
   - educiranje o digitalnoj pismenosti, kako bi se predvidjele i spriječile eventualne opasnosti,
   - organiziranje različitih programa i radionica koje djecu podučavaju o zaštiti osobnih podataka i sigurnom komuniciranju na internetu.
3. Zaštita djece od rizika i štetnog sadržaja na internetu
   - jačanje sigurnosnih sustava,
   - unaprjeđenje zakonodavnog okvira koji štiti djecu u virtualnom svijetu.
4. Sudjelovanje djece u oblikovanju digitalnih politika
   - prilagođavanje interneta potrebama za mlađe uzraste,
   - organiziranje inicijativa koje potiču inovativnost i kreativnost djece te im omogućuju aktivno sudjelovanje u oblikovanju virtualnog svijeta. (Europska komisija, 2024)

4.4. Odgovorna uporaba interneta

Kako bi prevenirali djecu od izlaganja opasnim situacijama potrebna su ograničenja i nadzori prilikom korištenja virtualnog svijeta. Mnogi roditelji prakticiraju ovakve preventivne mjere koje uključuju razne aplikacije ili softverske alate za roditeljski nadzor. Alati su raznovrsni i pružaju raznolik odabir zaštite te omogućuju filtriranje neprimjerenog sadržaja, praćenje aktivnosti na internetu, postavljanje

vremenskih ograničenja te blokiranje pristupa određenim aplikacijama ili mrežnim preglednicima odnosno stranicama. Neke od njih nazivaju se Qustodio, Net Nanny i Norton Family. Korištenjem navedenih, postavljaju se jasna pravila o vremenu provedenom online i vrstama sadržaja prema kojima dijete ima dozvoljen pristup.

Ovakav pristup kao što je i prije u radu bilo navedeno vrsta je aktivnog nadzora, čime roditelji imaju punu kontrolu korištenim sadržajima te na taj način mogu bolje razumjeti djetetovo virtualno okruženje. Naravno, takvi alati većinom nisu besplatni pa će roditelji za primjerice, godišnje korištenje Qustodio morati izdvojiti do 76 eura. Dok primjerice oni besplatni poput Google Family Link-a ili Microsoft Family Safety-a nude osnovne funkcionalnosti praćenja i zaštite bez dodatnih troškova. Iako besplatni alati mogu biti dovoljni za osnovnu kontrolu, napredniji alati poput Qustodio-a često nude više opcija i detaljnije izvještaje, što može opravdati cijenu za roditelje koji traže dodatnu sigurnost i kontrolu. Kod ovakvih alata djetetu se automatski blokira pristup neprimjerenim sadržajima pa na primjer roditelji mogu postaviti ograničenja i na taj način. Roditelji korištenjem ovakvih alata često postavljaju dnevne ili tjedne limite za vremensko ograničenje, a također isti alati omogućuju geolokacijsko praćenje kako bi roditelji u svakom trenutku znali gdje se dijete nalazi. Roditelji mogu primati obavijesti o sumnjivim aktivnostima i pregledavati detaljne izvještaje o ponašanju djeteta na internetu. Ovakav alat funkcionira da se instalira na djetetov uređaj što može uključivati računalo, tablet ili mobitel, a roditelji putem vlastite nadzorne ploče mogu pratiti i postavljati razna dostupna ograničenja. Roditelji kao obavijesti mogu dolaziti alarmi i upozorenja na nekakva sumnjiva događanja ili primjerice posjeti zabrinjavajućim internetskim stranicama. Također, alati pružaju SOS gumb koje dijete može poslati roditelju kao poziv u pomoć. Konkretno spomenuti alat Qustodio omogućava praćenje i blokiranje telefonskih poziva te poruka usmjerenih na djetetov uređaj. (Qustodio, 2025)

Postoje i sigurne tražilice koje su dizajnirane kako bi zaštitile djecu te osigurale sigurnije i privatnije iskustvo pretraživanja. Takve tražilice nude većinom edukativne rezultate i mjerodavne izvore informacija te ne prikazuju štetne reklame. Među najpopularnijima su Kiddle (https://www.kiddle.co) ili KidzSearch (https://www.kidzsearch.com). Tražilice kao takve funkcioniraju na način da filtriraju neprimjeren sadržaj ili sadržaj koji izlaže djecu opasnostima. Tražilice su osmišljene

tako da vode računa o dječjoj privatnosti te ujedno i sprječavaju prikupljanje osobnih podataka. (Školski portal, 2016)

Kako danas postoji velik broj aplikacija i platformi to bi značilo da je potrebito kreirati više lozinki. Pojedini korisnici koriste jednu lozinku za sve kako bi pojednostavili, ali tada se zapravo izlažu potencijalnom riziku. Ako primjerice, hakeri probiju lozinku, a za sve je ista, to znači da su svi korisnikovi podaci ugroženi. Kao velika pomoć u tome, upravitelj lozinki odnosno aplikacija za čuvanje i sigurno pohranjivanje lozinki je osmišljena. Postoje različiti upravitelji lozinki, a neki čak dolaze i automatski instalirani na mobilne uređaje. Ovisi o tome koliko mogućnosti same aplikacije nude, plaćaju li se iste ili ne. (Centar za sigurniji internet, 2023)

4.4.1. Mrežni bonton

Kako bi korištenje virtualnim svijetom bilo kontrolirano, postoje nekoliko pravila osmišljena primarno za djecu za korištenje internetom i njegovim sadržajem. Neka od najbitnijih kodeksa ponašanja jesu:

- Podrazumijeva se da mjesta poput internetskih stranica, foruma ili blogova uključuju pristojno ponašanje. Bez uvreda ili zlobnih komentara.
- Prilikom slanja informacija – priupitajte se tri stvari: „Jesu li informacije koje šaljete: dobre, istinite i korisne?“
- Zabranjeno je koristiti se psovkama te vrijeđati i širiti agresivno ponašanje. Razmislite prije unošenja teksta!
- Izbjegavajte komunikaciju u kojoj se drugu žrtvu napada.
- Izbjegavajte na internetu objavljivati ili unositi osobne podatke te podatke svojih bližnjih. Štitite svoju i tuđu privatnost!
- Ne komunicirajte s nepoznatim osobama.
- Ne činite ništa protuzakonito i neskladno s moralnim normama. (Oblak znanja, 2012)

5. Budućnost zaštite podataka

Globalna povezanost omogućila je sve brži pristup informacijama te svakodnevni protok raznih informacija i podataka. Međutim, uz sve brojne prednosti koje samo virtualno okruženje donosi s time dolazi i mnoštvo pitanja vezana za budućnost, posebno kada je riječ o sigurnosti i privatnosti korisnika. Obzirom da se svakim danom generiraju i pohranjuju ogromne količine podataka, od onih osobnih do povjerljivih poslovnih, postavlja se pitanje zaštite. S jedne strane, napredne tehnologije otvaraju vrata novim mogućnostima, no s druge strane, stvaraju i ranjivost koje mogu biti iskorištene na štetu korisnika.

Aktualnih pitanja za zaštitu podataka je sve veći broj, a odgovori su tek u fazi razvoja. Stalno prilagođavanje postojećih sigurnih strategija i zakonodavnih okvira u korak je s tehnološkim inovacijama. Mnoge zemlje i organizacije nastoje uspostaviti učinkovitije načine za zaštitu podataka međusobnom suradnjom. U tom kontekstu, budućnost zaštite podataka zahtijeva globalnu suradnju, inovativne pristupe te stalno obrazovanje korisnika.

5.1. Implementacija Blockchain tehnologije

Blockchain tehnologija kako i sam naziv ističe sastoji se od nanizanih blokova koji su povezani u lanac gdje svaki blok sadrži niz zapisa. Takva vrsta tehnologije koristi se za upisivanje transakcija na računalima. Svaki blok ima određenu količinu zapisa ovisno o tome koliko može pohraniti. Također, blok sam za sebe veže se na prethodni blok putem njihovog redoslijeda. Vezu između blokova teško je probiti jer njen algoritam koristi visoku razinu slanja poruka koje može razumjeti samo onaj kojemu je poruka namijenjena. Kada bi se redoslijed pokušao poremetiti primjerice napadom na blokove, onda bi se vrlo lako pomoću referenci povezao s prethodnim blokom.

Danas mnoge industrije pokušavaju implementirati takvu vrstu tehnologije u svoje poslovanje. Postoje mnoge vrste blockchainova jer je tehnologija istih fleksibilna te se prilagođava željenim potrebama i uvjetima. Najpoznatiji tip blockchaina jest upravo onaj javni gdje su svi podaci javno dostupni te se mogu čitati i pisati od bilo koga tko je dio te mreže na primjer – Bitcoin. Dok je privatni blockchain ograničen na

određene entitete ili organizacije. Pristup mreži je kontroliran i samo odabrani korisnici mogu obavljati transakcije. Postoje još mnogi nenavedeni oblici blockchain tehnologije, a razlika je većinom u sigurnosti i primjeni te performansama.

Primjena Blockchain tehnologije sadrži široku raspodjelu putem računala kao prednost korištenja. Kao još veću prednost ističe se decentarlizirana mreža što znači da svaka osoba može sudjelovati u mreži, potvrđivati transakcije i koristiti se njenim uslugama. Iako su transakcije javno dostupne, tretiraju se kao povjerljive, što može zvučati nesigurno na prvi pogled. S druge strane, blockchainovi suočavaju se s problemima poput velike potrošnje energije pa tako usporavaju procesiranje transakcija. Izbor između vrsta blockchainova ovisi o potrebama i prioritetima korisnika. (Živković, 2018)

5.2. Razvoj umjetne inteligencije kao utjecaj na zaštitu podataka

Umjetna inteligencija prema definiciji simulira ljudsku inteligenciju te predstavlja sposobnost nekog uređaja da riješi problem. Sustavi umjetne inteligencije dizajnirani su kako bi rasuđivali, zaključivali i donosili odluke. Glavni ciljevi umjetne inteligencije su automatizacija procesa i stvaranje inteligentnih rješenja koja moju pomoći u raznim industrijama poput zdravstva, industrije ili financija. Računalo radi na način da prima podatak koje u konačnici obradi te daje odgovor. Kako bi umjetna inteligencija pravilno funkcionirala, potrebne su velike količine podataka. Primjene umjetne inteligencije su razne – od inovacija vezane za transport automobilima i njegovim modernim sustavom do usluga na društvenim mrežama koje se temelje na korisničkim interesima. Umjetna inteligencija je već nekoliko godina korištena za filtriranje neželjene i phishing elektroničke pošte. Takva tehnologija danas pomaže u prepoznavanju perspektivnih prijetnji te dodatno osigurava mrežu. Sustavi umjetne inteligencije rade na način da analiziraju moguće probleme i usputno ih rješavaju pa tako isti rade na boljoj analizi i rukovanju samih podataka. Kao prednosti umjetne inteligencije kod zaštite podataka izdvajaju se

- automatsko šifriranje podataka i kontroliranje pristupa te provjera autentičnosti korisnika
- analiza sumnjivih transakcija kako bi se otkrile neautorizirane financijske aktivnosti i spriječile prijevare

- prepoznavanje i blokiranje sumnjivih zahtjeva
- identifikacija biometrijom poput otiska prsta i prepoznavanja lica te analizom ponašanja koja se očitava praćenjem načina unosa lozinke ili kretanja miša
- korištenje analitike za pravovremeno prepoznavanje potencijalnih ranjivosti i sprječavanje budućih napada

Integracija umjetne inteligencije u sustav zaštite podataka donosi značajne prednosti te povećava sigurnost korisnika i pruža bržu detekciju mogućih prijetnji. Umjetna inteligencija koristi napredne algoritme koje automatizirano otkrivaju probleme. Još uvijek, umjetna inteligencija nije dostigla besprijekoran rad te je potrebno još mnogo usavršavanja, prilagodbe i učenja. (Sabo, 2024)

6. ZAKLJUČAK

Ovim radom zaključuje se da osobni podaci nikada nisu bili u potpunosti sigurni. Doza privatnosti na koju pojedinac ima potpuno pravo je sve manja. Zaštita osobnih podataka uvijek će predstavljati veliku važnost jer sadržava sve bitne dokumente, informacije i podatke vezane za pravna ili ljudska tijela. Zahvaljujući zakonu te Europskoj konvenciji i općim uredbama o očuvanju podataka te zaštiti ljudskih prava i temeljnih sloboda osigurana je određena zaštita od neovlaštenih pristupa i zloupotreba osobnih podataka. Osobne podatke teško je zaštititi pogotovo zbog interneta i korištenje platformi istog. Osim što tehnologija napreduje brže nego ikad, načini na koji se komunicira, radi i dijeli podatke omogućava različite oblike prijetnji, a da pojedinac često nije ni svjestan kakve posljedice te prijetnje mogu izazvati. Nikada se ne zna tko se nalazi iza drugog ekrana te pokušava li osobu prevariti ili ne te je stoga potrebito biti oprezan i pokušati zaštititi osobne podatke koliko je god to moguće. Pogotovo zbog važne činjenice koja pokazuje da se tehnologija u današnjem svijetu brzo izgrađuje te još brže napreduje.

Kada je riječ o sigurnosti podataka, korisnici moraju biti svjesni da ih neće moći u potpunosti zaštititi ako ih dijele s drugim korisnicima na mrežnim stranicama. Kroz moguće napade phishinga, virusa i druge oblike prijetnji, podaci se mogu ukrasti i zloupotrijebiti. Kao odgovor na navedene prijetnje, veliku ulogu ima zakon poput Opće uredbe o zaštiti podataka (GDPR). Uredba je postavljena na visokoj razini sadržavajući veću kontrolu nad korisničkim osobnim podacima.

Međutim, zaštita podataka nije do kraja osigurana, a značajnu promjenu u načinu zaštite podataka obećava upravo Blockchain tehnologija. Ista omogućava sigurniji način pohrane podataka te nudi snažnu zaštitu od krađe istih.

Umjetna inteligencija također zauzima veliki utjecaj na zaštitu podataka. Ona može pomoći u identifikaciji te analizi potencijalnih sigurnosnih prijetnji. Sustavi umjetnih inteligencija mogu prepoznati napade na korisnika ili neuobičajene transakcije koje nisu autorizirane. Korištenjem umjetne inteligencije osigurava se jača autentifikacija putem biometrijskih podataka, kao što su prepoznavanje lica ili otisak prsta. Takvim se strogim sigurnosnim sustavom smanjuje rizik od neovlaštenog pristupa podacima. Nedostaci dolaze na vidjelo kada umjetna inteligencija uključuje prikupljanje i obradu velikih količina osobnih informacija.

Iako će se tehnologija uvijek razvijati, važnost podataka će uvijek biti na prvom mjestu. Moderne već spomenute tehnologije kao što su Blockchain i umjetna inteligencija svakako pomažu u zaštiti podataka, ali prava zaštita počinje s osobnom odgovornošću korisnika. Stoga je ključno biti u korak s vremenom i poduzeti proaktivne mjere zaštite koje uključuju jake lozinke, autentifikacije putem dvaju faktora do permanentne edukacije o mogućim prijetnjama.

Literatura

Aftab, P. (2003). *Kako prepoznati opasnosti interneta, vodič za škole i roditelje*. 103-104, 106-107, 115-124, Zagreb: NERETVA d.o.o.

Agencija za zaštitu osobnih podataka (2025). *Phishing napadi – kako ih prepoznati i zaštititi se.* Preuzeto 20.1.2025. s https://azop.hr/phishing-napadi-kako-ih-prepoznati-i-zastititi-se/

Barjaktar, B., i Ivanović, M. (2019*). Pravo na pristup informacijama i zaštita podataka. Zbirka propisa*. 5, 65, 69-71, 74, Zagreb: Grafički zavod Hrvatske.

Bilić, V. (2020). *Odgajanje i odrastanje u digitalnom vremenu.* 10-22, 126-129, Zagreb: Obrazovni izazovi.

Bilić, V. i sur. (2012). *Nasilje nad djecom i među djecom.* 304, Zagreb: Naklada Slap.

Boban, M., (2012). *Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu.* 575.-598, Zbornik radova pravnog fakulteta u Splitu. Preuzeto 24.1.2025. s https://hrcak.srce.hr/file/129212

Brljafa, B. (2022). *Utjecaj društvenih mreža na razvoj društva* (Završni rad). 9, Pula: Sveučilište Jurja Dobrile u Puli. Preuzeto 18.1.2025. s https://urn.nsk.hr/urn:nbn:hr:137:229242

Centar za sigurniji internet (2022). *Lažna online prijateljstva – Grooming.* Preuzeto 31.1.2025. s https://csi.hr/2022/11/09/lazna-online-prijateljstva-grooming/

Centar za sigurniji internet (2023). *Aplikacije za sigurno čuvanje lozinki*. Preuzeto 31.1.2025. s https://csi.hr/2023/09/28/aplikacije-za-sigurno-cuvanje-lozinki/

Centar za sigurniji internet (2023). *Opasnosti dijeljenja lokacije*. Preuzeto 25.1.2025. s https://csi.hr/2023/11/24/opasnosti-dijeljenja-lokacije/

Centar za sigurniji internet (2023). *Roditeljski nadzor kao alat za digitalnu dobrobit.* Preuzeto 28.1.2025. s https://csi.hr/2023/01/11/roditeljski-nadzor-kao-alat-za-digitalnu-dobrobit/

Centar za sigurniji internet (2024). *Kako aplikacije za roditeljski nadzor pomažu u zaštiti djece u digitalnom svijetu*. Preuzeto 28.1.2025. s

https://csi.hr/2024/11/21/kako-aplikacije-za-roditeljski-nadzor-pomazu-u-zastiti-djece-u-digitalnom-svijetu/

Centar za sigurniji internet (2024). *Koliko je privatno 30.1.2025. pretraživanje (Incognito Mode) uistinu privatno?* Preuzeto s https://csi.hr/2024/08/08/koliko-je-privatno-pretrazivanje-incognito-mode-uistinu-privatno-auto-skica/

Centar za sigurniji internet (2025). *Pravni aspekti zaštite djece na internetu*. Preuzeto 1.2.2025. s https://csi.hr/2025/01/09/pravni-aspekti-zastite-djece-na-internetu/

CERT. *O virusima.* Preuzeto 22.1.2025. s https://www.cert.hr/virusi/

Ciboci, L. i sur. (2011). *Djeca medija – od marginalizacije do senzacije*. 11-12, 16-24, 35-52, Zagreb: Matica Hrvatska.

Europska komisija (2024). *Europska strategija za bolji internet za djecu (BIK+).* Preuzeto 31.1.2025. s https://digital-strategy.ec.europa.eu/hr/policies/strategy-better-internet-kids

Goljački, M. (2022). *Metode prijevara na internetu* (Završni rad). 3-4, 6-7, 10, 12, 14, 16, Zagreb: Sveučilište u Zagrebu, Filozofski fakultet. Preuzeto 17.1.2025. s https://urn.nsk.hr/urn:nbn:hr:131:372132

Hrvatska akademska i istraživačka mreža – CARNET (2018). *Sigurnije na internetu*. Preuzeto 15.1.2025. s https://www.cert.hr/wpcontent/uploads/2018/02/Sigurnije_na_internetu.pdf

Ilišin, V. i sur. (2001). *Djeca i mediji – uloga medija u svakodnevnom životu djece*. 15-19, Zagreb: Državni zavod za zaštitu obitelji, materinstva i mladeži; Institut za društvena istraživanja.

Jelavić, M. i sur. (2009). *Zaštita privatnosti djece u medijima – Zbornik priopćenja s tribine.* 9-21, Zagreb: Pravobranitelj za djecu.

Kamar, E. i sur. (2022). *Computers in Human Behavior - Parental guardianship and online sexual grooming of teenagers: A honeypot experiment*. Preuzeto 27.1.2025. s https://www.sciencedirect.com/science/article/abs/pii/S0747563222002084

Kelam, I. (2018). *Socijalni inženjering kao metoda otkrivanja povjerljivih informacija* (Završni rad). 1-2, 4, 17, Split: Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti. Preuzeto 25.1.2025. s https://urn.nsk.hr/urn:nbn:hr:227:562560

Klarić, M. (2016). *Zaštita osobnih podataka i Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda.* Zbornik radova Pravnog fakulteta u Splitu*, 53* (4), 973-990. Preuzeto 10.1.2025. s https://doi.org/10.31141/zrpfs.2016.53.122.973

Knez Radolović, J. i Renić, M. (2024). *Djeca u digitalnom okruženju – Vodič za roditelje predškolaraca*. 4-10, Zagreb: Roditelji u akciji – RODA.

Krbavac, F. (2023). *Utjecaj Opće uredbe o zaštiti podataka na privatnost osobnih podataka na internetu* (Diplomski rad). 3, Zagreb: Sveučilište u Zagrebu, Ekonomski fakultet. Preuzeto 10.1.2025. s https://urn.nsk.hr/urn:nbn:hr:148:519914

Kušer, M. (2016). *Zaštita od virusa u Windows operacijskim sustavima* (Završni rad). 2, 3, 7, Osijek: Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek. Preuzeto 20.1.2025. s https://urn.nsk.hr/urn:nbn:hr:200:102828

Lessig, L. (2004*). Code and Other Laws of Cyberspace*. 91, 141, 192-197, New York.

Li, Q. (2010). *Cyberbullying in High Schools: A Study of Student Behaviours and Believes about this New Phenomenon. Journal of Agression, Maltreatment and Trauma*. Preuzeto 16.1.2025. s https://www.tandfonline.com/doi/full/10.1080/10926771003788979#d1e247

MacEachern, R. (2012). *Cyberbullying - učini nešto: prekini lanac elektroničkog nasilja*. 4-5, 9-14, Zagreb: Mosta Viridis.

Maleš, D. i Stričević, I. (2005). *Moja prava*. 24, Zagreb: Udruženje Djeca prva.

Mamula, M. i Mihaljević, K. (2019). *#surfambezstraha* (brošura). 8-9, Zagreb: Ženska soba – Centar za seksualna prava.

Marjanović, B. i sur. (2008). *Jeste li još uvijek sigurni da ste sigurni*? 58-67, Zagreb: Mozaik knjiga.

Microsoft Security (2025). *Što je dvostruka provjera autentičnosti?* Preuzeto 20.1.2025. s https://www.microsoft.com/hr-hr/security/business/security-101/what-is-two-factor-authentication-2fa

Microsoft Support (2025). *Sprječavanje i uklanjanje virusa i drugog zlonamjernog softvera.* Preuzeto 20.1.2025. s https://support.microsoft.com/hr-hr/topic/sprje%C4%8Davanje-i-uklanjanje-virusa-i-drugog-zlonamjernog-softvera-53dc9904-0baf-5150-6e9a-e6a8d6fa0cb5

Mihaljević, K. i Tukara Komljenović, J. (2017). *#reagiraj - elektroničko seksualno nasilje nad i među djecom i mladima* (brošura). 28, Zagreb: Ženska soba – Centar za seksualna prava.

Ministarstvo unutarnjih poslova (2025). *Internet prijevare.* Preuzeto 18.1.2025. s https://policija.gov.hr/prevencija/racunalna-sigurnost/internet-prijevare/456

Narodne novine (2009). *Opća deklaracija o ljudskim pravima*. 11.1.2025. Preuzeto s https://narodne-novine.nn.hr/clanci/medunarodni/2009_11_12_143.html

Narodne novine (2012). *Zakon o zaštiti osobnih podataka*. Preuzeto 12.1.2025. s https://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html

Narodne novine (2021). *Zakon o elektroničkim medijima*. Preuzeto 29.1.2025. s https://narodne-novine.nn.hr/clanci/sluzbeni/2021_10_111_1942.html

Oblak znanja (2012). *Internetski bonton – Pravila lijepog ponašanja na internetu*. Preuzeto 31.1.2025. s https://www.oblakznanja.com/2012/01/internetski-bonton-pravila-lijepog-ponasanja-na-internetu/

Radelić, B. i sur. (2017). *Zaštita osobnih podataka i granice zaštite privatnosti radnika.* 28-50, Zagreb: Orbis impressio d.o.o.

Ružić, N. (2011). *Zaštita djece na internetu*. 156-160, pregledni rad. Preuzeto 24.1.2025. s file:///C:/Users/Vanesa/Desktop/DIPLOMSKI/zastita%20djece%20na%20internetu.pdf

Sabo, A. (2024). *Umjetna inteligencija u prostoru kibernetičke sigurnosti* (Završni rad). 2-9, Zagreb: Sveučilište u Zagrebu, Filozofski fakultet. Preuzeto 2.2.2025. s https://urn.nsk.hr/urn:nbn:hr:131:023600

Stanković, D. (2024). *Osobe treće životne dobi kao mete internetskih prijevara* (Diplomski rad). 6-10, 17, Osijek: Sveučilište Josipa Jurja Strossmayera u Osijeku, Akademija za umjetnost i kulturu u Osijeku. Preuzeto 22.1.2025. s https://urn.nsk.hr/urn:nbn:hr:251:472090

Školski portal (2016). *Kiddle: Internet preglednik za djecu*. Preuzeto 30.1.2025. s https://www.skolskiportal.hr/sadrzaj/iz-skolskog-svijeta/kiddle-internet-preglednik-za-djecu/

Šostar, Z. i sur. (2006). *Nasilje preko interneta (cyberbullying).* 12, Zagreb: Poliklinika za zaštitu djece grada Zagreba.

Tandara, L. (2020). *Virtualni svijet i pitanje otuđenosti mladih* (Diplomski rad). 36. Zagreb: Sveučilište u Zagrebu, Fakultet hrvatskih studija. Preuzeto 25.1.2025. s https://urn.nsk.hr/urn:nbn:hr:111:515760

Težak, Đ. (2010). *Internet – poslije oduševljenja*. 44, Zagreb: Hrvatska sveučilišna naklada.

Vrančić, I. (2019). *Hakeri i njihova etika* (Diplomski rad). 11,13,17,36, Zagreb: Sveučilište u Zagrebu, Filozofski fakultet. Preuzeto 22.1.2025. s https://urn.nsk.hr/urn:nbn:hr:131:065368

Vukoje, G. (2022). *Sigurnost djece na internetu - zaštita osobnih podataka* (Diplomski rad). Pula: Sveučilište Jurja Dobrile u Puli. Preuzeto 18.1.2025. s https://urn.nsk.hr/urn:nbn:hr:137:463774

Zakon.hr (2018.). *Opća uredba o zaštiti podataka*. 14.1.2025. Preuzeto s https://www.zakon.hr/z/1021/Op%C4%87a-uredba-o-za%C5%A1titi-podataka---Uredba-%28EU%29-2016-679

Zgrabljić Rotar, N. (2017). *Novi mediji digitalnog doba. Informacijska tehnologija i mediji.* 56-67, Zagreb: Hrvatski studiji Sveučilišta u Zagrebu.

Žderić, J. (2009). *Medijska kultura djece i mladih – Mogućnosti i zamke*. 47-50, Zagreb: Udruga Medioteka.

Žilić, M. i Maček, N. (2022). *Mali koraci za sigurno dijete – priručnik za roditelje i stručnjake koji rade s djecom rane, predškolske i rane školske dobi*. 38-39, Zagreb: Novi redak.

Živković, S. (2018). *Blockchain tehnologija : Blockchain tehnologija* (Završni rad). 2-4, Rijeka: Sveučilište u Rijeci. Preuzeto 2.2.2025. s https://urn.nsk.hr/urn:nbn:hr:195:472651

Qustodio (2025). Preuzeto 1.2.2025. s https://www.qustodio.com/en/

Your Europe (2021). *Zaštita podataka na temelju Opće uredbe o zaštiti podataka.* Preuzeto 17.1.2025. s https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_hr.htm

SAŽETAK

Sigurnost i zaštita podataka ključni su izazovi u virtualnom svijetu današnjice. Posebice u kontekstu rastuće prisutnosti korisnika. Uz brojne prednosti kao takvo, virtualno okruženje donosi i svakakve oblike prijetnji poput krađe osobnih podataka, identiteta i mnogih drugih. Poseban izazov predstavlja zaštita djece koja su jedna od najranjivijih skupina na internetu. Sama budućnost i sve što ona nosi znatno će ovisiti o tehnološkom napretku i razvitku zaštite podataka. Sigurnost na internetu postaje sve složenija, no budući razvoj sigurnosnih mehanizma i edukacija korisnika itekako mogu pridonijeti stvaranju sigurnijeg virtualnog okruženja za sve korisnike.

Ključne riječi: sigurnost, zaštita podataka, privatnost, edukacija, tehnološki napredak, virtualni svijet

SUMMARY

Security and data protection are key challenges in today's virtual world, especially in the context of the growing presence of users. Despite numerous advantages, the virtual environment also brings various threats, such as identity theft, personal data theft, and many others. A particular problem is the protection of children, who are one of the most vulnerable groups on the Internet. The future, and everything it holds, will largely depend on technological progress and the development of data protection. Internet security is becoming increasingly complex, but the future development of security mechanisms and stronger user education can contribute to creating a safer virtual environment for all users.

Key words: security, data protection, privacy, education, technological progress, virtual world