Izazovi digitalnog svijeta

Borić Letica, Ivana; Borovac, Tijana; Duvnjak, Ivana; Grgić, Krešimir; Herceg Pakšić, Barbara; Horvat, Ivan; Ilakovac, Vesna; Kralik, Kristina; Nenadić, Krešimir; Romstein, Ksenija; ...

Izazovi digitalnog svijeta

UREDILI
Tena Velki
Krešimir Šolić

Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakulet za odgojne i obrazovne znanosti

Izazovi digitalnog svijeta

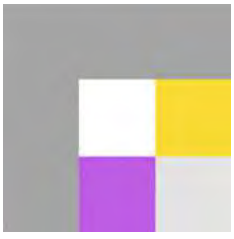
Uredili:
Tena Velki
Krešimir Šolić

Autori:
Ivana Borić Letica
Tijana Borovac
Ivana Duvnjak
Krešimir Grgić
Barbara Herceg Pakšić
Ivan Horvat
Vesna Ilakovac
Kristina Kralik
Krešimir Nenadić
Ksenija Romstein
Valentina Ružić
Daniela Šincek
Krešimir Šolić
Tena Velki
Goran Vojković
Marin Vuković

Izdavanje udžbenika sufinanciralo je
Društvo psihologa Osijek

Fakultet za odgojne i obrazovne znanosti
Sveučilišta Josipa Jurja Strossmayera u Osijeku

Izazovi digitalnog svijeta



Osijek, 2019.

Urednici:
izv. prof. dr. sc. Tena Velki
doc. dr. sc. Krešimir Šolić

Autori:
Ivana Borić Letica
Tijana Borovac
Ivana Duvnjak
Krešimir Grgić
Barbara Herceg Pakšić
Ivan Horvat
Vesna Ilakovac
Kristina Kralik
Krešimir Nenadić
Ksenija Romstein
Valentina Ružić
Daniela Šincek
Krešimir Šolić
Tena Velki
Goran Vojković
Marin Vuković

Recenzenti:
prof. dr. sc. Marin Golub, Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu
prof. dr. sc. Mirela Župan, Pravni fakultet, Sveučilište Josipa Jurja Strossmayera u Osijeku
izv. prof. dr. sc. Silvija Ručević, Filozofski fakultet, Sveučilište Josipa Jurja Strossmayera u Osijeku

Lektorica:
Lidija Bakota

Naslovnica:
Igor Plac

Oblikovanje i grafička priprema:
Zebra, Vinkovci

Nakladnici:
Fakultet za odgojne i obrazovne znanosti
Sveučilište Josipa Jurja Strossmayera u Osijeku

Naklada
500 komada

ISBN 978-953-6965-88-5
CIP zapis dostupan je u računalnom katalogu Gradske i sveučilišne
knjižnice Osijek pod brojem 141218058.

Objavljivanje ove knjige odobrio je Senat Sveučilišta Josipa Jurja Strossmayera u Osijeku
na sjednici 29. listopda 2019. pod brojem 26/19.

Sadržaj

Predgovor

Izdavanje sveučilišnog interdisciplinarnog udžbenika pod nazivom *Izazovi digitalnog svijeta* rezultat je višegodišnjeg znanstvenog istraživanja, a obuhvaća inženjere, psihologe i pravnike – doktore znanosti i priznate stručnjake u svojim područjima. Ukupno 14 autora s različitih fakulteta Sveučilišta J. J. Strossmayera u Osijeku te Sveučilišta u Zagrebu napisalo je ukupno 12 poglavlja koja obuhvaćaju pregled psiholoških, pravnih i tehničkih aspekata informacijske sigurnosti i zaštite privatnosti i općenito digitalnog svijeta. Osim analize trenutnog stanja te prikaza uzročno-posljedičnih odnosa između ponašanja i rizika od mogućih posljedica, navedene su i preporuke za zaštitu pojedinaca.

Obrađene su teme koje obuhvaćaju područja informacijske sigurnosti i zaštite privatnosti, a koje su posljednjih godina izuzetno aktualne, kako u javnosti tako i u znanstvenim krugovima, zbog sve većih sigurnosnih problema koji se pojavljuju u gotovo svim aspektima ljudskoga života. Upravo je interdisciplinarni pristup, temeljen na analizi ponašanja korisnika raznih informacijsko-komunikacijskih sustava, omogućio sveobuhvatni pristup u ovome udžbeniku.

Prvi sveučilišni udžbenik na temu informacijske sigurnosti nastao je prije godinu dana u sklopu provedbe projekta *Safer Internet Centre Croatia: Making internet a good and safe place*, Agreement Number: INEA/CEF/ICT/A2015/ 1153209: Velki, T. i Šolić, K. (2018). *Priručnik za informacijsku sigurnost i zaštitu privatnosti.* Osijek: Fakultet za odgojne i obrazovne znanosti Sveučilišta J. J. Strossmayera u Osijeku.

Ideja za pisanje *Priručnika za informacijsku sigurnost i zaštitu privatnosti* nastala je prije više godina tijekom razvoja prvih inačica upitnika o rizičnom ponašanju računalnih korisnika. Urednici su tada prvi puta spojili znanja iz različitih područja, informacijske i komunikacijske te bihevioralne znanosti, kako bi se pozabavili pitanjem najslabije karike u lancu informacijske sigurnosti, odnosno ponašanjem računalnoga korisnika. Prvi su rezultati bili poražavajući; ukazivali su da su najveći propusti u informacijskoj sigurnosti nastali neprimjerenim ljudskim ponašanjem te su upućivali na nužnu dodatnu izobrazbu računalnih korisnika iz područja informacijske sigurnosti. Tada se i razvila ideja o pisanju *Priručnika* i pokretanju odgovarajuće sustavne izobrazbe računalnih korisnika.

U manje od godinu dana cijelo je tiskano izdanje *Priručnika za informacijsku sigurnost i zaštitu privatnosti* podijeljeno stručnjacima iz područja informacijske sigurnosti, ali i šire, odgojno-obrazovnim djelatnicima, ustanovama socijalne skrbi,

fakultetima i ostalim zainteresiranim korisnicima informacijsko-komunikacijskh sustava te su dobiveni upiti brojne šire publike za njegovo korištenje. Umjesto ponovnog izdanja postojećeg udžbenika urednici su odlučili napraviti novi, prošireni sveučilišni udžbenik na temu *Izazovi digitalnog svijeta.* Kako se digitalni svijet rapidno mijenja, istodobno mijenja naše poglede na život te utječe na sve aspekte života korisnika informacijsko-komunikacijskih sustava, ove novine i promjene bilo je potrebno obuhvatiti u novom proširenom sveučilišnom udžbeniku.

Novi je udžbenik nastao interdisciplinarnom suradnjom brojnih znanstvenika, a potaknut je brzim i brojnim promjenama koje se odvijaju u digitalnom svijetu. Upravo potaknuti tim promjenama stručnjaci različitih profila dali su svoj pogled na ovu problematiku koja se javlja u današanjem digitalnom dobu. Udžbenik je namijenjen svim korisnicima informacijsko-komunikacijskih sustava koji se u svojem svakodnevnim radu i aktivnostima susreću s raznim problemima digitalnog doba, od proboja informacijske sigurnosti, odnosno otuđenja i krađe digitalnih podatka te njihove zlouporabe, do različitih oblika zlostavljanja novim informacijsko-komunikacijskim tehnologijama.

Urednici

Tena Velki i Krešimir Šolić

1. Uvod

Danas je pojam privatnosti kako na internetu tako i u svakodnevnom životu sveprisutan. Štoviše, danas je internet postao svakodnevni ako ne i najvažniji dio života. Opće je poznato da „ako nije bilo na *faceu*, kao da se nije niti dogodilo!" Međutim, mnogi od nas i danas ne shvaćaju potencijalne opasnosti uporabe interneta, od lažnog predstavljanja tuđim profilima, lažnih obećanja kojima se nudi ili čak traži financijska i druga pomoć do različitih oblika zlostavljanja koja ostavljaju trajne psihološke posljedice na korisnika.

Digitalni svijet, nekada zvan *virtualni* svijet, već je godinama dio realnog, takozvanog *stvarnog* svijeta. Naše ponašanje u digitalnome svijetu ima itekako realne posljedice na stvarni svijet. Razne vrste komunikacija, financijske transakcije, kupovina, informiranje i učenje, razne vrste zabave, sve je to dio naših svakodnevnih aktivnosti koje konzumiramo „u hodu" osobnim ili prijenosnim računalima, pametnim mobitelima, igraćim konzolama, pametnim televizorima ili nekim drugim „pametnim" uređajima koji omogućavaju pristup internetu.

A mi, korisnici raznih informacijsko-komunikacijskih sustava (sustavi koji su svi redom na neki način dio interneta) često se ponašamo vrlo naivno iako smo više puta bili upozoreni na moguće opasnosti. Na primjer, najlakši način da saznate nečiju lozinku jeste da ga jednostavno pitate ili ako je potrebno izvedete neku sitniju prevaru u smislu lažnog predstavljanja telefonom ili lažne suosjećajnosti o bolesnom djetetu iz ratom zahvaćenog područja!

Nacionalno istraživanje na razini Republike Hrvatske o ponašanju korisnika na internetu te znanju o pitanjima sigurnosti i privatnosti (rezultati prikazani u trećem poglavlju ovog udžbenika) pokazalo je visok postotak lakovjernosti te možda ne tako loše znanje, ali sigurnosno izrazito riskantno ponašanje većine korisnika. Možda je najzanimljiviji rezultat kako nam je većina ispitanika tijekom provođenja istraživanja dragovoljno (trik pitanjem o kvaliteti lozinke) odala svoju lozinku!

Naše riskantno ponašanje može dovesti do krađe identiteta, financijske štete, gubitka ugleda, zdravstvenih poteškoća te raznih drugih problema u privatnome životu ili na radnome mjestu. To naravno vrijedi kako za privatne tako i za poslovne korisnike; razlika u šteti samo je u apsolutnim iznosima, ne možda i u relativnim!

Pojavom novih opasnosti na internetu pojavljuju se novi izazovi za njihovo sprječavanje. Inženjeri informacijski tehnologija poboljšavaju postojeće te razvijaju nove tehničke oblike zaštite, no ne postoji potpuna odnosno apsolutna zaštita. Često

je upravo korisnik, odnosno ljudski čimbenik, presudan i najslabiji dio sigurnosti informacijsko-komunikacijskoga računalnoga sustava. Tehnička zaštita pokazala se nedovoljnom te je uz edukaciju korisnika potrebno i pravno regulirati pravila ponašanja te sankcije za prekršitelje.

Intredisciplinarni pristup ovom problemu omogućuje kvalitetnija rješenja, a upravo je ovaj udžbenik jedno od njih. Cilj nam je na temelju pregleda prethodnih istraživanja, kao i na temelju provedenoga nacionalnog istraživanja, dati korisne savjete te konkretne preporuke korisnicima raznih informacijsko-komunikacijskihm sustava u cilju bolje zaštite na internetu!

Prvih pet poglavlja udžbenika analizira ***psihološke aspekte*** sve prisutne digitalizacije. Istraživanjima rizičnih ponašanja korisnika informacijsko-komunikacijskih sustava, povezanostima rizičnog ponašanja s potencijalnim opasnostima te karakteristikama samih korisnika, nastoji se dobiti uvid koje su osobe sklonije rizičnom *online* ponašanju, u kojem uvjetima i iz kojih razloga. Svrha je navedenih poglavlja prikazati koji su najčešći propusti informacijske sigurnosti zabilježeni među računalnim korisnicima, koja su najučestalija i najrizičnija ponašanja računalnih korisnika glede privatnosti i sigurnosti digitalnih podataka, koji se oblici zlostavljanja i nasilja pojavljuju na internetu te koje su opasnosti učestalog igranja *online* računalnih igara. Naglasak je u ovom dijelu knjige na savjetima i preporukama korisnicima računalnih sustava za sigurno korištenje informacijsko-komunikacijskih tehnologija.

Slijede dva poglavlja koja obuhvaćaju ***pravne aspekte*** digitalnog doba. Napredak tehnologije prati i pravni sustav pri čemi je i kriminalitet poprimio nove oblike, a koje Kazneni zakon nastoji suzbijati propisivanjem kaznenih djela i prikladnih sankcija za njih. Detaljno je opisano pravo na zaštitu privatnosti pravnim propisima hrvatskog Kaznenog zakona i europske Opće uredbe (GDPR). Definiraje pravila ponašanja, definiranje prava i obveza sudionika (kako korisnika tako i pravnih subjekata) te definiranje sankcija za prekršitelje neophodan su dio zaštite podataka u informacijsko-komunikacijskim sustavima.

Sljedećih pet poglavlja analizira ***tehničke aspekte*** zaštite objašnjavajući tehničke elemente zaštite informacijsko-komunikacijskih sustava uz pojašnjenja u kojem nas smjeru vodi napredak, na što trebamo obratiti pozornost te koje su potencijalne opasnosti (sve one tehničke zamke koje nam razni zlonamjerni pojedinci na internetu postavljaju). Svrha je ovih poglavlja educirati prosječnog korisnika informacijsko-komunikacijskih računalnih sustava bez dubljeg ulaženja u same tehničke detalje o zaštiti privatnosti te načinima zaraze podataka zloćudnim kodom, kako se kriptiraju podatci te koji su osnovni načini zaštite digitalnih mreža. Ističući specifičnosti zaštite medicinskih podataka, istaknut je i problem lažnih informacija na internetu.

Rezultati naših dosadašnjih istraživanja pokazuju kako je za povećanje informacijske sigurnosti (i zaštitu privatnosti) informacijsko-komunikacijskih sustava neophodno znanje i svijest prosječnog korisnika o potencijalnim opasnostima. Stoga je neophodno educirati korisnike te ih sustavno upozoravati na postojeće i nove opasnosti kako bi ojačali najslabiji dio toga sustava, odnosno čovjeka.

izv. prof. dr. sc. Tena Velki

doc. dr. sc. Krešimir Šolić

PSIHOLOŠKI ASPEKTI DIGITALNOG SVIJETA

doc. dr. sc. Tijana Borovac

Fakultet za odgojne i obrazovne znanosti
Sveučilišta Josipa Jurja Strossmayera u Osijeku

2. PREGLED ISTRAŽIVANJA O INFORMACIJSKOJ SIGURNOSTI

Sažetak

Ubrzan protok informacija i sve veća dostupnost informacija kao posljedica digitalnog doba donijela je za sobom i pitanja o sigurnosti na internetu; koliko smo svjesni važnosti sigurnog korištenja interneta, zaštite osobnih podataka te znamo li uopće kako se zaštiti u slučajevima zlouporabe podataka? U ovome poglavlju dan je pregled istraživanja u svijetu i Republici Hrvatskoj koji nastoji odgovoriti na neka pitanja o sigurnosti na internetu. Poseban je naglasak na istraživanjima i projektima koji su se bavili sigurnošću djece osnovnoškolske i srednjoškolske dobi ali i studenata i odraslih zaposlenih osoba. Na kraju rada dan je pregled organizacija i projekata koji se bave sigurnošću na internetu.

2.1. UVOD

Razvojem digitalnog doba, koje uključuje pojavu društvenih mreža i mobilnih aplikacija (pametni telefoni, društvene mreže, mobilne aplikacije i sl.), ubrzao se protok informacija što je svakako donijelo značajne prilike i koristi današnjem životu, ali su istodobno nove digitalne tehnologije povećale niz socijalnih i etičkih pitanja. Informacijska i komunikacijska tehnologija (IKT) omogućuje prijenos i uporabu svih vrsta informacija i predstavlja najprodorniju generičku tehnologiju današnjice. Pitanja koja su se pojavila odnose se na sigurnost na internetu, uključuju slučajeve zlouporabe IKT-a u obliku neželjenih podataka, krađe podataka, kršenja intelektualnog vlasništva (plagijata i piratstva), delinkvencije, prekomjerne izloženosti igrama na internetu, nasilju na internetu (engl. *cyberbullying*), prijevari, krađi identiteta, pornografiji, trgovini seksom... Prema UNESCO-ovom izvješću (2015) slični problemi pojavljuju se u cijelom svijetu i zabrinjavaju pa je donesena preporuka za aktivnijim istraživanjima digitalnog građanstva, posebno u zemljama u razvoju, kako bi se dobiveni rezultati mogli koristiti u izradi intervencijskih programa koji su prikladni za potrebe svake zemlje. Djeca i mladi prepoznati su kao osobito ranjiva skupina jer često nisu svjesni opasnosti kojima se izlažu kada pristupaju internetu.

Sukladno nastalim promjenama glede sigurnosti na internetu, a time i zaštite osobnih podataka u Republici Hrvatskoj, došlo je do donošenja novog propisa koji osigurava ujednačeno i jednoobrazno postupanje u svim državama članicama EU-a po pitanju zaštite osobnih podataka. Agencija za zaštitu osobnih podataka u Republici Hrvatskoj navodi kako će posljedica donošenja novog propisa biti jednostavnija i jednaka zaštiti prava svih pojedinaca u Europskoj uniji. Europski parlament i Vijeće EU-a postigli su dogovor o novim EU pravilima o zaštiti podataka: Uredba o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (Opća Uredba o zaštiti podataka) stupila je na snagu 24. svibnja 2016., a primjenjuje se izravno u svim državama članicama EU-a od 25. svibnja 2018. U kontekstu navedenoga slijedi kako će djeca moći rabiti određene internetske usluge i servise za koje je potrebno dati osobne podatke isključivo uz roditeljski pristanak (dobna granica bit će između 13 i 16 godina).

2.1.1. PREGLED ZNANSTVENIH ISTRAŽIVANJA O SIGURNOSTI NA INTERNETU

Čini se kako se dobna granica prvog pristupanja internetu spušta diljem Europe. Dob u kojoj se djeca prvi put koriste internetom varira od zemlje do zemlje. Prema Livingston i sur. (2011) prosječna je dob prve upotrebe interneta sedam godina u Danskoj i Švedskoj, a osam u nekim drugim sjevernim zemljama (Nor-

veška, Finska, Nizozemska i Velika Britanija), kao i u Estoniji. Prosječne dobi su više (10 godina) u Grčkoj, Italiji, Turskoj, Cipru, Danskoj, Austriji i Portugalu. Budući da se sve mlađa i mlađa djeca počinju koristiti internetom, internetske sigurnosne kampanje i inicijative moraju biti usmjerene i prilagođene mlađim dobnim skupinama, a istodobno održavati postojeće napore vezane za sigurnost starije djece. U onoj mjeri u kojoj su se dosadašnja nastojanja usredotočila na srednje škole više nego li na osnovne škole, sada je potrebno usmjeriti se na obrazovanje i usavršavanje nastavnika u osnovnim školama.

Livingston i sur. (2011) predstavili su rezultate međunarodne studije EU-a Kids Online koja je provedena 2010. godine u kojoj je sudjelovalo 25 europskih zemalja (Velika Britanija, Grčka, Italija, Španjolska, Slovenija, Finska, Njemačka, Rumunjska, no ne i Republika Hrvatska). U istraživanju je sudjelovalo 25 142 djece u dobi od 9 do 16 godina koja se koriste internetom zajedno s jednim od roditelja. Istraživanje je proučavalo ključne online rizike internetske rizike: gledanje pornografije, nasilničko ponašanje, primanje seksualnih poruka, kontakt s ljudima koji im nisu poznati „licem-u-lice", izvanmrežni sastanci s internetskim kontaktima, potencijalno štetni korisnički sadržaji i zlouporaba osobnih podataka. Livingstone i sur. (2011) u anketi su postavili pitanja djeci o tome koliko često su na internetu te kojim uređajima se koriste kako bi mogli pristupiti internetu. Čak 93 % djece između 9 i 16 godina barem jednom tjedno su na internetu (60 % su na internetu svaki dan ili skoro svaki dan). Većina djece (58 %) još uvijek pristupa internetu preko zajedničkog osobnog računala (PC) iako je pristup vlastitom računalu odmah sljedeći najčešći odgovor (35 %). Gotovo trećina djece (32 %) pristupa internetu spajajući se na televizor, a oko trećine to radi mobilnim telefonom (31 %) dok četvrtina pristupa internetu na igraćim konzolama (26 %). S obzirom da pristup računalom već dugo prevladava kao najpristupačniji i na prvome mjestu, postalo je jasno kako su posljednjih godina i neki drugi načini pristupanja internetu postali sve rasprostranjeniji. Oko četvrtine djece koristi se internetom pomoću osobnog prijenosnog računala (24 %) ili dijeljenog prijenosnog računala (22 %) što odražava rast uporabe prijenosnih računala općenito i omogućuje djeci sve veći pristup internetu. Osim toga, 12 % djece internetu pristupa tabletom ili prijenosnim uređajem (na primjer, iPod Touch, iPhone ili BlackBerry) (Livingstone, 2011).

U Maleziji u 2013. godini u školama se provodio program DigiCyberSAFE u sklopu kojega je provedeno istraživanje u kojemu je sudjelovalo 13 945 učenika u dobi od 7 do 19 godina (učenici osnovnih i srednjih škola) u kojemu su iskazali svoje stavove o cyber sigurnosti, prikladnom ponašanju na internetu i sposobnosti zaštite od rizika DiGi (2014). Rezultati studije bili su od ključne važnosti u razvoju pristupa za unaprjeđenje digitalnog građanstva u Maleziji kao i izgradnji kapaciteta usmjere-

nih na nastavnike, savjetnike i roditelje. Iako više od 80 % sudionika smatra sigurnost na internetu važnom, kada se analiziraju rezultati na koji način djeca to čine, još je uvijek oko 40 % djece koja ne znaju kako se zaštititi na internetu. Usporedbe između dobnih skupina pokazuju da su djeca u dobi od 15 godina ili manje izloženija riziku od onih u dobi od 16 do 19 godina. Istraživanje je pokazalo da se 45 % svih školskih učenika ne osjeća posve sigurno na internetu. Unatoč tomu, 52 % ispitanika kaže da se osjećaju sigurno na internetu. Još 38 % ispitanika nije svjesno da je potrebno poduzeti različite korake kako bi sami sebe zaštitili na internetu DiGi (2014).

Davis i James (2013) suočene s malim brojem istraživanja koja obuhvaćaju stariju djecu osnovnoškolske dobi odlučili su intervjuirati 42 učenika u dobi od 11 do14 godina u okolici Bostona (Sjedinjene Američke Države) te prikupiti i analizirati njihova razmišljanja o sigurnosti na internetu, pitanju privatnosti na društvenim mrežama te kako se nose s tim izazovima. U spomenutom istraživanju odlučili su se za intervju i kvalitativnu metodologiju kako bi dobili što bolji uvid u razmišljanja učenika. Istraživanje su provodili u prostorima njihovih škola gdje su dva puta intervjuirali svako dijete te na taj način ostavljali više vremena za razgovor i bolje upoznavanje sa svakim sudionikom pri čemu su ih pitali o njihovim osobnim definicijama privatnosti te o strategijama kojima se koriste za stvaranje privatnosti na mreži. Rezultati studije ukazuju na to da učenici cijene privatnost, traže privatnost od stranaca i poznatih osoba te provode različite strategije kako bi zaštitili svoju privatnost na mreži. Davis i James (2013) navode kako se gotovo svi sudionici studije (njih 40 ili 95 %) koriste strategijom koja podrazumiijeva zadržavanje sadržaja na internetu. Učenici su rekli kako ne objavljuju određene osobne podatke (kao što su njihova puna imena, adrese i telefonski brojevi) na društvenoj mreži, u porukama i sl. Više od jedne trećine sudionika u istraživanju reklo je kako bi zaštitili svoju privatnost na mreži objavljujući neistinite informacije o sebi. Iako je riječ o malom uzorku i kvalitativnoj metodologiji, autorice su željele ukazati na važnost provođenja sličnih istraživanja za dobivanje što preciznijih i relevantnih informacija.

Istraživanje u Republici Hrvatskoj pokazalo je kako postoji razloga za zabrinutost zbog rizičnog ponašanja učenika na internetu bez obzira na spol ili dob učenika. Cilj je studije bio ispitati problematiku rizičnoga ponašanja računalnih korisnika na srednjoškolskoj populaciji, a autori su podatke prikupljali Upitnikom znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK) prilagođenog za srednjoškolce. Autori su prikupili informacije o rizičnom ponašanju računalnih korisnika i znanju o informacijskoj sigurnosti između 355 učenika iz triju srednjih škola: gimnazija, ekonomska (četverogodišnja srednja škola) i trgovačka škola (trogodišnja srednja škola). Rezultati su pokazali da je postotak učenika srednjih škola koji su otkrili svoju lozinku za pristup sustavu e-pošte izuzetno visok (77,7 %). Učenici

srednjih škola bolje su se procjenjivali na subskalama održavanja osobnog računala i uvjerenja da znaju osigurati računalne podatke, no unatoč tomu iskazivali su na ponašajnim mjerama niz rizičnih ponašanja koja se odnose na informacijsku sigurnost (npr. posuđivanje pristupnih podataka –zaporki, nezaštićena komunikacija i/ili komunikacija s nepoznatim osobama na internetu i sl.). Osim toga, postoji relativno visok postotak učenika koji su bili cyber-žrtve kao i određeni postotak učenika koji su bili cyber-nasilni (Velki i sur., 2017). Prema Velki i sur. (2017) dobiveni rezultati istraživanja trebali bi upozoriti državne institucije i nastavnike u školama i potaknuti na razvoj učinkovitijih obrazovnih programa i programa prevencije s ciljem povećanja sigurnoga ponašanja kada se radi o internetskoj i informacijskoj sigurnosti i zaštiti privatnosti.

Uloga digitalnog građanstva u obrazovnom sustavu je pružiti sredstvo koje pomaže učenicima razumjeti kako se tehnologija upotrebljava na siguran i prikladan način. Neke od ključnih vještina koje učenici trebaju imati za učinkovito kretanje digitalnim svijetom podrazumijevaju: pronalaženje pouzdanih informacija na internetu, otkrivanje sumnjivog sadržaja, poznavanje pravila o privatnosti s prikupljenim informacijama na mreži i iskorištavanja tehnologije koju nude sudjelovanjem na odgovoran način s drugima širom svijeta (Hui i Campbell, 2018). Slično tomu govori i Thierer (2009) koji kaže da sam fokus na sigurnost djece nije dovoljan. Djeca moraju naučiti kako smanjiti rizike, ali i naučiti odgovorno i etično ponašati se u digitalnom svijetu. Osim toga, trebaju razumjeti medijsku pismenost kako bi mogli kritički razmišljati o sadržajima koje konzumiraju i sve više stvaraju. Stoga najbolje prakse moraju nastojati osigurati zabavna, obrazovna i sigurna iskustva za djecu.

2.1.1.1. Pregled istraživanja o sigurnosti studenata na internetu

Vještine i sklonosti korištenja informacijsko-komunikacijske tehnologije rezultat su odrastanja u tehnološki zasićenome okruženju u kojem tehnološke naprave, računala, mobiteli, tableti, postaju sastavni dio života. Zbog toga se mlađe generacije razlikuju od starijih ne samo prema sklonostima i stavovima već i prema načinu procesuiranja informacija i učenja pa se sve češće susrećemo s terminima kao što su cyber-djeca, digitalni urođenici, Google generacija… Navedeni pojmovi oblikuju diskurs o mladima i njihovoj uporabi računala. Lasić-Lazić, Špiranec, Banek i Zorica (2012, str. 126) navode kako se novi diskurs temelji „na predodžbi o iznimnim vještinama mladih u uporabi tehnologija i pretpostavci da će se one automatizmom uspješno i pozitivno odraziti na procese učenja, no rezultati istraživanja o informacijskim navikama, interakcijama i načinima procesuiranja informacija pokazuju da se radi o horizontalnim ili površnim interakcijama koje su usmjerene na kvantitetu podataka umjesto na njihovo kvalitetno tumačenje i kritičko razmatranje koji su

pretpostavka za dubinsko, smisleno i istinsko učenje." Shodno tomu, postavlja se i pitanje sigurnosti jer sadašnji su digitalni urođenici već na fakultetima i ušli su u visokoobrazovni sustav.

Kim (2014) je utvrdio kako su neki studenti svjesni sigurnosnih problema i razumiju da bi trebali biti oprezniji zbog svoje vlastite sigurnosti, ali nisu ustrajni u provođenju sigurnosnih mjera predostrožnosti uporabe interneta. Do navedenih rezultat Kim (2014) je došao istražujući osviještenost o važnosti informacijske sigurnosti među studentima kako bi na temelju toga razvijali učinkovitu edukaciju o važnosti sigurnosti uporabe informacija (ISAT). U navedenom istraživanju došli su do rezultata kako studenti razumiju važnost i potrebu za takvom vrstom edukacije kao što je ISAT, ali mnogi od njih ne sudjeluju u tome. Teer, Kruck i Kruck (2007) ispitivali su računalnu sigurnost prakse studenata preddiplomskih studija i zaključili da „studenti ostavljaju svoja osobna računala ranjiva na viruse." Lomo-David, Shannon i Ejimakor (2009) ispitivali su studente (867 studenata različitih smjerova i razina – preddiplomska i diplomska razina studija) o poznavanju i uporabi sigurnosnih mjera na internetu. Pod sigurnosnim mjerama mislilo se na uporabu jednostavnih zaporki, sofisticiranih zaporki (sastoje se od kombinacije velikih i malih slova, brojeva te znakova), zaporki u privitku e-pošte, svakodnevno skeniranje računala, korištenje antivirusnih softvera, biometrijske identifikacije, sustava za otkrivanje upada i višenamjenskih sustava provjere autentičnosti. Što se tiče uporabe zaporki, 69 % sudionika upoznato je s primjenom jednostavnih zaporki ili ih svjesno koristi. Na pitanje koliko često rabe jednostavne lozinke, 64 % studenata navodi kako ih rabi više od 50 % vremena, što u tom slučaju i nije tako impresivno s obzirom da je čak i jednostavna lozinka neophodna kako bi neki podatci bili sigurni i održali integritet sustava. Što se tiče sofisticiranih zaporki, čak 87 % sudionika nije upoznato s takvim načinom zaštite i načinom na koji se formiraju pa je pretpostavka da ih zato i manje koriste, a na pitanje koliko se često koriste sofisticiranim zaporkama, njih 90 % se koristi manje od 3 % vremena. U tom slučaju nepoznavanje uporabe sofisticiranih zaporki može se tumačiti kao ne-uporaba, što je razumljivo jer poznavanje mora prethoditi upotrebi. Autori Lomo-David i suradnici (2009) u skladu s dobivenim rezultatima preporučuju obrazovnim institucijama da bi trebale još više informirati studente o uporabi sigurnosnih mjera na računalima. Mensch i Wilkie (2011) uspoređivali su sigurnosne prakse studenata s obzirom na spol, dob, socioekonomski status, a ispitani su stavovi studenata glede upravljanja zaporkama za za račune na internetu, instalaciji i uporabi antivirusnog softvera, instalaciji i uporabi antispam softvera, otvaranju veza unutar e-pošte ili izravnih poruka, korištenja bežičnog računalstva, krađa identiteta itd. Studentima preddiplomskog i diplomskog studija ponuđena je mogućnost sudjelovanja u istraživanju a od njih 2000 u istraživanju je pristalo sudjelovati 127 studenata. Sudionici su u e-pošti dobili poveznicu i popunjavali anketu na internetu. Najviše

sigurnosnih ponašanja u odnosu na dob pokazuju najmlađi sudionici, od 18 do 23 godine (M = 85,97), dok najmanje sigurnosnog ponašanja iskazuju stariji studenti, od 24 do 30 godina (M = 79,94). Većina sudionika nije bila žrtva krađe identiteta (85,8 %), imaju instaliran antivirusni softver (80,3 %), kao i instaliran antispywarwe na svojim računalima (74,8 %). Međutim, 70,9 % sudionika gotovo nikada ili nikada ne pokreće antivirusni softver na USB memorijskim uređajima, a samo 11 % to čini uvijek ili većinu vremena. Kada je riječ o informacijskoj sigurnosti, Mensch i Wilkie (2011) smatraju kako bez obzira na postojanje sve sofisticiranijih tehnoloških rješenja, krajnji korisnik mora naučiti prihvatiti odgovornost i poduzeti proaktivne mjere kako bi ostao educiran o dostupnim sigurnosnim alatima i procedurama za zaštitu osobnih podataka i informacija na mrežnim i izvanmrežnim mjestima.

Siponen (2000) smatra kako sadašnji pristupi u pogledu informacijske sigurnosti i obrazovanja nisu orijentirani na dostignuće niti prepoznavanje činjenica, a trenutne studije ne istražuju mogućnosti koje nude teorije motivacije i ponašanja. Prva pretpostavka, razina deskriptivnosti, smatra se upitnom jer na kraju može dokazati da krajnji korisnici ne uspijevaju internalizirati zadane ciljeve i, primjerice, ne slijede sigurnosne smjernice – što je neprimjereno. Autor Siponen (2000) smatra kako se uloga motivacije u području informacijske sigurnosti ne smatra dovoljno ozbiljnom iako je njezina uloga široko priznata.

U istraživanju koje su provodili Er i sur. (2017) sudjelovali su studenti privatnog sveučilišta u dobi od 19 do 24 godine. Cilj je bio odrediti osviještenost ispitanika o pitanjima sigurnosti na internetu i njihovoj sposobnosti da se zaštite od rizika na internetu. U istraživanju su se koristile i kvalitativne i kvantitativne metode istraživanja. Anketni upitnik upotrebljen je kako bi se utvrdila osviještenost i razumijevanje problema sigurnosti na internetu i sposobnost zaštite od rizika. Intervju fokusnih skupina upotrebljen je za ispitivanje percepcije i iskustva studenata o rizičnim aktivnostima na internetu. Rezultati pokazuju sljedeće: (i) studenti su se osjećali prilično sigurno kada su bili na internetu; (ii) imaju dobro razumijevanje onoga što predstavlja rizične online aktivnosti; (iii) studenti također znaju kako se zaštititi tijekom korištenja interneta; (iv) unatoč tomu, još uvijek prepoznaju važnost učenja o sigurnosti na internetu. Navedeno istraživanje dio je kontinuiranog niza istraživanja na različitim područjima kojima je cilj identificirati razinu svijesti o sigurnoj i odgovornoj uporabi IKT-a.

Istraživanje Robertsona i suradnika (2001) obuhvatilo je studente druge godine studija (16 studenata) te srednjoškolce (15 maturanata). Dob za srednjoškolsku grupu kretala se od 17 do 18 godina, a za sveučilišnu skupinu od 18 do 42 godine te osam studenata u dobi iznad 30 godina. Ukupni uzorak (N=31) obuhvaćao je šesnaest muškaraca i petnaest žena. Svi su studenti imali račune e-pošte, a većina je imala kućna

računala iako ne uvijek i internetsku vezu. Kada su im postavljena pitanja koja se odnose na osobnu sigurnost, ponovno su istaknute neke jasne razlike između sudionika istraživanja – maturanata i studenata. Kada se pitaju o osobnoj sigurnosti, studenti vide svojevrsne opasnosti i znaju da potpuna anonimnost u konačnici nije moguća. Nasuprot tomu, čini se da maturanti tako ne razmišljaju.

Hall (2012) je pokušao utvrditi kakva je percepcija studenata o važnosti očuvanja osobnih podataka i njezina digitalna dostupnost. U istraživanju su sudjelovali studenti informatike koji su već imali neke nastavne predmete kao što su društvene mreže, mediji, nove tehnologije i sl. dok je druga grupa studenata bila „netehničarska", odnosno obuhvatila je studente kriminologije koji nisu imali toliko nastavnih predmeta iz područja informatike. Rezultati do kojih je Hall (2012) došao pokazuju kako se 57 % studenata ne brine ili se malo brine zbog osobnih podataka dostupnih na internetu, dok je 50 % spremno ostaviti računala „prijavljena" duže vrijeme. No, 90 % koristi se nekim oblikom privatnosti, a 56 % ne upotrebljava javna računala iz osobnih razloga. „Netehničarska" skupina studenata bila je još manje zabrinuta zbog dostupnosti informacija, ali je više pazila kada bi prestajala raditi na računalu. Iako studenti uglavnom nisu zabrinuti ako su njihovi osobni podatci digitalno dostupni, vode brigu da ih ipak na neki način mogu kontrolirati. Podatci upućuju da su studenti samo djelomice svjesni kako postoji potencijalna opasnost od zlouporabe ili neetičnih akcija temeljenih na njihovim digitalnim informacijama. Pretpostavka je da bi ti brojevi bili vrlo različiti kada bi se više njih osobno ili profesionalno „opeklo" zbog zlouporabe svojih digitalnih informacija ili ako bi točno znali koje su informacije dostupne. Osobito ako 50 % njih ostavlja račune aktivnima (ne odjavi se), a koristi se javnin računalima za osobne potrebe.

Istraživanja među studentima u Republici Hrvatskoj provedena su također s ciljem utvrđivanja njihovih stavova i mišljenja o sigurnosti na internetu, mogućim opasnostima, zlouporabi te zaštiti identiteta. Vrana (2013) je u svom radu prikazao rezultate istraživanja studenata Filozofskog fakulteta u Zagrebu, njihova stajališta i mišljenja o sigurnoj uporabi društvenih mreža. Istraživanje je provedeno u ožujku 2013. godine s ukupno 197 studenata koji su dobrovoljno sudjelovali u istraživanju. Iako se može reći da je broj studenata možda nedovoljan, još uvijek ukazuje na neke važne trendove korištenja interneta u cjelini i na mrežnim društvenim mrežama. Rezultati pokazuju da je većina sudionika iskusnih korisnika društvenih mreža, međutim, rijetko mijenjaju zaporke u mrežnim profilima, a većina njih nikada nije imala nikakvo obrazovanje općenito o sigurnosti na internetu i načinu zaštite osobnih podataka na društvenim mrežama. Srećom, većina njih nikada se nije susrela s provalama na svojim profilima na društvenim mrežama. Općenito govoreći, studenti su vrlo zainteresirani za uporabu mrežnih društvenih mreža i čini se da ih ništa neće

spriječiti da tako nastave u budućnosti. Međutim, trebali bi uložiti više vremena u obrazovanje o sigurnoj upotrebi društvenih mreža i primijeniti zdrav razum pri prihvaćanju sadržaja drugih ljudi koji su im poznati i onih koji se pretvaraju da su njihovi prijatelji kako bi se zaštitili. Buduća istraživanja mogu obuhvaćati druge skupine čestih korisnika mrežnih društvenih mreža kako bi se istražilo postoji li isti obrazac uporabe mrežnih društvenih mreža kao kod studenta Filozofskog fakulteta u Zagrebu.

Autori Velki, Šolić i Očevćić (2014) željeli su razviti Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK). Razvoj upitnika sastojao se od odabira prikladnih čestica za koje se pretpostavlja da mjere razinu znanja o informacijskoj sigurnosti te rizična ponašanja računalnih korisnika. Upitnik se sastojao od dva dijela s ukupno 37 čestica. Sudionici te studije bili su studenti (N=135) druge godine preddiplomskog studija s triju različitih fakulteta Sveučilišta J. J Strossmayera u Osijeku. Dobiveni rezultati optimistični su jer upitnik UZPK-a ima potencijal postati priznat i pouzdan upitnik za mjerenje svjesnosti o sigurnosti informacijskih korisnika. U svakom slučaju, IT stručnjaci moći će analizirati korisnike informacijskih sustava kako bi se uočili problemi s niskom razinom sigurnosti, a znanstvenici će moći općenito kategorizirati korisnike informacijskih sustava u pogledu razine svijesti o njihovoj informacijskoj sigurnosti. Analizom dovoljno uzoraka svih vrsta korisnika informacijskih sustava trebalo bi biti moguće dobiti neke opće zaključke o potencijalno rizičnom ponašanju korisnika, korelaciji s razinom sigurnosti i identifikacijom većine nesigurnih vrsta korisnika. Kranji je cilj autora razvoj validirane međunarodne verzije UZPK-a koja je, između ostaloga, omogućila i primjenu upitnika za mjerenje svjesnosti o sigurnosti zaposlenika prilikom korištenja IKT-a na poslu, o čemu će biti riječi u sljedećem poglavlju.

2.1.1.2. Pregled istraživanja o sigurnosti zaposlenika na internetu

Pitanja s kojima se susreće veliki broj poduzeća u svijetu pitanje je zaštite povjerljivosti, integriteta i dostupnosti informacija. Upotrebom novih tehnologija postoje novi informacijski rizici koji mogu dovesti do „curenja" podataka, poteškoća u kontinuitetu poslovanja, reputacijski rizici kroz gubitak vrijedne intelektualne imovine, povjerenje potrošača i konkurentske prednosti.

Hagen i Albrechtsen (2009) u svom su radu nastojali mjeriti i raspraviti učinke alata za e-učenje s ciljem poboljšanja znanja, svijesti i ponašanja zaposlenika o informacijskoj sigurnosti. Pomoću eksperimenta procjenjivali su se stavovi zaposlenika prije i nakon intervencije. Ukupno 1897 djelatnika odgovorilo je na anketu prije i nakon intervencije. Uzorak je podijeljen na intervencijsku i kontrolnu skupinu pri

čemu je jedina razlika između tih dviju skupina bila sudjelovanje u intervenciji (tj. korištenje alata za e-učenje). Rezultati istraživanja ukazuju na značajna kratkotrajna poboljšanja u znanju i ponašanju članova eksperimentalne skupine. Studija je utvrdila kako softver koji podržava programe informiranja o sigurnosti informacija ima kratkotrajni učinak na znanje, ponašanje i svijest zaposlenika. Rad je inovativan u području istraživanja informacijske sigurnosti jer pokazuje kako se mogu mjeriti učinci intervencije na informacijsku sigurnost.

Pojam koji se vrlo često povezuje u istraživanjima o sigurnosti zaposlenika na internetu je socijalni inženjering koji podrazumijeva manipuliranje ljudima u svrhu otkrivanja povjerljivih informacija ili pristupa resursima do kojih manipulator ne može doći sam. Autori Wilcox, Bhattacharya i Islam (2014), proučavajući utjecaj socijalnog inženjeringa na ugled tvrtki, naglašavaju kako socijalni inženjering napada najslabiju organizacijsku sigurnosnu vezu – čovjeka. Sve je veći broj zaposlenika koji rabe društvene medije u radnom okruženju što stavlja stručnjake za informacijsku sigurnost pred velike izazove. Brojne su studije (Gross i Acquisti, 2005; Meister i Willyerd, 2010; Furnell, 2008; prema Wilcox i sur., 2014) pokazale kako postoji rastuća povezanost socijalnog inženjeringa i društvenih medijskih stranica, kao što su Facebook i Twitter, zbog bogatstva osobnih i organizacijskih informacija koja se nalaze u tim okruženjima. Ti izazovi također pokazuju izuzetno velik utjecaj na povjerljivost, integritet i dostupnost informacijske imovine koja se nalazi unutar organizacije. Wilcox i sur. (2014) u istraživanju su željeli prikazati dubinski uvid u klasifikaciju i načine smanjivanja socijalno inženjerskih sigurnosnih pitanja s kojima se suočavaju tvrtke kod korištenja društvenih medija za poslovnu uporabu. Autori smatraju kako su zaposlenici ključni za reputaciju organizacije, ali ako objavljuju neprikladne ili netočne komentare, osobito ako su u suprotnosti s korporativnom porukom kompanije, oni također mogu uzrokovati štetu s ogromnim posljedicama po ugledu tvrtke. Drugo gledište koje se odnosi na gubitak ugleda koji bi se mogao pojaviti izvan službenih ili profesionalnih računa jest šteta koju uzrokuje forumska aktivnost u kojoj potrošači govore o sviđanju ili ne sviđanju određenoga poduzeća. Wilcox i sur. (2014) smatraju kako je najučinkovitija sigurnosna mjera protiv socijalnog inženjeringa povećati svijest zaposlenika o mnogim trikovima kojima se socijalni inženjeri koriste protiv njih na radnome mjestu.

U pregledu istraživanja koja se odnose na ponašanje zaposlenika o pitanju sigurnosti informacijskih sustava u zadnjem desetljeću Lebek i sur. (2014) analizirali su 113 publikacija i smatraju kako bi se buduće empirijske studije trebale usredotočiti na dodatne čimbenike koji utječu na svijest o informacijskoj sigurnosti zaposlenika i njihovo ponašanje. Iako je prisutna dominantnost kvantitativnih istraživanja, Lebek i sur. (2014) mišljenja su kako nedostaju kvalitativna istraživanja u vidu

akcijskih istraživanja i intervjua što može dodati vrijednost ovome istraživačkom polju sigurnosti.

Istraživanja koja se bave sigurnošću zaposlenika na internetu nisu vrlo česta u Republici Hrvatskoj međutim Velki, Šolić i Nenadić (2015) razvili su valjan i pouzdan instrument koji mjeri utjecaj korisnika na sigurnost informacijskoga sustava – Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK; Velki i Šolić, 2014; prema Velki, Šolić i Očević, 2014). Istraživanje je provedeno u tri navrata prikupljanja podataka. Prvi se uzorak sastojao od 135 studenata druge godine preddiplomskoga studija na kojemu je provjerena konstruktna valjanost, pouzdanost i osjetljivost pojedinih subskala te odabrane odgovarajuće čestice. Drugi se uzorak sastojao od 211 studenata i zaposlenika, a na njemu su provjerene metrijske karakteristike poboljšanog instrumenta te je dobivena konačna inačica. Treći se uzorak sastajao od 152 zaposlenika i na njemu je validiran UZPK. Autori Velki, Šolić i Nenadić (2015) došli su do zaključka kako studenti, u odnosu na zaposlenike, statistički značajno češće brinu o održavanju računalnih sustava, što je i očekivano jer se radi o studentima Elektrotehničkoga fakulteta kojima je to sastavni dio obrazovanja. Sukladno očekivanom, zaposlenici procjenjuju komunikaciju računalom manje sigurnom za razliku od studenata koji se za komunikaciju na računalu vjerojatno odlučuju u različite svrhe (npr. za upoznavanje, druženje, razmjenu informacija i sl.) i ne uzimaju u obzir sve potencijalne opasnosti, već su usmjereni na prednosti elektroničke komunikacije. Također je moguće da imaju i dodatna znanja kako zaštiti svoj računalni sustav pa stoga tu vrstu komunikacije smatraju sigurnijom. Na trećem je uzorku zaposlenika dobivena i jedna statistički značajna razlika između muškaraca i žena. Muškarci, za razliku od žena, smatraju da je komunikacija računalom sigurnija. Moguće da je dobivena razlika odraz društva u kojemu živimo, ali i stvarnih situacija u kojima su žene češće žrtve zlouporabe i internetskoga nasilja (West, 2014, prema Velki i sur., 2015) pa ne iznenađuje da one procjenjuju internetsku komunikaciju manje sigurnom. Dobivena je dobra konstruktna valjanost UZPK-a, sve skale i subskale imaju zadovoljavajuće metrijske karakteristike (pouzdanost i osjetljivost) te je dobivena i dobra kriterijska valjanost tako da se može reći kako UZPK predstavlja valjan i pouzdan mjerni instrument zadovoljavajućih psihometrijskih karakteristika.

Nadalje, u Republici Hrvatskoj povodom „Europskog mjeseca kibernetičke sigurnosti 2017" predstavljeno je redovno godišnje istraživanje Hrvatske udruge banaka o stanju sigurnosti na internetu. Anketa provedena na uzorku od tisuću ljudi iz cijele Republike Hrvatske, a s namjerom da se utvrdi stupanj osjećaja ugroženosti i razinu osviještenosti kod građana o potrebi sigurnosne zaštite tijekom obavljanja uobičajenih aktivnosti na internetu, s posebnom naglaskom na preuzimanje internetskoga sadržaja mobitelom. Riječ je o aktivnostima kao što su uporaba e-pošte,

komunikacija društvenim medijima, pristup internetu besplatnim, nezaštićenim bežičnim (engl. *WiFi*) mrežama, samozaštita pri obavljanju transakcija mobilnim bankarstvom, paze li koje stranice posjećuju na internetu i preuzimaju li aplikacije za mobitel samo s regularnih trgovina (App Store, Google Play) ili nepotrebno riskiraju negdje drugdje.

2.2. PRIVATNOST I OSOBNI PODACI NA INTERNETU

Odrasle osobe su one koje određuju koliko će dijete imati pristup digitalnim alatima i kako su njegovi osobni podatci zaštićeni. Zaštita osobnih podataka u Republici Hrvatskoj te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj uređuje se Zakonom o zaštiti osobnih podataka („Narodne novine", broj 103/03, 118/06, 41/08, 130/11, 106/12 – pročišćeni tekst). Svrha je zaštite osobnih podataka zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Zaštita osobnih podataka u Republici Hrvatskoj osigurana je svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište te neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili drugim osobinama.

Zakonom o zaštiti osobnih podataka osnovana je Agencija za zaštitu osobnih podataka kao samostalno i neovisno tijelo s temeljnom zadaćom provedbe nadzora nad obradom osobnih podataka u Republici Hrvatskoj.

2.2.1. KAKO POVEĆATI SIGURNOST PRI UPOTREBI MOBILNIH UREĐAJA?

Posljednjih godina neki oblici IKT-a, poput mobilnih telefona, postali su pristupačni svima i danas omogućuju lak pristup informacijama, ljudima, uslugama i dobrima. Townsend (2010) navodi kako je širenje mobilne telefonije među najbržim inovacijama. Slično računalima, tabletima i mobitelima lako se mogu zamijeniti i trebaju biti osigurani kako bi jamčili sigurnost pojedincu i ustanovi.

Prema podatcima Međunarodne telekomunikacijske unije (2017) do kraja 2017. godine bilo je gotovo 7 milijardi mobilnih telefonskih pretplata na globalnoj razini, s oko 4,5 milijardi jedinstvenih pretplatnika i oko 3 milijarde ljudi (40 % svjetske populacije) imalo je pristup internetu mobilnim i/ili fiksnim širokopojasnim pretplatama (International Telecommunication Union, 2017).

Beth i sur. (2014) proveli su istraživanje na jednom sveučilištu u SAD-u u kojem je sudjelovalo 500 studenata ekonomije. U radu se opisuje istraživanje o stupnju sigur-

nosti koju studenti prakticiraju prilikom uporabe pametnih telefona. Cilj navedenoga istraživanja bio je dobiti uvid u ključna motrišta studentskog ponašanja pri uporabi mobilnih tehnologija. Dok se studenti često oslanjaju na više vrsta mobilnih uređaja, opseg istraživanja bio je ograničen na uporabu pametnih telefona. Rezultati ankete pokazuju veliku razliku u praksi među studentima. Dok se dio studenata bavi nekim motrištima sigurnosti pametnih telefona, i dalje ostaju ranjivi na napad: 44 % nije bilo suglasno da je uporaba zaporke važna, manje od trećine odjavljuje se sa e-pošte i društvenih mreža kada ih ne koriste, oko polovice ispitanika nije bilo neodlučno otvoriti privitak iz nepoznatog izvora, samo 40 % ograničilo je svoje (engl. *WiFi*) aktivnosti na zaštićene mreže.

Slično kao u svijetu i u Republici Hrvatskoj velik je porast preuzimanja internetskoga sadržaja mobitelom. Mobitel postaje sve traženija platforma pa tako i u bankarstvu; u Hrvatskoj bilježimo oko 600 000 korisnika mobilnog bankarstva, istaknuo je predstavljajući istraživanje direktor Hrvatske udruge banaka Zdenko Adrović i naglasio: „U digitalnom dobu, u koje postupno i neupitno ulazimo, sigurna zaštita podataka i komunikacije postaju sve važnije za građane i tvrtke, a posebno za financijski sektor čije se poslovanje svodi na povjerenje koje klijenti imaju u banke. Zato će zaštita i edukacija o kibernetičkoj sigurnosti za nas ostati prioritet."

Na koji način povećati sigurnost pri uporabi mobilnih telefona navodimo preporuku koju su dali Internet Crime Complaint Center (IC3) u suradnji s Federalnim zavodom za istrage (FBI) i National White Collar Crime Center (NWCCC), (IC3, 2012) (prema Beth i sur., 2014):

- ✓ isključiti značajke koje nisu potrebne; koristiti šifriranje (ako je dostupno) za zaštitu osobnih podataka
- ✓ pogledati recenzije razvojnog programera / tvrtke koja je objavila aplikaciju
- ✓ pregledati i razumjeti dozvole koje dajemo prilikom preuzimanja aplikacija
- ✓ koristiti zaštitu lozinkom
- ✓ dobiti zaštitu od zlonamjernog softvera
- ✓ imati na umu aplikacije koje omogućuju geografsku lokaciju
- ✓ ne zatvarati *jailbreak* (*jailbreak* ili *rooting* koristi se za uklanjanje određenih ograničenja proizvođača uređaja ili mobilnog telefona)
- ✓ ne povezivati se s nepoznatim bežičnim mrežama
- ✓ obrisati sve na uređaju (resetirati ga na tvorničke postavke) prilikom prodaje ili mijenjanja
- ✓ koristiti ažuriranja
- ✓ izbjegavati otvaranje softvera ili poveznica iz nepoznatih izvora

- ✓ upotrijebiti iste mjere opreza na mobilnom telefonu kao i na računalu prilikom uporabe interneta.

U Republici Hrvatskoj prema *Izvješću Hrvatske udruge banaka o stanju sigurnosti na Internetu za 2016. godinu* (2017) u slučajevima kada se susretnu s porukom (e-pošta, SMS) nepoznatog pošiljatelja, koja ih navodi na primamljivu ponudu i nosi u sebi poveznicu prema nekom mrežnom odredištu, 93 % ljudi takvu će poruku ignorirati i odmah obrisati, a preostalih 7 % riskirat će i na neki način nastaviti baviti se tom porukom. Što se tiče besplatnog, nezaštićenog, bežičnog pristupa internetu (engl. *WiFi*) čak 37 % ljudi se njime koristi kad god može, 31 % koristi SE bežičnim mrežama povremeno, a 32 % uopće se ne koristi besplatnim bežičnim pristupom internetu. Oni koji se koriste bežičnim internetom, koriste se uglavnom kao metodom štednje – smanjenja troška prijenosa podataka na mobilnoj mreži koju koriste. Na tim mrežama rade ono što i inače rade kad su na internetu: čitaju vijesti, komuniciraju e-poštom i druže se na društvenim mrežama. Dobra je vijest da među onima koji se bežičnim internetom (engl. *WiFi*) koriste bilo često ili samo povremeno ima samo 3 % onih koji putem tih nezaštićenih otvorenih veza pristupaju mobilnom bankarstvu.

Sudionici istraživanja, iako među njima ima još uvijek previše neopreznih, pokazali su dosta opreza pri pregledavanju internetskoga sadržaja koji ih zanimaju na mreži nad mrežama. Njih 55 % ne otvara internetske stranice za koje nisu sigurni da su autentične, međutim čak 34 % sudionika ankete o pouzdanosti mrežnih odredišta koje posjećuju uopće nije razmišljalo. Većini je najvažnije da su sadržaji koji ih zanimaju lako i jednostavno dostupni na mobitelu. Što se tiče preuzimanja aplikacija, 56 % sudionika preuzima aplikacije samo trgovinom koje ponudi mobitel, no njih 34 % uopće ne preuzima nikakve aplikacije na mobitele.

2.2.2. SIGURNOST I ZAŠTITA KORISNIČKOG IMENA I ZAPORKE

Ovisno o društvenoj mreži, e-pošti kojom se koristite ili bilo kojom stranicom koja zahtijeva upotrebu korisničkog imena i zaporke, važno je da one budu dobro odabrane kako biste spriječili da se netko drugi koristi vašim korisničkim profilom. Odabir kvalitetne sigurnosne zaporke ponekad nije jednostavan, stoga donosimo savjete kako odabrati najbolju.

Kad je u pitanju uporaba zaporki pri komunikaciji e-poštom ili na društvenim mrežama, u Republici Hrvatskoj prema Izvješću Hrvatske udruge banaka o stanju sigurnosti na internetu za 2016. godinu (2017), 59 % sudionika zaporke mijenja jednom godišnje ili rjeđe, a 34 % samo kada zaborave staru zaporku. Uz to, znatno je manji broj ljudi koji redovito mijenjaju zaporku – sa 16 % u svibnju 2016. na samo 7 % u rujnu 2016.

Laka pamtljivost zaporka – pobrinite se da je zaporka nešto što možete zapamtiti. Najbolje je odabrati nešto specifično kako biste to uvijek imali na umu, ali opet ne toliko preočito da je može svatko pogoditi. Odaberite neki vama pamtljiv dugačak izraz ili izreku te zaporku kreirajte od cijeloga izraza ili samo od njegovih prvih slova. Primjerice, preuzimanjem početnih slova svake riječi poslovice „Tko rano rani dvije sreće grabi" dobijete „trrdsg" te tome dodajte poneko veliko slovo i broj te vaša zaporka može biti "tRr7DsG".

U istraživanju Sharples i sur. (2009) zamolili su sudionike da predlože zaporku od najmanje šest znakova koje nisu prije upotrebljavali, ali za koje misle da se mogu sjetiti za pristup tom istraživanju. Izbor zaporke ukazuje na koji način sudionici pristupaju sigurnosti na internetu. Polovica sudionika dala je zaporku temeljenu na osobnim podacima kao što su datum rođenja ili ime člana obitelji koji se može naći iz osobnih evidencija. Daljnjih 25 % koristilo je zaporku koja se može naći u rječniku. To ukazuje na zabrinjavajući nedostatak sigurnosti (iako nema dokaza da su njihovi rezultati lošiji od odrasle populacije) ipak postoji jasna potreba da se pomogne djeci razumjeti rizike nesigurnih zaporki i kako ih spriječiti.

Jednostavnost zaporke – izbjegavajte jednostavne zaporke poput „123456", „abcdefg" i slično ili bilo koju riječ sadržanu u nekom od „rječnika zaporki". Naime, postoje liste riječi za koje hakeri znaju da se često koriste kao lozinke poput raznih pojmova iz astrologije, biologije, crtanih filmova, sporta, filmova, mjesta, znanstvene fantastike i slično.

Korištenje iste zaporke – ne koristiti istu zaporku za sve postojeće račune. Poznat je primjer lažnih servisa za dijeljenje podataka koji su postavljeni samo u svrhu upada u račune korisnika. Slični servisi traže registraciju korisnika u nadi da će upisati istu zaporku, a koja će se onda moći iskoristiti za pristup njihovim podacima.

Zapisivanje zaporke – zaporke su inače vrlo kratke te njihova duljina obično iznosi minimalno šest znakova. Ukoliko niste sigurni da ćete ih ipak sve zapamtiti, zapišite ih negdje gdje nitko drugi nema pristup. Zapis u računalu ipak nije najbolji odabir, posebice zbog mogućnosti njegova tehničkoga kvara. Najbolje je zapisati lozinku u neku bilježnicu koju držite na mjestu zajedno s vašim važnijim dokumentima.

Kad je u pitanju čuvanje zaporke kojima se pristupa uslugama mobilnog bankarstva, prema Izvješću Hrvatskih banaka 52 % sudionika ankete tvrdi da te podatke znaju samo oni i da ih nemaju nigdje pohranjene, a 29 % ih o tome ne razmišlja. U odgovoru na ovo pitanje pokazale su se statistički značajne razlike prema dobi. Mlađi korisnici bolje čuvaju zaporke za mobilno bankarstvo od starijih. Štoviše, stariji korisnici te zaporke zapisuju na više mjesta (Hrvatske udruga banaka, 2017).

Kombinacije na tipkovnici – ne koristiti kombinacije na tipkovnici poput „asqw12“, „yxasqw“, i slično ili neke uobičajene zaporke uz tipku „shift“, poput primjerice zaporku „!"#$%&/" koja možda djeluje sigurno, ali je zapravo riječ o znakovlju „shift + 1234567“, što većina rječnika koji se koriste za otkrivanje lozinki sadržava u sebi.

Kombinacija veličine slovaa – kod sustava koji prepoznaju razliku između velikih i malih slova, koristite obje veličine slova u kreiranju zaporke. Čak i ako se odabere jednostavan pojam za zaporku, raznovrsnost veličine znakova znatno će otežati pristup nekome tko želi ući u vaše korisničke račune.

Vlastiti algoritam – koristite vlastiti „algoritam“ za kreiranje zaporke. Primjerice, odabrati prva četiri znaka iz imena stranice na koju se registrirate i dodati zadnje četiri znamenke broja telefona nekog prijatelja. Navedeni algoritam može se dodatno razraditi tako da se od svakog slova odabere sljedeće ili prethodno slovo u abecedi, kombiniranjem velikih i malih slova i slično. Također, može se uvrstiti neko veliko slovo, i to najbolje negdje u sredini riječi, a ne na početku (npr. stoLica). Zatim, umjesto slova o ubaciti broj 0, a umjesto slova a staviti @ (st0Lic@). Može se dodati na kraju znak ! (st0Lic@!). Moguće je i neku riječ zapisati unazad, npr. stolica = acilots (iako nema smisla, ali je dovoljno da zapamtite pojam za koji ste se opredijelili). Što je više koraka u kreiranju algoritma, to je zaporka sigurnija. Prednost takvog načina stvaranja zaporki, osim njihove sigurnosti i različitosti, jest i pamtljivost jer je dovoljno zapamtiti način na koji kreirate zaporke da biste znali veliki broj istih napamet.

Poticanje informatičke pismenosti, računalne i komunikacijske tehnologije postalo je dio svakodnevnog života. Zbog raznih opasnosti koje nude elektronički mediji, važno je pravovremeno prepoznati i spriječiti neželjene događaje. Važno je educirati djecu i mlade o preuzimanju odgovornosti za svoje ponašanje i o posljedicama određenih postupaka na internetu kao i o sigurnosnim pravilima kako bi se zaštitila njihova prava, interesi i aktivnosti.

2.3. ZA RAZMIŠLJANJE

Thierer (2009) navodi primjer kako je u SAD-u imenovano pet radnih skupina sastavljanih od stotine stručnjaka iz cijeloga svijeta koji se bave sigurnošću djece na internetu i da se svih pet skupina složilo oko zajedničkih zaključaka/preporuka koje su se nametnule u svim skupinama.

- ✓ Obrazovanje je primarno rješenje za većinu internetskih problema glede sigurnosti djece naglašavajući važnost medijske pismenosti i napora u osvješćivanju

javnosti, javnih službi, primjena ciljanih intervencijskih tehnika i bolja strategija mentorstva i roditeljstva.

- ✓ Ne postoji „čarobni štapić" kojim bi se riješila zabrinutost glede sigurnosti djece, naročito u vremenu brzih promjena u digitalnom svijetu.
- ✓ Osnaživanje roditelja i skrbnika različitim alatima može pomoći obiteljima i školama više kontrolirati sadržaje i komunikaciju internetom.
- ✓ Tehnološki alati i roditeljski nadzor najučinkovitiji su dio složenog pristupa sigurnosti djece koji ih smatra jednim od mnogih strategija ili rješenja.
- ✓ Najbolje tehničke mjere kontrole su one koje zajedno s obrazovnim strategijama i pristupima vode dijete i mentoriraju ga. Stoga, tehnička rješenja mogu nadopuniti, ali nikada zamijeniti ulogu obrazovanja i mentoriranja.
- ✓ Kreatori politika trebali bi se usredotočiti na poticanje kolaborativnih, višestranih inicijativa i pristupa kako bi se poboljšala sigurnost na internetu. Dodatni resursi za obrazovanje i napore za izgradnju svijesti također su presudni.
- ✓ Na kraju, države bi trebale osigurati odgovarajuće kazne za teška kaznena djela protiv djece i osigurati da agencije za provedbu zakona imaju odgovarajuća sredstva za privođenje i kažnjavanje zločinaca.

2.4. KORISNE POVEZNICE

U Republici Hrvatskoj već postoje brojni projekti, udruge i organizacije koje se bave sigurnošću na internetu. Ovdje donosimo pregled nekih od njih kako bi vam olakšali snalaženje u pronalasku edukativnih brošura, prezentacija, radionica, aplikacija, obrazaca za uklanjanje osobnih podataka s društvenih mreža itd.

→ Na mrežnoj stranici Agencije za zaštitu osobnih podataka možete pronaći obrasce za uklanjanje osobnih podataka s društvenih mreža (prijava lažnog profila na Facebooku, prijava lažnog profila na Instagramu, uklanjanje videozapisa sa You Tubea, zahtjev prema Googleu za uklanjanje rezultata pretraživanja o fizičkoj osobi).

http://azop.hr/zahtjevi-za-uklanjanje-osobnih-podataka/ (Pristupljeno 6. 11. 2018.)

→ Agencija za zaštitu osobnih podataka izradila je niz promotivnih i edukativnih materijala o zaštiti osobnih podataka namijenjenih djeci, roditeljima i ostalim građanima koje također možete pronaći na poveznici Agencije.

- *Vodič ICC-a za informacijsku sigurnost u poslovanju*
- Letak *Korištenje kanala dpacasework@fb.com – obraćanje Facebooku*
- Letak *Deset najčešćih upita o zaštiti privatnosti na Facebooku*
- Brošura *Safety@Facebook*
- Letak *Prava potrošača u sustavu zaštite osobnih podataka u RH*
- Brošura *Zaštita podataka – Bolja pravila za mala poduzeća*
- Letak *Opća Uredba o zaštiti osobnih podataka*
- Brošura *Privatnost djece i mladih u svijetu modernih tehnologija*
- Letak P*rivatnost – zašita osobnih podataka građana*
- Vodič za voditelje zbirki osobnih podataka
- Vodič za građane EU – SAD *Štit privatnosti*
- Brošura *Zaštita osobnih podatka u RH*
- Brošura *Zaštita privatnosti na radnom mjestu*
- Brošura *Sigurno surfanje: zaštita osobnih podataka na internetu*
- Brošura *Moja Fejs priča*
- Letak *Ne budi meta kradljivaca identiteta*
- Letak *Zaštita osobnih podataka djece na internetu*
- Letak *Zaštita osobnih podataka djece na društvenim mrežama*
- Letak *10 koraka protiv govora mržnje na internetu*
- Letak *Bolja zaštita vaših osobnih podataka*

https://azop.hr/info-servis/detaljnije/promotivni-materijali/ (Pristupljeno 6. 11. 2018.)

→ CARNET – hrvatska akademska i istraživačka mreža na svojim stranicama posebno posvećuje pozornost sigurnosti na internetu gdje možete pronaći brošure namijenjene mladima, osnovne korake zaštite računalne infrastrukture poduzeća od sigurnosnih rizika. Savjeti su posebno prilagođeni prioritetima i zadaćama računala u poslovnom okruženju. Neke od tema su zaštita tajnosti podataka, izrada sigurnosne politike te sigurnosno podešavanje poslužitelja javnih usluga. Opasnostima kojima se izlažete postavljanjem osobnih podataka i sadržaja na najpopularniju društvenu mrežu te kako podesiti svoj profil na Fecebooku tako da čuva privatnost. Navedene brošure možete pronaći na stranici CARNETA.

- Brošura *Zaštitite privatnost na Facebooku*

- Brošura *Sigurnije na internetu*
- Brošura *Sigurnije poslovanje na internet*u

http://www.carnet.hr/sigurnost (Pristupljeno 6. 11. 2018.)

→ Antibot.hr besplatan je servis koji pruža CARNet zajedno s tvrtkama partnerima. Namjena antibot.hr servisa je smanjenje broja zaraženih računala, tableta i pametnih telefona kao i pomoć korisnicima pri čišćenju vlastitih uređaja za pristup internetu od zlonamjernih programa. Ovdje možete pronaći pregled općenitih informacija i savjeta o prijetnjama na internetu te prijedlozima za zaštitu (*phishing, ransomware*, neželjene poruke, sigurne zaporke, internet bankarstvo, siguran WLAN).

http://www.antibot.hr/ (Pristupljeno 6. 11. 2018.)

→ Centar za nestalu i zlostavljanu djecu neprofitna je udruga osnovana 2006. godine u Osijeku. Motiv za osnivanjem Centra osnivači su prepoznali u problemima nedovoljne zaštite djece od seksualnog iskorištavanja i zlostavljanja na internetu te širenja dječje pornografije i pedofilije, ali i drugih oblika zlostavljanja koji se odnose na uporabu interneta. Proizišle materijale s projekta možete pronaći na stranici projekta. Edukacijski paket za Dan sigurnijeg interneta 6. 2. 2018. sadrži:

Djeca i mladi

- Društvena igra (PDF)
- Edukacijski paket – radionice (PDF)

Nastavnici i roditelji

- *Cyberbullying* (PPT)
- Priručnik prevencija nasilja putem interneta
- Program edukacije – *Mediji današnjice*

Promotivni materijali

- 10 pitanja o sigurnosti – KVIZ (PDF)
- 5 savjeta za sigurno korištenje interneta (PDF)
- 5 savjeta za sigurno korištenje interneta (VIDEO)

http://www.csi.hr/p/materijali-i-savjeti (Pristupljeno 6. 11. 2018.)

→ Projekt „Safer Internet Centre Croatia: Making internet a good and safe place" (2015-HR-IA-0013) sufinancirala je Europska unija iz programa Department C – Connecting Europe Facility (CEF). Projekt se provodio pod pokroviteljstvom Innovation and Networks Executive Agency (INEA) na temelju ovlasti delegirane od strane Europske komisije. Koordinator projekta bio je Centar za nestalu i zlostavljanu djecu, a partneri Sveučilište Josipa Jurja Strossmayera, Osijek, Fakultet za odgojne i obrazovne znanosti, Grad Osijek te VIPnet d.o.o. Specifični ciljevi projekta bili su: daljnji razvoj i promocija centra za podršku i informiranje djece, roditelja, učitelja i drugih koji rade s djecom o boljoj i sigurnijoj upotrebi interneta; poboljšanje *Helpline* usluge za prijavljivanje i pružanje pomoći vezano uz štetne kontakte *(grooming)*, ponašanja (internetsko zlostavljanje – *cyberbullying*) i sadržaje, daljnje održavanje Hotline usluge za primanje i izvještavanje te prikupljanje podataka o protuzakonitom *online* seksualnom zlostavljanju djeteta.

http://cnzd.org/projekti/centar-za-sigurniji-internet (Pristupljeno 6. 11. 2018.)

→ Projekt „*Prepoznaj rizike digitalnog doba*" projekt je koji je financiralo Ministarstvo socijalne politike i mladih, a koji je provodio Centar za nestalu i zlostavljanu djecu u partnerstvu s Gradom Osijekom, Sveučilištem Josipa Jurja Strossmayera u Osijeku – Filozofskim fakultetom, Domom za odgoj djece i mladeži Osijek i Dječjim domom Sv. Ana Vinkovci. Specifični ciljevi projekta bili su: uspostava novih alata i mehanizama za prevenciju elektroničkoga nasilja nad i među djecom i mladima; edukacija o elektroničkom nasilju (rano uočavanje i prepoznavanje elektroničkog nasilja, sigurnost na internetu i zaštita osobnih podataka, zaštita prava djece i mladih, *web detektivi*, govor mržnje i *seksting*, simptomatologija žrtve/počinitelja, prevencija i intervencija); podizanje svijesti građana o problemu i prepoznavanju elektroničkog nasilja nad i među djecom i mladima te poticanje na njihovu prijavu. Proizišle materijale s projekta možete pronaći na stranici projekta.

Materijali za edukaciju

- Prepoznavanje elektroničkog nasilja (PPT)
- *Web detektivi* (PPT)
- Digitalni priručnik o elektroničkom nasilju

Promotivni materijali

- Plakat *Prepoznaj rizik*
- Letak *Prepoznaj rizik*e
- Brošura *Prepoznaj rizike*

http://digitalnirizici.org/materijali/ (Pristupljeno 6. 11. 2018.)

→ Projekt „*Dvaput razmisli, jednom klikni*" projekt je koji je financiralo Ministarstvo znanosti, obrazovanja i sporta, a koji provodi Centar za nestalu i zlostavljanu djecu u partnerstvu sa Sveučilištem Josipa Jurja Strossmayera u Osijeku – Fakultetom za odgojne i obrazovne znanosti, Domom za odgoj djece i mladeži Osijek i Centrom za rehabilitaciju „Mala Terezija". Opći je cilj projekta „Dvaput razmisli, jednom klikni" povećati mogućnost djece i mladih da izvan redovitog odgojno-obrazovnog sustava steknu znanja, vještine i usvoje primjerena stajališta o medijskoj pismenost. Razvoj medija čini sve značajnijim pitanja koja se odnose na utjecaj medija na konzumente medijskih sadržaja, osobito na djecu kao najosjetljiviji dio populacije. Sa svrhom ostvarenja općeg cilja, postavljeni su specifični ciljevi projekta: osvješćivanje djece i mladih o nužnosti kritičkog odnosa prema medijskim sadržajima; povećanje medijske pismenosti roditelja djece s teškoćama, asistenata u nastavi te odgajitelja u domovima za nezbrinutu djecu. Proizišle materijale s projekta možete pronaći na stranici projekta.

Materijali za edukaciju

- Mediji – *web detektivi* (PPT)
- Edukacijska brošura
- Bonton na internetu (PPT)

Promotivni materijali

- Brošura *Dvaput razmisli*
- Plakat *Dvaput razmisli*

Mobilna aplikacija

- Mobilna aplikacija *Dvaput Razmisli*

Digitalna brošura

- Digitalna brošura *Dvaput razmisli*

http://razmisli.org/materijali-za-strucnjake/ (Pristupljeno 6. 11. 2018.)

→ Projekt „*Web detektivi"* pokrenut je s ciljem obrazovanja i osposobljavanja djece diljem Republike Hrvatske za usvajanje i razvijanje vještina prepoznavanja neprimjerenih i opasnih medijskih sadržaja održavanjem tematskih predavanja i praktičnih radionica s učenicima osnovnoškolske dobi. *Web detektivi* su djeca obučena za prepoznavanje i prijavljivanje neprimjerenih sadržaja na internetu. Stoga je namjera projekta u skladu s odredbama o sigurnosti i zaštiti zdravlja odgojno-obrazovnih

ustanovama jer potiče stvaranje uvjeta za zdrav mentalni i fizički razvoj te socijalnu dobrobit učenika, sprječava neprihvatljive i rizične oblike ponašanja, brine se o sigurnosti učenika, omogućava praćenje socijalnih problema i pojava kod učenika i poduzimanja mjera za otklanjanje njihovih uzroka i posljedica u suradnji s tijelima socijalne skrbi odnosno s drugim nadležnim tijelima te pospješuje vođenje evidencije o neprihvatljivim oblicima ponašanja učenika, uz mogućnost unaprjeđivanja usluga savjetodavnoga rada s učenicima (Članak 67., Zakon o odgoju i obrazovanju u osnovnoj i srednjoj školi, NN, br 87/08).

http://webdetektivi.org/ (Pristupljeno 6. 11. 2018.)

2.5. LITERATURA

Beth, H., Jones, B. H., Goyal Chin, A. i Aiken, P. (2014). Risky business: Students and smartphones. *TechTrends*, *58*(6), 73-83.

Davis, K. i James, C. (2013). Tweens' conceptions of privacy online: implications for educators.*Learning, Media and Technology*, *38*(1), 4-25. https://doi.org/10.1080/17439884.2012.658404

DiGi. (2014). *Safety net: Capacity building among Malaysian school children on staying safe online. A national survey report*. Preuzeto s https://digi.cybersafe.my/files/article/ CyberSAFE_Survey_Report_2014.pdf, 25.3.2018.

Er, P. H., Cheah, P. K., Moses, P., Chong, C. K. i Ang, B. H. (2017). Awareness of Safe and Responsible Use of ICT Among Students in a Malaysian University. U: G.B. Teh i S.C. Choy (ur.), *Empowering 21st Century Learners Through Holistic and Enterprising Learning*, (str.41-48). Singapore: Springer Nature Pet Ltd. https:// doi.org/10.1007/ 978-981-10-4241-6_5

Gasser, U., Maclay, C. M. i Palfrey Jr. J. G. (2010). Working Towards a Deeper Understanding of Digital Safety for Children and Young People in Developing Nations. *Harvard Law School Public Law & Legal Theory Working Paper Series*, 10-36.

Hall, B. R. (2012). An Ethics Whirlwind: A Perspective of the Digital Lifestyle of Digital Natives and Initial Thoughts on Ethics Education in Technology. *Information Systems Education Journal, 10*(1), 4-12.

Hagen, J. M. i Albrechtsen, E. (2009). Effects on employees' information security abilities by e- learning. *Information Management & Computer Security*, *17*(5), 388-407. https:// doi.org/10.1108/09685220911006687

Hrvatska udruga banaka (2017). *Godišnje izvješće Hrvatske udruge banaka o stanju sigurnosti na Internetu u 2016. godini*. Preuzeto s http://www.sigurnostnainternetu. hr/index. php/istrazivanja/item/53-novo-istrazivanje-hub-a-otkriva-hrvati-lezerno-koriste-internet-no-vecina-je-oprezna, 13.5.2018.

Hui, B. i Campbell, R. (2018). Discrepancy between Learning and Practicing Digital Citizenship. *Journal of Academic Ethics, 16*(2), 117–131. https://doi.org/10.1007/s10805-018-9302-9

International Telecommunications Union (2017). *ICT Facts and Figures: The World in 2017*. Geneva, ICT Data and Statistics Division, ITU. Preuzeto s https://www.itu. int/en/ITU-D/Statistics/Pages/facts/default.aspx, 15.3.2018.

Jones, B. H., Goyal Chin, A. i Aiken, P. (2014). Risky business: Students and smartphones. *TechTrends*, *58*(6),73-83.

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security*, *22*(1), 115-126. https:// doi.org/ 10.1108/IMCS-01-2013-0005

Lasić-Lazić, J., Špiranec, S. i Banek Zorica, M. (2012). Izgubljeni u novim obrazovnim okruženjima-pronađeni u informacijskom obrazovanju. *Medijska istraživanja,* 18(1), 125-142.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. i Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049-1092. https://doi.org/10.1108/MRR-04-2013-008

Livingstone, S., Haddon, L., Görzig. A. i Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings.* London, EU Kids Online. Preuzeto s http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/ EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf, 11.2. 2018.

Lomo-David, E., Shannon, L. i Ejimakor, G. (2009). Information systems security and safety measures: The dichotomy between students' familiarity and practice. U: S. Johnson (ur.), *First Annual General Business Conference Conference Proceedings* (str. 268 - 282). Houston: Sam Houston University.

Mensch, S. i Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Acad. Inform. Manage. Sci. Journal, 14,* 91-116.

Robertson, M., Fluck, A. i Thomas, S. (2001). Expert versus novice users: power rules in virtual space. *Australian Educational Researcher*, *28*(1), 147-167. https://doi.org/10.1007/BF03219748

Sharples, M., Graber, R., Harrison, C. i Logan, K. (2009). E-Safety and Web2.0 for children aged 11-16. *Journal of Computer-Assisted Learning*, *25*, 70-84.

Siponen, M.T. (2000). A conceptual foundation for organizational information security awareness, *Information Management & Computer Security*, *8*(1), 31-41. https://doi.org/10.1108/09685220010371394

Thierer, A. (2009). *Parental Controls & Online Child Protection: A Survey of Tools & Methods*. Washington D.C.: The Progress & Freedom Foundation.

Teer, F., Kruck, S. i Kruck, G. (2007). Empirical study of students' computer security practices/perceptions. *Journal of Computer Information Systems*, *47*(3), 105-110. https://doi.org/10.1080/08874417.2007.11645971

Townsend, A. M. (2010). Mobile communications in the twenty- first century city. U: B. Brown, N. Green, i R. Harper (ur.) *Wireless World: Social and Interactional Aspects of the Mobile Age* (str. 62 - 77). New York: Springer.

UNESCO (2015). *World Trends In Freedom of Expression and Media Development: Special Digital Focus 2015*. Preuzeto s http://unesdoc.unesco.org/images/0023/002349/234933e.pdf, 22.2.2018.

Velki, T., Šolić, K. i Očević, H. (2014). Development of Users' Information Security Awareness Questionnaire (UISAQ) - Ongoing Work. *Hrvatska udruga za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku – MIPRO proceedings,* 1564-1568.

Velki, T., Šolić, K., Gorjanac, V. i Nenadić, K.(2017). Empirical study on the risky behavior and security awareness among secondary school pupils - validation and preliminary

results. *Hrvatska udruga za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku – MIPRO proceedings,* 1496-1500.

Velki, T., Šolić, K. i Nenadić, K. (2015). Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK). *Psihologijske teme*, *24*(3), 401-424.

Vrana, R. (2013). Online social networks and security of their users: an exploratory study of students at the Faculty of humanities and social sciences Zagreb. U: T. Hunjak, S. Lovrenčić i I. Tomičić (ur.), *Central European Conference on Information and Intelligent Systems* (str. 214 - 221). Varaždin: University of Zagreb Faculty of Organization and Informatics.

Wilcox, H., Bhattacharya, M. i Islam, R. (2014). Social Engineering through Social Media: An Investigation on Enterprise Security. U: L. Batten, G. Li, W. Niu i M. Warren (ur.), *Applications and Techniques in Information Security. ATIS 2014: Communications in Computer and Information Science*, vol. 490 (str. 243 - 255). Berlin: Heidelberg Springer.

izv. prof. dr. sc. Tena Velki

Fakultet za odgojne i obrazovne znanosti Sveučilišta Josipa Jurja Strossmayera u Osijeku

doc. dr. sc. Ksenija Romstein

Fakultet za odgojne i obrazovne znanosti Sveučilišta Josipa Jurja Strossmayera u Osijeku

3. NACIONALNO ISTRAŽIVANJE RIZIČNOG PONAŠANJA I ZNANJA RAČUNALNIH KORISNIKA

Sažetak

U idućem poglavlju dan je prikaz rezultata nacionalnog istraživanja provedenog na računalnim korisnicima te će se podastrijeti jednostavne strategije zaštite korisnika koji oni mogu primjenjivati sami iako su prema zakonskim regulativama provajderi interneta dužni zaštiti svoje korisnike, no o tome nemamo dovoljno istraživanja na području EU-a. U istraživanju je sudjelovalo 4859 sudionika (37,5 % muških) iz cijele Hrvatske, podijeljenih u tri velike skupine; srednjoškolci (n=3250), studenti (n=883) i zaposlenici (n=726). Cilj je bio ispitati znanja i rizična ponašanja korisnika računalnih sustava u cijeloj Republici Hrvatskoj uzimajući pri tom u obzir dobne i spolne razlike. Provjereno je i stvarno ponašanje odavanja zaporke korisnika računalnih sustava. Također je utvrđena povezanost informacijskoga znanja s rizičnim ponašanjem računalnih korisnika. Rezultati istraživanja pokazali su kako veliki broj sudionika (31 % – 54,2 %) dobrovoljno odaje svoju zaporku te su studenti u tom pogledu najrizičnija skupina. Odrasli zaposlenici pokazuju najviše rizičnog ponašanja glede korištenja informacijskih sustava, ali istodobno i najveći stupanj znanja. Potom slijede studenti, a na kraju srednjoškolci

s najnižim stupnjem znanja ali i rizičnoga ponašanja. Općenito je utvrđeno da osobe s višom razinom znanja o informacijskoj sigurnosti pokazuju i viši stupanj rizičnih oblika ponašanja na internetu. Dobiveni podatci u skladu su s istraživanjima koja su provedena u zemljama EU-a u kojima je potvrđena povezanost rizičnih ponašanja i kronološke dobi korisnika te rizičnih ponašanja i količine vremena provedene na internetu. Tako djeca i mladi koji provode više vremena na internetu češće manifestiraju rizična ponašanja, kao npr. odavanje svojih osobnih podataka nepoznatim osobama, prihvaćanje prijateljstava i poruka od nepoznatih osoba, sve do sastajanja offline s online prijateljima koje nisu prethodno upoznali u stvarnom životu. Što se tiče odraslih, istraživanja provedena u zemljama EU-a nešto su manje opsežna i govore uglavnom o korištenju alata kao što su net-banking ili nadgledanje korištenja interneta djece, nedostaju podaci za populaciju odraslih, što se djelomice tumači smanjenjem rizika porastom kronološke dobi, no ta pretpostavka nije do kraja potvrđena. Ukratko, ponašanja korisnika interneta ovise o trima čimbenicima, a to su: kulturni kontekst, zakonska regulativa i odgojno-obrazovni kontekst što treba uvažiti prilikom provođenja budućih istraživanja kao i kreiranja smjernica za zaštitu internetskih korisnika od najmlađe dobi.

3.1. UVOD

Sveprisutnost interneta u svakodnevnom životu ljudi dovela je do pojave da virtualni svijet postaje sve više dio stvarnog realnog svijeta, odnosno gube se jasne granice između virtualnog i stvarnog svijeta. Internet sve više obuhvaća postojeći realni svijet te kao takav ulazi u sva područja života čovjeka gdje današnji suvremeni život postaje nezamisliv bez svakodnevne upotrebe interneta. Upravo ta promjena suvremenog društva gdje se aktivnosti sele iz realnog u virtualni svijet omogućuje i ubrzani razvoj socijalnog inženjeringan odnosno razvoj internetskih prijevara koje se ciljano usmjeravaju na lakovjernog korisnika (Haley, 2011; Mitnick, Simon i Wozniak, 2002; Selmar i Tibert, 2018). Početno, naizgled beznačajno, odavanje manjeg broja osobnih podataka, npr. pri instalaciji manjih aplikacija, korištenjem društvenih mreža, kupnji kino-ulaznica na internetu i sl., može u konačnici dovesti do materijalnih gubitaka, ali i dijelom gubitka privatnosti. Korisnici koji su neoprezni, nesmotreni i općenito nesvjesni potencijalnog rizika predstavljaju najveći problem pri osiguravanju informacijske sigurnosti. Niz istraživanja tijekom posljednja dva desetljeća jasno pokazuje kako je sam računalni korisnik odnosno ljudska komponenta najslabija karika po pitanju informacijske sigurnosti (Lukasik, 2011; Sasse, Brostoffand i Weirich, 2001). Korisnici informacijskih sustava svojim nepromišljenim i rizičnim ponašanjem mogu značajno utjecati na cijeli sustav informacijske sigurnosti. Važnost znanja, ponašanja i svijesti o pitanjima sigurnosti informacijskih i privatnih podataka među korisnicima interneta prvo su prepoznali mrežni administratori i stručnjaci za sigurnost, a tek nakon toga tom se problematikom počinju baviti znanstvenici. Međutim još je uvijek relativno malo znanstvenih istraživanja u tom području (Crossler i sur., 2013; Kwang i Choo, 2011), a većina se njih uglavnom bavila pitanjem kvalitete i snage zaporke korisnika računalnih sustava (Dell'Amico, Michiardi i Roudier, 2010; Kelley i sur., 2012; Voyiatzis, Fidas, Serpanos i Avouris, 2011; Wanli, Campbell, Tran i Kleeman, 2010). Tako je, npr. jedno novije istraživanje pokazalo kako većina korisnika jačinu i kvalitetu svoje zaporke procjenjuje kao prosječnu, a samo 13,8 % korisnika kao lošu (Šolić, Očevćić i Blažević, 2015), no postavlja se pitanje kako bi stručnjaci procijenili njihove zaporke. Nadalje, isti korisnici (53,4 %) preferiraju koristiti istu zaporku za pristup većini korištenih informacijskih sustava što uvelike narušava informacijsku sigurnost. Drugim riječima, percepcija sigurnosti i rizika individualna je. O osobnom, individualnom tumačenju sigurnosti (engl. *safety/ security*) i rizika govori i Europska agencija za informacijsku sigurnost (ENISA, 2014) te pojašnjava kako su osobna ponašanja ključna za pitanje sigurnosti pojedinca, a i interneta općenito.

Literatura na području internetske sigurnosti uglavnom ne daje veliku važnost istraživanjima rizičnih ponašanja odraslih korisnika, već je uglavnom usmjerena na

djecu i maloljetnike koje vidi kao izrazito vulnerabilnu populaciju u odnosu na virtualni svijet. Izostajanje propitivanja rizičnih ponašanja odraslih vodi prema simplificiranom pristupu sistemske perspektive prevencije opasnosti kojima djeca mogu biti izložena. Naime, istraživanje ENISA-e (2014) pokazuje kako su ponašanja roditelja uporabom interneta i djece slična te se može zaključiti kako se takva ponašanja uče, tj. ponašanja odraslih na internetu mogu biti model ponašanja djeci. Prvi veći pomaci napravljeni su razvojem upitnika koji mjere znanja i ponašanja korisnika informacijskih sustava, a znanstvenici iz Republike Hrvatske bili su među prvima u svijetu koji su se počeli baviti razvojem *Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava* – UZPK (Velki, Šolić i Očevćić, 2014). Prva istraživanja na punoljetnim zaposlenicima otkrila su zabrinjavajuće podatke. Čak oko 30 % zaposlenika dobrovoljno je otkrilo svoju zaporku istraživačima koju koriste za službenu e-poštu (Šolić, Velki i Galba, 2015). Još više zabrinjava podatak dobiven od srednjoškolaca od kojih je čak 78 % otkrilo svoju zaporku koju koriste za privatnu e-poštu, što je statistički značajno više nego kod zaposlenika (Velki, Šolić, Gorjanac i Nenadić, 2017). Upravo problem davanja zaporke i osobnih podataka ENISA (2014) navodi kao vodeći izazov u informatičkom opismenjavanju jer je sigurnost osobnih podataka (uključujući i zaporku) jedna od prvih tema u programima informatike pa nije do kraja jasno otkuda ta vrsta rizičnog ponašanja iako se na formalnoj razini o tome razgovara s korisnicima već u školskim klupama. Zaposlenici koji rade u privatnom sektoru češće su odavali svoju zaporku od zaposlenika koji rade u državnom sektoru. Zaposlenici s višim stupnjem obrazovanja (završenim fakultetom) u odnosu na zaposlenike s nižim stupnjem obrazovanja (završena srednja škola) bili su pouzdaniji i rjeđe su otkrivali zaporku. Općenito osobe koje nisu otkrile svoju zaporku pokazale su bolje znanje o informacijskoj sigurnosti (npr. prave kopije važnih dokumenata, provjeravaju antivirusnim programom vanjsku memoriju i sl.) i manje rizičnog ponašanja (npr. održavaju zaštitu kućnog računala, ne govore drugima svoje PIN brojeve i zaporke i sl.) (Šolić, Velki i Galba, 2015) dok su studenti koji nisu odali svoju zaporku pokazivali manje rizičnog ponašanja uporabom računala, ali podjednaku razinu znanja kao i studenti koji su odali svoju zaporku (Velki, Šolić i Nenadić, 2015). U odnosu na odrasle zaposlenike srednjoškolci su pokazali rizičnije ponašanje na internetu (npr. posuđuju svoje pristupne podatke prijateljima i rođacima, šalju lančane poruke, odgovaraju na e-poštu nepoznatih osoba i sl.), problematičniju komunikaciju na internetu (npr. dopisivanje e-poštom s nepoznatim osobama, odavanje osobnih podataka na društvenim mrežama i sl.) te su slabije pohranjivali računalne podatke, no bili su bolji u održavanju računala i po pitanju uvjerenja o informacijskoj sigurnosti podataka, tj. mogućnosti krađe i zlouporabe informacijskih podataka gdje su pokazali veću svjesnost vezano uz navedenu problematiku (Velki i sur., 2017). Žene (studentice i odrasle zaposlenice) u odnosu na muškarce opreznije su i skeptičnije u

otkrivanju privatnih podataka putem *online* sustava (Šolić, Velki i Galba, 2015) što vrijedi i za srednjoškolce (Velki i sur., 2017). Stariji zaposlenici u odnosu na mlađe (mlađe od 30 godina) pokazali su veće ukupno znanje glede informacijske sigurnosti i manje rizičnog ponašanja (Šolić, Velki i Galba, 2015) dok su studenti u odnosu na zaposlenike bolje održavali računala, ali su istodobno bili neoprezni i prakticirali nesigurniji način komunikacije na internetu (Velki, Šolić i Nenadić, 2015). I za srednjoškolce i za odrasle sudionike istraživanja dobivena je statistički značajna povezanost između skala znanja o informacijskoj sigurnosti i skala rizičnog ponašanja korisnika računala pri čemu osobe koje imaju više znanja i svjesnije su potencijalne opasnosti ujedno se i rizičnije ponašaju pri uporabi informacijskih sustava (Velki i sur., 2017). Također su i neka prijašnja istraživanja pokazala da je sama svjesnost i znanje o informacijskoj sigurnosti nedovoljni da se osoba ponaša u skladu s tim, čak i među vrlo obrazovanim sveučilišnim profesorima (Šolić i Ilakovac, 2009; Šolić, Ilakovac, Marušić i Marušić, 2009).

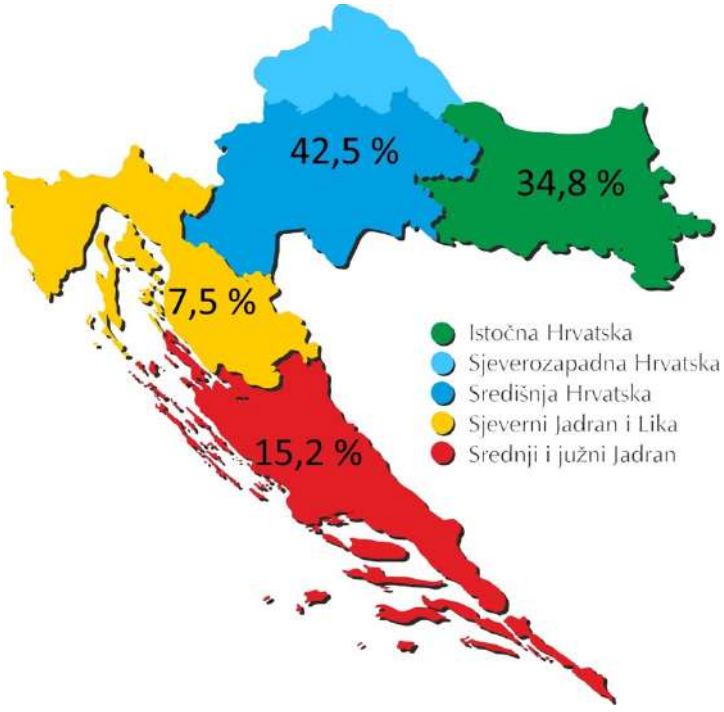
Što se tiče istraživanja u zemljama EU-a, ona su uglavnom usmjerena na identifikaciju rizičnih oblika ponašanja na internetu za djecu i mlade, dok se u odnosu na odraslu dob (nakon 21. godine života) vrlo rijetko pojavljuju. Čini se kako se interes za odrasle kao korisnike interneta javlja uglavnom u kontekstu zaštite djece, dok se odrasla dob ne vidi kao posebno osjetljiva dob za rizične oblike ponašanja na internetu. ENISA (2014) u svojem istraživanju potvrđuje kako rizici opadaju s kronološkom dobi, no to nije do kraja moguće potvrditi iz nekoliko razloga: prvi je temeljenje istraživanja na samoprocjenama korisnika, tj. izostanak softvera koji bi prikupio i izračunao podatke o rizičnim ponašanjima korisnika neovisno o njihovoj procjeni vlastita ponašanja u *online* svijetu. Nadalje, odrasli su skloniji socijalnom konformizmu pa ako i prakticiraju rizična ponašanja, manja je vjerojatnost da će to otvoreno i priznati. Naposljetku, moguće je da su se odrasli tijekom služenja internetom susreli sa sadržajima koji su ih uznemirili, no vremenom su razvili strategije nošenja s rizicima i nelagodom pa lakše mogu prepoznati potencijalne rizične situacije što djeci i mladima uglavnom nedostaje. Odnosno, odrasli imaju iskustvo koje im može olakšati učinkovitije snalaženje u informatičkom svijetu komunikacije. Upravo prepoznavanje rizičnih situacija iznimno je bitno gledište sigurnosti na internetu jer se sigurnost nikada ne može u potpunosti postići, ali je moguće prepoznavanje rizika i reduciranje njihovih učinaka ako se na vrijeme prepoznaju (ENISA, 2014). Stoga je prikupljanje podataka od samih korisnika prvi korak u razvijanju algoritama sigurnosti na internetu što je bila i glavna svrha navedenog istraživanja.

3.2. NACIONALNO ISTRAŽIVANJE

Cilj provedenog nacionalnog istraživanja bio je ispitati osnovne karakteristike računalnih korisnika i međusobno usporediti rezultate za različite korisnike. Ukupno je sudjelovalo 4859 sudionika (37,5 % muških) iz cijele Republike Hrvatske. Raspon dobi kretao se od 14 do 65 (M=20,78, SD=9,52), prosječna dob srednjoškolaca bila je M=16,24 (SD=1,08), prosječna dob studenata M=21,93 (SD=4,29) te prosječna dob odraslih djelatnika (odrasle zaposlene osobe) M=39,68 (SD=11,26). U Tablici 1. prikazana je raspodjela sudionika prema spolu, a na Slici 1. rasprostranjenost prema regijama iz koje dolaze sudionici.

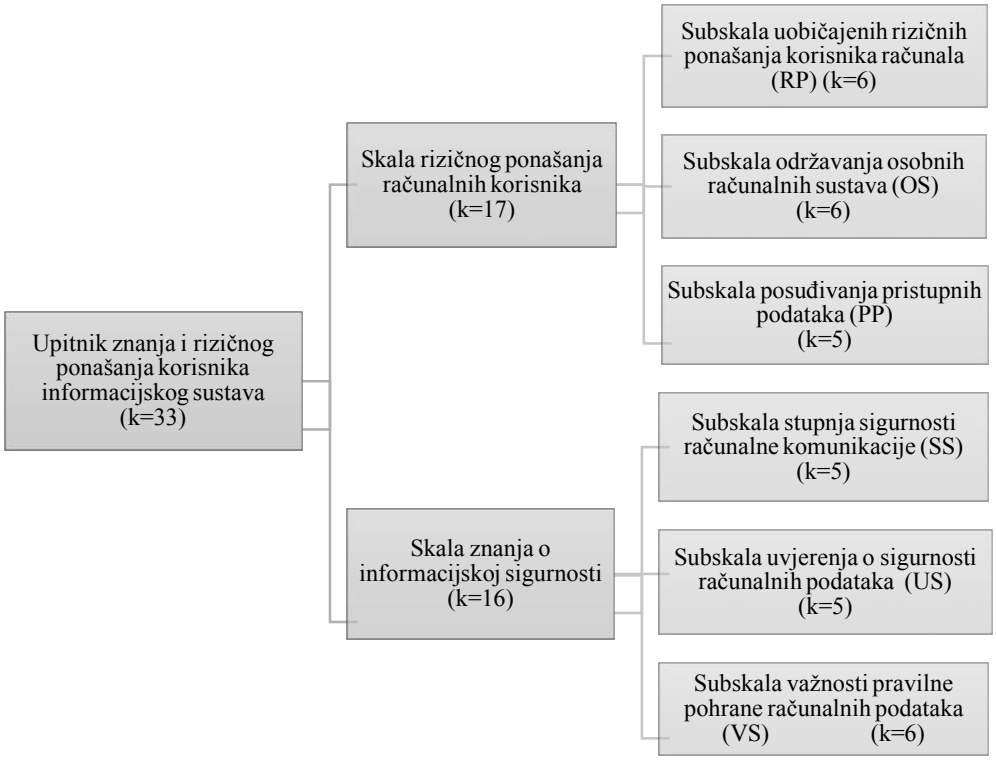
Tablica 1. Raspodjela sudionika po spolu

			muško		žensko	
Sudionici	N	%	N	%	N	%
srednjoškolci	3250	66,9	1317	40,5	1933	59,5
studenti	883	18,2	216	24,5	667	75,5
djelatnici	726	14,9	287	39,5	439	60,5
Ukupno	**4859**	**100,0**	**1820**	**37,5**	**3039**	**62,5**



Slika 1. Rasprostranjenost sudionika prema regijama Republike Hrvatske iz kojih dolaze

U istraživanju je korišten *Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava* (UZPK) koji ispituje rizična ponašanja i znanja računalnih korisnika. Upitnik se sastoji od općih demografskih pitanja (spol, dob, mjesto stanovanja i sl.), testnog pitanja o odavanju zaporke te dvije glavne skale: Skala rizičnog ponašanja računalnih korisnika (k=17) i Skala znanja o informacijskoj sigurnosti (k=16). Skala rizičnog ponašanja računalnih korisnika dijeli se u tri subskale pri čemu Subskala uobičajenih rizičnih ponašanja računalnih korisnika (k=6) mjeri različita rizična ponašanja (npr. *Otvarate, bez provjere, priloge nepoznatih pošiljatelja)*, Subskala održavanja osobnih računalnih sustava (k=6) mjeri učestalost i kvalitetu održavanja osobnih računalnih sustava (npr. *Koristite različite lozinke za različite sustave, npr. za Facebook jedna, za e-poštu druga, za poslovni sustav treća lozinka itd.*), a Subskala posuđivanja pristupnih podakata (k=5) mjeri učestalost odavanja različitih pristupnih podataka (npr. *Posuđujete svojim prijateljima, rođacima, poznanicima svoje privatne pristupne podatke za pristup osobnoj/privatnoj adresi e-pošte*). Drugi dio upitnika, koji mjeri znanje o informacijskoj sigurnosti, također se sastoji od triju subskala. Subskala stupnja sigurnosti računalne komunikacije (k=5) mjeri procjenu stupnja informacijske sigurnosti korisnika (npr. *Što mislite koliko je sigurna komunikacija na društvenim mrežama (npr. Facebook, Twitter)*, Subskala uvjerenja o sigurnosti računalnih podataka (k=5) mjeri stupanj uvjerenja korisnika o informacijskoj sigurnosti podataka (npr. *Koliko ste uvjereni da postoji realna opasnost da će vam netko ukrasti privatne podatke s vašeg kućnog računala*) te posljednja Subskala važnosti pravilne pohrane računalnih podataka (k=6) procjenjuje stupanj važnosti pravilnog čuvanja računalnih podataka (npr. *Prema vašem mišljenju koliko je važno provjeriti tuđi USB memorijski štapić od virusa prije učitavanja podataka*). Pouzdanost (tipa Cronbach α) UZPK-a za mlade se sudionike kretala između 0,69 i 0,84, a za odrasle djelatnike Cronbach α je bila od 0,67 do 0,88.



Slika 2. Prikaz skala i subskala Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava

Istraživanje je provedeno *online*, u potpunosti anonimno, tijekom jedne godine. Ustanove (škole, fakulteti i tvrtke) prvo su kontaktirane telefonski i elektroničkom poštom, a koje su pristale na suradnju, dobile su i pismenu zamolbu s detaljnim objašnjenjem svrhe istraživanja kao i uputama o provođenju istraživanja. Nakon toga poslani su im linkovi za pristup ispunjavanju upitnika. Svaka ustanova dobila je svoju poveznicu. Poveznice su bile aktivne između 3 i 6 mjeseci, a podaci su se automatski upisivali u bazu podataka za svaku ustanovu. Po završetku istraživanja svaka ustanova koja je sudjelovala u istraživanju dobila je podatke za svoje sudionike i njihovu usporedbu u odnosu na ostale sudionike u Republici Hrvatskoj.

3.3. ŠTO JE NACIONALNO ISTRAŽIVANJE POKAZALO?

Rezultati istraživanja (Tablica 2.) pokazuju kako između 31 % i 54,2 % sudionika istraživanja dobrovoljno daje svoju zaporku koje koriste za elektroničku poštu što

upućuje na zabrinjavajući činjenicu o odavanju osobnih podatka pri uporabi interneta. Prijašnja istraživanja pokazala su kako nešto manji broj zaposlenika (oko 30 %), ali znatno veći broj srednjoškolaca (oko 78 %) odaju svoju zaporku za e-poštu (Šolić, Velki i Galba, 2015; Velki i sur., 2017). ENISA (2014) istraživanje pokazuje kako je odavanje zaporke povezano s uporabom interneta na nacionalnoj razini odnosno u državama EU-a u kojima se internet koristi u većem postotku (primjerice Danska, Švedska), da odrasli rjeđe daju zaporke drugima, ali su i manje zabrinuti za sigurnost djece i mladih na internetu. S druge strane, u zemljama u kojima se internet manje koristi (npr. Grčka, Španjolska, Portugal) davanje je zaporke češće, ali je i zabrinutost za sigurnost djece na internetu veća. Razlog tomu može biti nedostatno poznavanje interneta, rizično ponašanje na internetu i strategija prevencije, tj. korisnici koji slabije poznaju internet zabrinutiji su za sigurnost djece, dok u isto vrijeme oni sami manifestiraju rizična ponašanja. Z-testom proporcija utvrđene su i statističke značajne razlike u odavanju zaporka za različite skupine sudionika istraživanja. Srednjoškolci su statistički značajno najmanje skloni odavanju zaporke ($z=12,7$, $p<0,01$ u odnosu na studente, te $z=4,9$, $p<0,01$ u odnosu na zaposlenike) što djelomično može biti odraz odrastanja u virtualnom svijetu odnosno informacijske pismenosti koju su usvojili odgojem i/ili školovanjem. Iako se broj odraslih koji odaju zaporku nešto povećao na temelju podataka prijašnjih istraživanja (Šolić, Velki i Galba, 2015; Velki i sur., 2017), trend sve intenzivnijeg korištenja informacijskih sustava, pa posljedično tome i potencijalnih opasnosti koje donose elektornički sustavi, za mlađe sudionike primijećen je pozitivan trend. Moguće je da su zbog školovanja, posebice u sklopu nastave informatike, srednjoškolci postali svjesniji zlouporabe privatnih podatka koji dobrovoljno odaju pa imaju potrebu i želju bolje se zaštiti, odnosno sačuvati svoju privatnost. Također je moguće, zbog velike uporabe, a posebice zlouporabe društvenih mreža, da su srednjoškolci upravo skupina koja je tim promjenama najpogođenija i vrlo je vjerojatno da imaju i izravnog iskustva u vidu doživljajna ili činjenja elektroničkog nasilja, što je i pokazano u nekim istraživanjima (Velki i sur., 2017), pa su stoga postali oprezniji pri odavanju osobnih podataka. Što se tiče rizičnoga ponašanja na internetu djece i mladih u zemljama EU-a, Livingstone i Haddon (2009) pronalaze kako u prosjeku 75 % djece u dobi od 7 do 18 godina koristi se internetom na dnevnoj razini, a rizična ponašanja koja pritom prakticiraju su: davanje osobnih podataka i zaporke drugim (nepoznatim) osobama, prihvaćanje prijateljstava i poruka od nepoznatih osoba te nalaženje licem u lice s *online* prijateljima, a koje prethodno nisu upoznali, što je ujedno i najveći rizik za djetetovu sigurnost. Davanje zaporke i osobnih podataka najučestalije je i ono dostiže i do 50 % u državama s niskom razinom uporabe interneta (i informatičke pismenosti), dok su nalaženja licem u lice najrjeđa i o njima zapravo ne postoje egzaktni podaci, no autori procjenjuju da se oko 10 % djece i mladih odlučuje na taj korak.

Tablica 2. Prikaz odavanja zaporke za različite sudionike (svi sudionici, N=4662)

	srednjoškolci		studenti		djelatnici		ukupno	
zaporka	N	%	N	%	N	%	N	%
ne	2244	69,0	404	45,8	313	59,2	2961	63,5
da	1006	31,0	479	54,2	216	40,8	1701	36,5
Ukupno	3250	10,0	883	100,0	529	100,0	4662	100,0

* napomena: 197 djelatnika nije imalo pitanje o zaporci zbog sigurnosne politike tvrtke

Djelatnici različitih poduzeća statistički značajno manje odaju zaporku u odnosu na studente ($z=4,1$, $p<0,01$) što nas vodi zaključku da su studenti najrizičnija skupina glede odavanja zaporke u provedenom istraživanju. Taj rezultat može se objasniti paradoksom obrazovanja. Iako su studenti u prosjeku najobrazovanija skupina sudionika, znanje o informacijskoj sigurnosti i općenito informacijska pismenost za njih ne predstavlja čimbenik zaštite, već rizični čimbenik u kontekstu informacijske sigurnosti. Upravo svjesnost da imaju znanja o zaštiti podataka u informacijskim sustavima čini ih sklonijima odavanju vlastite zaporke jer smatraju da se njima ne može dogoditi krađa podataka u informacijskom sustavu. Navedeno su pokazala i prijašnja istraživanja uključujući i visoko obrazovane sudionike (Šolić i Ilakovac, 2009; Šolić i sur., 2009). Međutim, upravo ta lažno stvorena sigurnost čini ih najrizičnijom skupinom. Drugi je mogući razlog testiranje vlastitih mogućnosti nošenja s rizicima, tj. psihološki čimbenici koji se u literaturi ne spominju. Ipak, Starčević (2015) govori kako je kod uporabe interneta ključan psihološki čimbenik, tj. osobine ličnosti korisnika koje određuju njegovo ponašanje, što je katkada teško mijenjati edukacijom.

Nadalje, istražilo se i razlikuju li se sudionici istraživanja u rizičnom ponašanju na internetu s obzirom na dob, spol i otkrivanje zaporke.

Multivarijantna analiza varijance pokazala je postojanje dobnih ($F_{(2,4857)}=20,80$, $p<0,01$), spolnih ($F_{(1,4858)}=88,02$, $p<0,01$) i razlika u odavanju zaporke ($F_{(1,4858)}=72,12$, $p<0,01$) za skale i subskale UZPK-a.

U provedenom istraživanju sudionici su prema dobi bili podijeljeni u tri skupine, učenici srednjih škola, studenti i odrasle zaposlene osobe. Cilj istraživanja bio je i provjeriti razlikuju li se te tri dobne skupine međusobno u rizičnom ponašanju na internetu te u svojem znanju o informacijskoj sigurnosti. Rezultati su pokazali kako odrasli zaposlenici pokazuju najviše rizičnog ponašanja glede korištenja informacijskih sustava, ali istodobno i najviši stupanj znanja. Iza njih slijede studenti, a potom srednjoškolci s najmanjim stupanjem znanja, ali i rizičnog ponašanja. Iako je očekivano da će studenti pokazati najviši stupanj znanja, ali i rizičnog ponašanja, što je u skladu s njihovim odavanjem zaporke, ali i nekim prijašnjim istraživanjima (Velki,

Šolić i Nenadić, 2015; Velki i sur., 2017), moguće je da su zapravo samo oni zaposlenici koji imaju visoku informacijsku pismenost i često se služe računalom na radnom mjestu ispunili tražene upitnike dok ostali sudionici, koji su manje informacijski pismeni, nisu ni pristupili ispunjavanju upitnika, čemu u prilog idu i prijašnja istraživanja na visoko obrazovnim institucijama.

Analizirajući rezultate za različite subskale UZPK-a, vidimo slične obrasce ponašanja. Na subskali posuđivanja pristupnih podataka srednjoškolci i zaposlenici statistički značajno češće posuđuju pristupne podatke za razliku od studenata koji su očito prijašnjim iskustvom uporabe interneta, ali i razinom obrazovanja postali svjesniji mogućih rizika pri odavanju privatnih podataka. Na subskali održavanja računalnih sustava srednjoškolci su se pokazali kao najbolji, zatim zaposlenici, dok studenti najmanje vode računa o održavanju računala kojima se svakodnevno koriste. Za srednjoškolce je održavanje računala sastavni dio školskog gradiva pa ne čudi da o tome pokazuju najviša znanja, ali i kao najmlađa generacija koja je odrasla uz virtualni svijet, odnosno niz različitih informacijskih sustava, za njih je praksa održavanja sustava svakodnevna i uobičajena pojava, a ne nešto što se dodatno mora savladati i naučiti kao kod starijih sudionika. Na subskali uobičajenih rizičnih ponašanja korisnika računala najviše rizičnog ponašanja pokazali su zaposlenici, zatim studenti, a najmanje srednjoškolci. Iako bi se možda očekivalo da srednjoškolci, odnosno adolescenti, zbog razvojne životne dobi pokazuju najviše rizičnih ponašanja koji se odnose na informacijske sustave, upravo su oni skupina koja je od najranijih dana upoznata s različitim informacijskim sustavima (npr. pametni telefoni, tableti, prijenosna računala) i koja ima najviše izravnog iskustva u korištenju različitih aplikacija (npr. društvenih mreža, aplikacija za komunikaciju i sl.) kao i drugih programa (npr. različitih antivirusnih programa i dr.) što ujedno predstavlja sklop specifičnih znanja stečenih na temelju svakodnevne prakse i omogućuje im bolje snalaženje u svakodnevnom radu s informacijskim sustavima, za razliku od najstarije dobne skupine koja ta znanja stječu tijekom rada ili se moraju dodatno formalno obrazovati da bi se znali pravilno služiti informacijskim sustavima. Nisu na svim subskalama znanja dobivene statistički značajne razlike. Na subskali uvjerenja o sigurnosti računalnih podataka nisu dobivene dobne razlike, što znači da su bez obzira na dob sudionici podjednako uvjereni da im treće osobe mogu ukrasti privatne podatke s računala ili mobitela. Subskala stupnja sigurnosti računalne komunikacije pokazala je isti obrazac, odnosno najviši stupanj znanja o sigurnosti računalne komunikacije pokazali su zaposlenici, zatim studenti, a najmanje srednjoškolci. Srednjoškolci su skupina koja je najviše izložena komunikaciji u virtualnom svijetu, posebice na društvenim mrežama, pa s obzirom na količinu vremena koju provodi na internetu s vršnjacima ne čudi da su najmanje svjesni mogućih posljedica takvog tipa komunikacije (npr. krađa podataka, presretanje informacija koje prosljeđuju jedni drugima i sl.). Što se tiče važnosti pravilne pohrane podataka,

zaposlenici u odnosu i na studente i na srednjoškolce pokazuju višu razinu znanja, što je i očekivano. Zaposlenicima je pravilna pohrana nužna za svakodnevno obavljanje posla i vjerojatno iz toga proizlazi i shvaćanje koliko je važno imati sačuvane podatke s kojim se svakodnevno radi.

Zanimljivu činjenicu o rizičnom ponašanju na internetu korisnika pronalazi ENISA (2014). Naime, savjete o smanjenju rizika i povećanju sigurnosti korisnici uglavnom traže upravo na internetu pri čemu nerijetko krše uobičajena pravila zaštite kao što su odavanje zaporke ili adrese. Također, prema njihovu istraživanju, jednu od najnižih razina informatičko-komunikacijskih kompetencija imaju učitelji i nastavnici, zbog čega preporučuju revidiranje programa temeljnog profesionalnog obrazovanja učitelja na fakultetima te evaluaciju postojećih programa informatike u školama. Razlog tomu vide u nedostatku didaktičkih materijala u školama, tj. nedostatnoj opremljenosti škola te nepostojanju cjeloživotnih programa obrazovanja učitelja i nastavnika na temu elektroničke sigurnosti djece i mladih. Posljednje smatraju posebno problematičnim jer su zabilježili porast elektroničkih programa osposobljavanja i usavršavanja (webinara) kojima je tema elektroničkog nasilja i rizici korištenja interneta kod djece, dok izostaju programi cjeloživotnoga obrazovanja učitelja i nastavnika za njih same, tj. odrasle korisnike interneta. Upravo bi jačanje temeljnih kompetencija učitelja i nastavnika da se samostalno i što sigurnije koriste internetom trebala biti osnova na kojoj će se graditi sigurnost djece i mladih.

Također se istraživanjem željelo provjeriti razlikuju li se muškarci od žena u rizičnom ponašanju na intrenetu te u svojem znanju o informacijskoj sigurnosti.

Spolne razlike dobivene su samo za skalu znanja, odnosno subskalu važnosti pravilne pohrane računalnih podataka, pri čemu su ženske sudionice pokazale veće znanje od muških sudionika. Prijašnja su istraživanja jasno pokazala kako su žene u odnosu na muškarce opreznije i nepovjerljivije u otkrivanju privatnih podataka (Šolić, Velki i Galba, 2015; Velki i sur., 2017).

U svojemu istraživanju ENISA (2014) ne pronalazi statistički značajne razlike u uporabi interneta i rizičnim ponašanjima muškaraca i žena. Ipak, važno je reći kako je njihovo istraživanje bilo o učestalosti uporbae interneta bez naznačavanja o kojoj se komponenti radi (znanje, iskustvo ili nešto treće). Stoga se može zaključiti kako su potrebna dodatna istraživanja u odnosu na različite varijable kao što su osobine ličnosti ili kulturološka praksa uporabe interneta te svakako socijalni konformizam koji pritom sudionici istraživanja mogu iskazati.

Istražujući uporabu interneta u odnosu na spol sudionika istraživanja, Helsper (2010) zaključuje kako su razlike u spolu manje u razvijenijim društvima u kojima dječaci i djevojčice imaju podjednake prilike za stjecanje informatičkih kompetencija,

u kojima je i dječacima i djevojčicama internet jednako dostupan i u društvima u kojima se informatičko opismenjavanje dječaka i djevojčica provodi u jednakim odgojno-obrazovnim uvjetima. Ukoliko se uzmu u obzir njezina tumačenja, moglo bi se zaključiti kako je Republika Hrvatska još uvijek u procesu tranzicije društva iz tradicionalističkog u suvremeno.

Konačno, ispitalo se razlikuju li se osobe koje odaju svoju zaporku u odnosu na osobe koje ne odaju svoju zaporku u rizičnom ponašanju na internetu te u svojem znanju o informacijskoj sigurnosti. Prijašnja istraživanja jasno su pokazala kako velik broj osoba odaje svoju zaporku (Velki, Šolić i Nenadić, 2015).

Za sudionike koji odaju svoju zaporku u odnosu na one koji je ne odaju dobivena je statistički značajna razlika na skali rizičnog ponašanja računalnih korisnika, odnosno na subskali održavanja računalnih sustava, i to u neočekivanom smjeru. Osobe koje ne odaju zaporku pokazuju statistički značajno više rizičnog ponašanja, odnosno lošije održavaju osobne računalne sustave, što je u suprotnosti s prijašnjim istraživanjima (Šolić, Velki i Galba, 2015). Očito stvarno ponašanje odavanja zaporke ne igra značajnu ulogu u znanju o informacijskim sustavima, a ni u rizičnom ponašanju glede korištenja informacijskih sustava, već je odraz ponašajnog stila osoba. Odnosno, kako kaže Starčević (2015), uporaba interneta i stilova ponašanja u značajnoj je mjeri određeno osobinama ličnosti. Treba napomenuti da istraživači nisu bili u mogućnosti provjeriti jesu li sudionici zaista dali svoju aktivnu zaporku pa je moguće da su neočekivani rezultati dobiveni zbog davanja neiskrenih odgovora sudionika (odnosno odavanja lažne zaporke).

Naposljetku, provedenim istraživanjem htjeli smo ispitati odnos između znanja o informacijskoj sigurnosti i rizičnog ponašanja računalnih korisnika. Neka prijašnja istraživanja govore u prilog tome da, što osoba posjeduje veće znanje o informacijskoj sigurnosti, sklonija je rizičnije se ponašati (Šolić i Ilakovac, 2009; Šolić, i sur., 2009; Velki i sur., 2017).

U Tablici 3. prikazani su rezultati korelacijske analize za sve skale i subskale UZPK-a. Skala rizičnog ponašanja računalnih korisnika i Skala znanja o informacijskoj sigurnosti u maloj su, ali statistički značajnoj povezanosti što znači da osobe koje imaju višu razina znanja ujedno čine i više rizičnih ponašanja.

Tablica 3. Povezanost skala i subskala UZPK-a (svi sudinici, N=4859)

	SRP	SZS	PP	OS	RP	SS	US	VS
Skala rizičnog ponašanja računalnih korisnika – SRP	-	,200**	,585**	,691**	,624**	,050**	-,048**	,369**
Skala znanja o informacijskoj sigurnosti – SZS		-	,075**	,207**	,058**	,567**	,675**	,660**
Subskala posuđivanja pristupnih podataka – PP			-	,034*	,429**	,032*	-,080**	,181**
Subskala održavanja osobnih računalnih sustava – OS				-	-,039**	-,031*	,057**	,353**
Subskala uobičajenih rizičnih ponašanja korisnika računala – RP					-	,120**	-,120**	,117**
Subskala stupnja sigurnosti računalne komunikacije – SS						-	,118**	,028
Subskala uvjerenja o sigurnosti računalnih podataka – US							-	,174**
Subskala važnosti pravilne pohrane računalnih podataka – VS								-

** p < 0,01; * p< 0,05

Općenito je isti trend dobiven i za većinu subskala. Za subskalu uobičajenih rizičnih ponašanja dobivena je vrlo mala statistički značajna negativna povezanost sa subskalom održavanja računalnih sustava i sa subskalom stupnja sigurnosti računalne komunikacije, što bi značilo da osobe koje bolje održavaju računalne sustave ujedno pokazuju i više rizičnih ponašanja na intrenetu te manje znanja glede sigurne računalne komunikacije. Subskala uvjerenja o sigurnosti računalnih podataka pokazala je malu statistički značajnu negativnu povezanost sa skalom rizičnog ponašanja računalnih korisnika te subskalama posuđivanja pristupnih podataka i uobičajenih rizičnih ponašanja. Osobe koje imaju veća znanja i uvjerenja o sigurnosti računalnih podataka ujedno pokazuju manje rizičnih ponašanja, odnosno rjeđe posuđuju vlastite pristupne podatke drugim osobama te općenito iskazuju nižu razinu uobičajenih rizičnih ponašanja računalnih korisnika. Iako u nekim slučajevima znanje, odnosno svjesnost o informacijskoj sigurnosti, može biti zaštitni čimbenik za rizična ponašanja na internetu ipak se u većini slučajeva viša razina znanja pokazala kao rizik za dodatna pro-

blematična ponašanja na intrenetu. Taj je trend u skladu s rezultatima prijašnjih studija koje su pokazale na različitim dobnim uzorcima kako osobe koje imaju više znanja i svjesnije su moguće opasnosti ujedno se i rizičnije ponašaju pri uporabi informacijskih sustava (Šolić i Ilakovac, 2009; Šolić, i sur., 2009; Velki i sur., 2017). Samo znanje i svijest o tome da osoba nešto zna stvara lažni osjećaj sigurnosti u računalnih korisnika te pridonosi tomu da ne paze i ne pridržavaju se naučenih pravila o informacijskj sigurnosti.

3.4. ZAKLJUČAK

Provedenim istraživanjem utvrđen je obrazac ponašanja različitih sudionika o informacijskoj sigurnosti. Zaposlenici pokazuju najviši stupanj znanja, ali i rizičnog ponašanja, iza njih odmah slijede studenti, dok srednjoškolci najmanje znaju o informacijskoj sigurnosti, ali pokazuju i najmanje rizičnih ponašanja korisnika računalnih sustava. Dobivena je i pozitivna povezanost između skala znanja i skala rizičnog ponašanja, odnosno što pojedinci pokazuju viši stupanj znanja o informacijskoj sigurnosti, ujedno pokazuju i viši stupanj rizičnog ponašanja računalnih korisnika. Navedeno ide u prilog činjenici da visoko znanje ne predstavlja zaštitu od rizičnog ponašanja na internetu odnosno da su u prevenciji rizičnog ponašanja na internetu potrebne dodatne mjere, a ne samo osviještenost sudionika i njihova razina znanja.

Dobiveni rezultati u značajnoj su mjeri slični onima koji su dobiveni u istraživanjima provedenim u zemljama EU-a (ENISA, 2014) u kojima Republika Hrvatska nije prethodno sudjelovala. Praktične implikacije koje se pritom nameću mogu se podijeliti u tri velike skupine: (1) kulturni kontekst – stilovi odgoja u pojedinim kulturama, (2) zakonski okviri – zakonska regulacija uporabe interneta i (3) odgojno-obrazovni kontekst – opremljenost škola i prisutnost programa informatike. Zakonska se ograničenja za Republiku Hrvatsku odnose na sprječavanje distribucije neprimjerenih sadržaja i sadržaja koji podliježu autorskim pravima, no posebnih zakonskih ograničenja nema te su česte internetske prijevare e-poštom u obliku dobitaka, nasljeđivanja i sl. što pružatelji internetskih usluga ne filtriraju u dovoljnoj mjeri. Kulturni kontekst odnosi se na stilove odgoja i viđenje djeteta u pojedinim kulturama. Tako se u zapadnim i skandinavskim kulturama djeca vide kao aktivni građani koji participiraju u svojemu društvu te se djeca i mladi u navedenom području u većem postotku koriste internetom bez nadzora roditelja. Također, u tim su zemljama češće prisutni tzv. *child-friendly* alati kojima djeca mogu nesmetano pretraživati internet bez straha roditelja da će tijekom pretraživanja naići na neprimjerene sadržaje. S druge strane, u državama koje su tradicionalno orijentirane (južna i istočna Europa),

građani se općenito u manjem postotku koriste internetom, njihova djeca manje vremena provedu na internetu, ali kada jesu, nemaju mogućnost softverske zaštite od nepoželjnih sadržaja. Kulturni kontekst uvelike određuje stilove ponašanja korisnika svih kronoloških dobi što bi i u budućnosti bilo zanimljivo propitati. Naposljetku – ključ je odgojno-obrazovni kontekst što se može naslutiti i iz dobivenih rezultata istraživanja. Prisutnost primjerenih i suvremenih programa informatike početna je razina u podizanju informacijske pismenosti djece i mladih. Uvidom u udžbenike informatike vidljivo je kako su prve lekcije uglavnom usmjerene na dijelove računala, uključujući diskete, iako istraživanje Livingstonea i Haddona (2009) pokazuje kako se djeca počinju koristiti internetom vrlo rano, čak i u prvim trima godinama života. To znači, kada se počnu informatički obrazovati u osnovnim školama, veliki broj djece već ima višegodišnje iskustvo uporabe interneta. U prilog potrebi kvalitetnijih programa informatike, već od najranije dobi, govori i statistika uporabe interneta na razini EU-a: 60 % djece u dobi od 6 do10 godina koristi se internetom te taj postotak raste sve do 86 % za dob od 15 do 17 godina. Prosječno 75 % djece i mladih u dobi od 7 do 18 godina koriste se internetom, dok je odraslih korisnika još više (84 %).

3.5. PREPORUKE

Stoga bi se preporuke za rad na temelju provedenoga istraživanja mogle razvrstati u odnosu na rizike koji su istraživanjem zabilježeni, a to su u prvome redu zaštita osobnih podataka i praćenje protokola sigurnosti. U tom dijelu moguće je činiti sljedeće:

- ukloniti osobne podatke s profila ili korisničkih računa (ime, prezime, adresa, detalji o školovanju, fotografije i zaporke)
- kod kreiranja zaporke kombinirati velika i mala slova i brojeve
- za različite korisničke račune osmisliti različita imena i zaporke
- osigurati pristup korisničkom računu sigurnosnim pitanjem
- instalirati programe zaštite računala i redovito održavati sustav
- održavati računalo – brisati nepotrebne dokumente i sadržaje što će rasteretiti memoriju računala i omogućiti bolji rad
- koristiti nadimak/alias u komunikaciji, koristiti avatare
- u slučaju neprimjerene komunikacije blokirati osobu ili ju prijaviti administratoru

- kod pretraživanja sadržaja koristiti se naprednim postavkama ili ključnim riječima kojima će se suziti izbor sadržaja i otvaranja linkova
- instalirati dodatne programe koji omogućuju zaštitu ili blokiranje neprimjerenih sadržaja
- provjeravati sigurnost mrežnih stranica i profile administratora
- kod kupovine internetom koristiti se provjerenim stranicama i/ili karticom koja ima samo onaj iznos koji je potreban za kupovinu (neka to ne budu kartice tekućih računa ili kartica na kojima imate ušteđevinu)
- informirati se o potencijalnim prijetnjama u odnosu na mrežne stranice koje posjećujete
- prihvaćanje poruka i ***online*** **prijateljstava** samo od poznatih osoba, tj. osoba koje poznajete i u stvarnom životu
- provjeriti štetnost sadržaja koje primate s molbom za prosljeđivanjem drugim korisnicima
- poštovati pravila komunikacije na portalima, grupama na društvenim mrežama i drugim oblicima virtualnog okupljanja (*chat rooms*, blogovi, forumi i sl.).

Navedene preporuke temeljni su preduvjeti sigurnosti, no stalni oprez i kontrola podataka potrebni su kako bi se održala primjerena razina sigurnosti i reducirali različiti oblici rizičnog ponašanja na internetu.

3.6. LITERATURA

Crossler, R. E., Johnston, A. C., Lowry, P. B, Hu, Q., Warkentin, M. i Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32,* 90-101.

Dell'Amico, M., Michiardi, P. i Roudier, Y. (2010). Password Strength: An Empirical Analysis. *Proceedings IEEE INFOCOM,* 1-9.

ENISA (2014). *Roadmap for NS education programmes in Europe.* Madrid: ENISA.

Haley, K. (2011). *Information robbery - The 2011 Internet security threat report. InfoSecToday*. Preuzeto s http://www.infosectoday.com/Articles/Information_ Robbery.htm, 3. 5. 2018.

Helsper, E. (2010). Gendered internet use across generations and life stages. *Communication Research, 37,* 352-374.

Kelley, P. G. i sur. (2012). Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms. *IEEE Symposium on Security and Privacy,* 523-537.

Kwang, K. i Choo, R. (2011). The cyberthreat landscape: Challenges and future research directions. *Compures & Security, 30,* 719-731.

Livingstone, S. i Haddon, L. (2009). *EU Kids online: Final report.* London: EC safer Internet/EU Kids online.

Lukasik, S. J. (2011). Protecting Users of the Cyber Common. *Communications of the ACM, 54*, 54-61.

Mitnick, K. D., Simon, W. L. i Wozniak S. (2002). *The art of deception: Controlling the human element of security*. Indianapolis, Indiana, USA: Wiley Publishing, Inc.

Sasse, M. A., Brostoffand, S. i Weirich, D. (2001). Transforming the 'weakest link' - a human/ computer interaction approach to usable and effective security. *BT Technology Journal, 19,* 122-131.

Selmar, M. i Tibert, V. (2018). Reducing consumer risk in electronic marketplaces. *Computer in Human Behavior, 86,* 205-217.

Starčević, V. (2018). Problematic Internet use, reward sensitivity and decision making. *Australian and New Zaeland Journal of Psychology, 49,* 937-938.

Šolić, K. i Ilakovac, V. (2009). Security perception of a portable PC user (The difference between medical doctors and engineers): a pilot study. *Medicinski Glasnik Ljekarske komore Zeničko-dobojskog kantona, 2,* 261-264.

Šolić, K., Ilakovac, V., Marusic, A. i Marusic, M. (2009). Trends in using insecure e-mail services in communication with journal editors. *Proceedings PRC*, 50.

Šolić, K., Očevćić, H. i Baležević, D. (2015). Survey on Password Quality and Confidentiality. *Automatika, 56*(1), 69–75.

Šolić, K., Velki, T. i Galba, T. (2015). Empirical study on ICT system's users' risky behavior and security awareness. *Hrvatska udruga za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku – MIPRO proceedings,* 1623-1626.

Velki, T., Šolić, K., Gorjanac, V. i Nenadić, K. (2017). Empirical study on the risky behavior and security awareness among secondary school pupils - validation and preliminary results. *Hrvatska udruga za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku – MIPRO proceedings,* 1496-1500.

Velki, T., Šolić, K. i Nenadić, K. (2015). Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZRPKIS). *Psihologijske teme, 24*(3), 401-424.

Velki, T., Šolić, K. i Očevćić, H. (2014). Development of Users' Information Security Awareness Questionnaire (UISAQ) - Ongoing Work. *Hrvatska udruga za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku – MIPRO proceedings*, 1564-1568.

Voyiatzis, A. G., Fidas, C. A., Serpanos, D. N. i Avouris, N. M. (2011). An Empirical Study on the Web Password Strength in Greece. *15th Panhellenic Conference on Informatics*, 212-216.

Wanli, M., Campbell, J., Tran, D. i Kleeman, D. (2010). Password Entropy and Password Quality. *4th International Conference on Network and System Security,* 583-587.

Ivana Borić Letica, mag. psych., doktorandica

Fakultet za odgojne i obrazovne znanosti
Sveučilišta Josipa Jurja Strossmayera u Osijeku

izv. prof. dr. sc. Tena Velki

Fakultet za odgojne i obrazovne znanosti
Sveučilišta Josipa Jurja Strossmayera u Osijeku

4. RIZIČNA PONAŠANJA DJECE I MLADIH NA INTERNETU

Sažetak

Današnja djeca i mladi koriste se internetom za komunikaciju, zabavu, učenje i informiranje. Unatoč prednostima, internet predstavlja i mogućnost razvoja niza problema. Rezultati istraživanja pokazuju kako većina djece i mladih ima profil na društvenoj mreži na kojem neselektivno dijele osobne informacije, čak 30 % njih uspostavilo je kontakt na internetu s nekim koga ne poznaje u stvarnom životu, a 9 % ih je doživjelo zloupotrebu osobnih podataka. Odavanje manjeg broja osobnih podataka pri instalaciji aplikacija, uporabom društvenih mreža, odgovaranjem na e-poštu i sl. može dovesti do materijalnih gubitaka, ugrožavanja sigurnosti osobe i gubitka privatnosti. Kombinacija impulzivnosti, naivnosti, sklonosti da svoje vještine uporabe interneta precjenjuju te slabo razvijene vještine donošenja odluka djecu i mlade čini populacijom koja je u današnje vrijeme najviše izložena riziku, prijevarama, zlostavljanju, ponižavanju, uznemiravanju i neprimjerenim sadržajima na internetu. Nepoznavanje pravila sigurne upotrebe interneta, rizično ponašanje na internetu i prekomjerna upotreba interneta ozbiljni su problemi jer istraživanja sugeriraju kako mogu uzrokovati pad samopoštovanja, tjeskobu, depresiju i zanemarivanje školskih obaveza.

Brojne teorije objašnjavaju utjecaj medija na rizična ponašanje djece, npr. Opći model agresivnosti Andersona i Bushmana (2001), Berkowitzeva kognitivno neoasocijalna teorija (1993), Teorija skripti Huesmanna i Erona (1986), Teorija simboličkog interakcionizma (Catalano, Kosterman, Hawkins, Newcomb i Abbott, 1996), Model različite podložnosti utjecaju medija (Valkenburg i Peter, 2013), no problematika korisnika koji na internetu ugrožavaju svoju sigurnosti i privatnost tek je u začecima. Istraživanja pokazuju kako su muški spol, loša obiteljska kohezija, slaba vršnjačka pripadnost i neke osobine ličnosti (neuroticizam, nesavjesnost, traženje uzbuđenja, impulzivnost) povezane s različitim oblicima rizičnih ponašanja na internetu. Oni koji se češće koriste internetom te oni koji su svjesniji rizika, susretat će se s više rizičnih situacija. Također, oni koji internet rabe zbog zabave, upoznavanja i komunikacije s nepoznatim osobama, u većem su riziku od ugrožavanja vlastite sigurnosti i privatnosti.

Zbog široke dostupnosti interneta, roditeljima je često teško nadzirati online aktivnosti svoga djeteta. U literaturi postoje razne klasifikacije roditeljskih medijacija, od metoda aktivnog posredovanja, posredovanja koje obuhvaćaju zadavanje pravila ponašanja do praćenja aktivnosti djeteta i postavljanja tehničkih ograničenja. Iako ne postoji konsenzus koliko je koja strategija učinkovita, istraživanja sugeriraju kako uključenost roditelja u aktivnosti djeteta na internetu može utjecati na smanjenje rizičnih situacija s kojima se dijete susreće.

4.1. TEORIJSKA OBJAŠNJENJA RIZIČNIH PONAŠANJA DJECE I MLADIH NA INTERNETU

Mediji su važan dio svakodnevnice većine djece i mladih. Uporabom medija mladi komuniciraju, izražavaju se, zabavljaju se, koriste ih u obrazovanju i učenju. Međutim, meta-analiza istraživanja Andersona i Bushmana (2001) ukazuje na povezanost medijskog nasilja i vršnjačkog nasilja. Djeca izloženija medijskom nasilju u ranoj školskoj dobi kasnije su verbalno i fizički agresivnija. Za objašnjenje rizičnog ponašanja adolescenata može poslužiti teorija socijalnog učenja (Bandura, 1986) prema kojoj uvijek oponašamo modele koji nam se čine privlačnima bez obzira na to jesu li njihova ponašanja pozitivna ili negativna. Dakle, djeca oponašaju modele – televizijske likove za koje smatraju da imaju poželjne osobine. Agresivni televizijski modeli često su za svoje ponašanje nagrađeni, odnosno nasilni načini rješavanja problema pomažu im u ostvarenju plemenitih ciljeva. Dugotrajna izloženosti nasilnim televizijskim sadržajima može rezultirati stvaranjem vjerovanja i stavova koji utječu na ponašanje pojedinca (Livazović, 2009). Istraživanja sugeriraju da učestala izloženost nasilju u videoigricama može utjecati na djecu tako što ih desenzitizira na nasilje, odnosno smanjuje njihove emocionalne odgovore na nasilne podražaje. Tom fenomenu pridonosi osjećaj da žrtva zapravo ne pati jer u igricama nisu prikazane posljedice nasilja i bol žrtava (Anderson i Bushman, 2001). Također, Hamer, Konijn i Keijer (2014) utvrdili su kako postoji pozitivna povezanost između izloženosti nasilnom sadržaju u medijima i činjenja nasilja na internetu.

Teorija priminga ili Kognitivno-neoasocijativna teorija (Berkowitz, 1993) pretpostavlja kako u interakciji s okolinom u mozgu nastaju povezane kognicije, osjećaji i tendencije prema određenim oblicima ponašanjaa – mreže asocijativnih neuronskih veza. Kada medijski sadržaj, koji predstavlja podražaj, potakne neuronsku mrežu, u njoj stvara specifičan niz kognicija. Opetovanim djelovanjem podražaja formira se automatski proces koji utječe na interpretaciju svih novih podražaja. Takvi procesi povećavaju vjerojatnost pojavljivanja agresivnog ponašanja koje pojedinac vidi u medijima te oni internalizacijom postaju kronično aktivni.

Teorija skripti (Huesmann i Eron, 1986; Tomkins, 1987) pretpostavlja da djeca i mladi iz medija preuzimaju i razvijaju tzv. skripte rješavanja problema. Navedena teorija objašnjava kako obrađujemo informacije primljene iz medija. Skripte predstavljaju mentalne programe koji su pohranjeni u pamćenju, a kojima se osoba služi pri rješavanju problema. Skripte sadrže informacije o očekivanom tijeku događaja i učinkovitom odgovoru na njih, tj. našem ponašanju usmjerenom prema okolini. Skripte koje često izvodimo, češće će biti temelj našeg ponašanja, osobito ako se temelje na onom što smatramo poželjnim ponašanjem. Medijski sadržaji predstavljaju

važan model učinkovitog rješavanja problema, tj. poželjnog ponašanja (Livazović, 2011).

Opći model agresivnosti integrira ideje kognitivne teorije učenja, priming koncepta i teoriju skripti s tezom stimulacije i osniva se na prijašnjim modelima ljudske agresivnosti (Anderson i Bushman, 2001). Nasilno ponašanje utemeljeno je na aktivaciji spoznajnih struktura pohranjenih u pamćenju (skripte i sheme) koje su povezane s agresivnošću. Situacijske odrednice (npr. nedavna izloženost nasilju u medijima) utječu na agresivno ponašanje tako što djeluju na trenutačno unutarnje stanje pojedinca (njegove kognitivne i afektivne procese). Nasilje u medijima jača agresivne spoznaje, tj. agresivne skripte i sheme, povećava uzbuđenje i utječe na pojavu agresivnih afektivnih stanja pojedinca (Anderson i Bushman, 2001). Djeca od najranijeg djetinjstva uče opažati, promišljati, prosuđivati i reagirati na događaje u svojoj okolini. Svako nasilje prikazano u medijima predstavlja učenje koje vodi uvježbavanju i jačanju spoznajnih struktura. Dugoročni učinci izloženosti nasilnim sadržajima za posljedicu imaju razvoj, ponavljanje i automatizaciju agresivnih shema i ponašajnih skripti. Ponavljanom izloženošću određenim podražajima sheme i skripte postaju sve složenije, stabilnije, raznovrsnije i otpornije na promjenu. Kao posljedica javljaju se desenzitizacija, tolerancija na nasilje i opća sklonost rizičnom ponašanju kao modelu rješavanja problema i stilu socijalnog djelovanja (Livazović, 2009).

Teorija simboličkog interakcionizma (Catalano i sur., 1996) pretpostavlja kako je za izgradnju identiteta potrebno preuzeti određene društvene uloge te kako društvenim interakcijama, pozitivnim i negativnim potkrepljenjima okoline, razvijamo emocionalne, kognitivne i ponašajne vještine. Izostankom pozitivnog potvrđivanja poželjnih ponašanja od strane značajnih drugih (obitelj, vršnjaci), dijete oblikuje stav kako mnogo ne gubi antisocijalnim ponašanjem. Pojedinac procjenjuje koliko gubi narušavanjem socijalnih odnosa, a koliko dobiva antisocijalnim ponašanjem (Catalano i sur., 1996). Proces socijalnog učenja odvija se u tri faze – prva je faza internalizacija pravila ponašanja nakon koje slijedi faza održavanja, faza osnaživanja i potvrđivanja pravila, dok je posljednja faza prisjećanja i manifestiranja kojom se internalizirani obrasci prikazuju u stvarnom ponašanju i postaju trajni dio ličnosti. U antisocijalnom razvojnom putu dijete prima inicijalnu pozitivnu potvrdu (ili izostanak reakcije) zbog antisocijalnog ponašanja, zatim se veže uz osobu, grupu ili instituciju koja sudjeluje u antisocijalnom ponašanju te razvija vjerovanje u antisocijalne vrijednosti. Ponovljeni prikazi nasilja u medijima utječu na djetetovu sposobnost dosjećanja nasilnih oblika ponašanja. Što je kontekst u kojem se odvija nasilno ponašanje sličnije djetetovoj situaciji, ono će ga vjerojatnije internalizirati kao poželjan oblik reagiranja u socijalnim situacijama. Mediji često jačaju negativni razvojni obrazac prikazujući rizična ponašanja kao poželjna (nasilje, ovisnosti, rizično seksualno ponašanje itd.) (Livazović, 2011).

Livingstone i Millwood Hargrave (2006) navode kako se istraživanja trebaju usmjeriti na prepoznavanje niza čimbenika koji interakcijski utječu na objašnjavanje određenih društvenih problema. Mediji uvijek djeluju u međuodnosu s različitim društvenim utjecajima. Stoga se posljedice moraju mjeriti praćenjem postupnih promjena u društvenim normama i običajima tijekom vremena.

Model različite podložnosti utjecaju medija (The Differential Susceptibility to Media Effects Model – DSMM; Valkenburg i Peter, 2013) suvremeni je model koji objašnjava utjecaj medija na ponašanje i temelji se na već postojećim, dobro poznatim teorijama poput Bandurine teorije socijalnog učenja (1986), Berkowitzeve neoasocijativne teorije (1993), Općeg modela agresivnosti (Anderson i Bushman, 2001) i sl. Prethodnim teorijama nedostaje konsenzus oko povezanosti nemedijskih i medijskih varijabli koje utječu na podložnost medijskim sadržajima. Spomenuti model medijske učinke promatra kao namjerne ili slučajne kratkoročne ili dugoročne promjene unutar spoznaje, emocija, stavova, uvjerenja, fiziologije i ponašanja koje proizlaze iz upotrebe medija. Upotreba medija široko je definirana kao upotreba različitih vrsta medija (npr. TV, računalne igre), sadržaja (npr. zabava, oglašavanje) i tehnologije (npr. društvene mreže).

Valkenburg i Peter (2013) razlikuju podložnost/sklonost (engl. *suspectibility*) od ranjivosti/vulnerabilnosti (engl. *vulnerability*). Podložnost se odnosi na reaktivnost kada određene karakteristike djeteta vode pozitivnim ili negativnim posljedicama ovisno o okolini, a ranjivost na to da će djeca koja imaju određene karakteristike biti u većem riziku od negativnih posljedica pri čemu im pozitivno okruženje neće pomoći koliko drugoj djeci.

Upotreba medija može se predvidjeti na temelju individualnih karakteristika osobe kao što su spol, stupanj razvoja ili temperament. Također, upotreba određenih medija posreduje kauzalnu povezanost između tih individualnih karakteristika osobe i ishoda, odnosno utjecaja koje će mediji imati na pojedinca. Model konceptualizira i indirektni učinak mentalnih i fizioloških procesa koji se pojavljuju tijekom korištenja medija kao medijatora između upotrebe medija i učinka medija. Npr. izloženost pobuđujućim sadržajima povećava pažnju i fiziološku pobuđenost korisnika koje zauzvrat stimuliraju dosjećanje istih sadržaja ili stavove prema njima. Također, određeni medijski sadržaji mogu potaknuti upotrebu medija. Na primjer, upotreba društvenih medija adolescenata može poboljšati njihovo samootkrivanje intimnih informacija prijateljima (medijatorski učinak medija) što zauzvrat utječe na njihovu percipiranu kvalitetu tih prijateljstava te upotrebu istih medija (medijatorski utjecaj medija drugog reda). Isto tako, informativna upotreba medija potiče interpersonalnu raspravu (medijatorski učinak medija) što zauzvrat povećava sudjelovanje u raspravama na internetu (medijatorski utjecaj medija drugog reda). Posljedice upotrebe medija

utječu na njhovu upotrebu, dakle upotreba medija ima transakcijski učinak – upotreba nasilnih medija adolescenata može povećati njihova agresivna nastojanja koja potom mogu stimulirati njihovu upotrebu medija u svrhu gledanja nasilnih sadržaja (Anderson i Bushman, 2001). Što više mladi gledaju pornografske sadržaje, to će se više na njih naviknuti i promijeniti svoje negativno mišljenje o njima te ih u konačnici češće gledati. Spmenuti model pretpostavlja da mladi na temelju svojih osobina biraju određene medije koji potom utječu na njihovo samopoimanje (Valkenburg i Peter, 2013).

Dobar model za objašnjenje medijskih utjecaja na pojedinca treba objašnjavati zašto su neki pojedinci podložniji medijskom utjecaju, kako upotreba medija utječe na te pojedince i kako se učinci medija mogu povećati ili poništiti (Valkenburg i Peter, 2013). Model različite podložnosti utjecaju medija odbacuje univerzalno gledanje na medije kao na loš ili dobar utjecaj te opisuje tri tipa nemedijskih varijabli koje mogu poslužiti kao prediktori upotrebe i utjecaja medija.

1) Razvojna podložnost podrazumijeva varijable djetetova socijalnog, emocionalnog i kognitivnog razvoja. Medijski sadržaji imaju jači ili slabiji utjecaj na različite aspekte djetetova razvoja. Pojedinci na određenoj razvojnoj razini podržavaju medijski sadržaj koji je njima zanimljiv i razumljiv, odnosno optimalan za njihovu razvojnu razinu. Djeca u dobi od dvije do tri godine birat će sadržaje sporijeg tempa te one koji su im poznatiji, predškolci će birati avanturističke sadržaje bržeg tempa, djeca osnovnoškolske dobi realistične sadržaje, a adolescenti sadržaje koje karakterizira humor ili rizično ponašanje. Mlađa djeca ulažu manje kognitivnog napora pri interpretaciji medijskog sadržaja te ih isti više uznemiruju (Valkenburg i Cantor, 2000).

2) Dispozicijska podložnost odnosi se na varijable kao što su: spol, temperament, osobine ličnosti (npr. neuroticizam, agresivnost, traženje uzbuđenja), stavovi, motivacija i vrijednosti, a predstavljaju predispoziciju za upotrebu medija te moderiraju utjecaj medija. Kod pojedinaca koji imaju sklonost više upotrebljavati medije, to je nastojanje u vezi s njihovim crtama ličnosti, razvojnim stupnjem te normama koje prevladavaju u društvenim skupinama kojima pripadaju. Model naglašava stabilne dispozicijske varijable nasuprot promjenjivim kao što su npr. raspoloženja. Pojedinci biraju medijske sadržaje koji se mnogo ne razlikuju od njihovih stavova, vrijednosti, kognicija, emocija i ponašanja. Također, dispozicijski kongruentni medijski sadržaj snažnije će djelovati na pojedinca od medijski nekongruentnog sadržaja jer će biti procesuiran brže i učinkovitije budući da se može povezati sa shemama pojedinca (Lang, Potter i Balls, 2009).

3) Socijalnu podložnost predstavljaju svi čimbenici socijalnog konteksta koji mogu utjecati na djetetovu upotrebu medija, što uključuje roditelje, prijatelje, vršnjake, školski sustav i kulturne norme (Valkenburg i Peter, 2013). Učinak je medija

transakcijski, odnosno osim samog sadržaja i vremena provedenog uz medije bitna je i interakcija pojedinca s jednom ili više drugih osoba (posebice roditelja, prijatelja i bliskih osoba) za vrijeme upotrebe medija. Roditelji i vršnjaci mogu ograničiti ili potaknuti izloženost određenim televizijskim programima ili igricama, a i škole i kulturne norme mogu zabraniti ili poticati upotrebu određenih medijskih sadržaja (Schultz, Izard, Ackerman. i Youngstrom, 2001).

Spomenuti model pretpostavlja kako traženje uzbuđenja može biti prediktorom gledanja nasilnih sadržaja u adolescenciji, ali ne i u djetinjstvu ili odrasloj dobi. Roditeljske strategije kontrole mogu biti uspješne u djetinjstvu, ali ne i u adolescenciji (Valkenburg i Peter, 2013). Varijable podložnosti medijskim utjecajima prediktori su, ali i moderatori, kao prvo predviđaju upotrebu medija, ali utječu i na odgovore, odnosno reakcije na medijske sadržaje.

Model pretpostavlja kako su učinci medija indirektni; tri vrste odgovora na medijske sadržaje medijatori su veze između upotrebe medija i utjecaja medija, a to su: (a) kognitivni odgovori – pažnja i zapamćivanje, odnosno ulaganje kognitivnog napora u razumijevanje medijskog sadržaja, zauzimanje tuđe perspektive i sl., (b) emocionalni odgovori – afektivni odgovori na medijske sadržaje, empatija prema likovima i (c) fiziološka pobuđenost. Učinak medija najdugotrajniji je i najočitiji kada su kognitivni, emocionalni i fiziološki odgovori jaki (Anderson i Bushman, 2001). Kada pojedinci primijete da medijski sadržaji kod njih izazivaju prejake odgovore, tada koriste samoregulirajuće strategije, npr. odmiču pogled s ekrana ili mijenjaju značenje promatranog sadržaja kako bi umanjili njegov utjecaj. Poznato je kako će nasilni sadržaj izazvati jače odgovore od tužnog sadržaja. Međutim, postavlja se pitanje jesu li odgovori pobuđeni nasilnim sadržajima i kvalitativno drukčiji. Buduća bi istraživanja trebala otkriti koji medijski sadržaji vode do kojih odgovora, kako ti odgovori variraju s obzirom na individualne karakteristike te koja kombinacija odgovora rezultira kakvom vrstom medijskog utjecaja (Valkenburg i Peter, 2013).

Interpretacija medijskog sadržaja ovisi o spolu, socioekonomskom statusu, rasi i dobi (Livingstone, 1998), međutim malo je istraživanja koja su uzela u obzir socijalni kontekst tijekom korištenja medija, a gotovo da nema istraživanja koja ispituju moderacijsku ulogu socijalno podložnih varijabli (Valkenburg i Peter, 2013). Socijalni konteksti na mikro, mezo i makro razini potiču ili inhibiraju upotrebu medija (McDonald, 2009). Društveni se utjecaji javljaju na dva načina: namjerno, kada roditelji, braća i sestre, vršnjaci, škole ili institucije ograničavaju ili reguliraju upotebu medija (Nathanson, 2001) ili otvorenije, normama koje prevladaju u obitelji, vršnjačkim skupinama ili supkulturama (McDonald, 2009). Socijalni kontekst može moderirati učinak medija tijekom zajedničke upotrebe određenih medija. Roditelji mogu namjerno utjecati na poruku koja se prenosi medijima ako npr. objašnjavaju sadržaj i

poruku koju mediji prenose djetetu (Nathanson, 2001). Također, tijekom zajedničke upotrebe medija može se dogoditi i „emocionalna zaraza" (McDonald, 2009) jer su korisnici medija vrlo osjetljivi na tuđe stavove, raspoloženja i emocionalne reakcije pa stoga vlastite kognicije, emocije i uzbuđenje mogu pojačati ili smanjiti ovisno o stanju osobe s kojom se zajednički koriste medijem.

Istraživanje Velki i Duvnjak (2017) bavilo se testiranjem tog modela. Rezultati su pokazali kako je učestalija upotreba interneta povezana s većim stupnjem impulzivnosti, nižom razinom afektivne empatije, slabijim školskim uspjehom, većim brojem prijatelja i boljom vršnjačkom prihvaćenosti. Stupanj impulzivnosti jače se vezuje uz igranje računalnih igrica i uz upotrebu interneta nego uz gledanje televizije, dok je stupanj afektivne empatije u jačoj vezi s igranjem računalnih igrica nego s upotrebom interneta. Osjećaj vršnjačke prihvaćenosti povezaniji je s igranjem računalnih igrica i upotrebom interneta nego s gledanjem televizije, dok je školski uspjeh u jačoj korelaciji s gledanjem televizije nego s upotrebom interneta. Što se tiče prihvaćenosti i broja prijatelja, neki autori (Bargh i McKenna, 2004) navode kako upotreba interneta može biti negativno povezana s problemima prilagodbe, pri čemu se socijalno kompetentne osobe jednako ponašaju prema okruženju na internetu kao i prema bilo kojem drugom okruženju u kojem ostvaruju interakciju s prijateljima i proširuju socijalnu mrežu. Rezultati pokazuju kako gotovo 40 % učenika provodi vrijeme s prijateljima u igranju računalnih igrica. Poznato je kako postoji mnogo grupnih računalnih igrica koje se igraju na internetu (npr. na Facebooku) u dogovoru s prijateljima te se djeca na takav način ujedno i druže. Stoga ne iznenađuje činjenica kako se takvi učenici osjećaju prihvaćeno od strane vršnjaka. Shaw i Gant (2002) uočili su da se s povećanjem upotrebe takvih sredstava znatno smanjio osjećaj usamljenosti, ali i da je došlo do povećanja osjećaja samopoštovanja. Veza školskog uspjeha i vremena provedenog na internetu moderirana je vrstom sadržaja koje djeca traže na internetu, oni koji traže obrazovne sadržaje imat će bolji školski uspjeh od onih koji traže zabavne sadržaje (Jackson Biocca, von Eye, Barbatsis, Zhao i Fitzgerald, 2004). Socijalni kontekst ima značajnu (iako skromnu) ulogu kod igranja igrica i gledanja televizije (npr. više vremena provedenog uz televiziju znači i bolji školskih uspjeh ako djeca sama gledaju televiziju, međutim, kada gledaju televiziju s roditeljima ili vršnjacima, više sati provedenih gledajući televiziju znači i slabiji školski uspjeh, gledanje televizije uz roditelje ili vršnjake predviđa viši stupanj empatije, više vremena provedenog u igranju računalnih igrica u društvu roditelja znači slabiju vršnjačku prihvaćenost nego u slučaju samostalnog igranja, igranje uz vršnjake predviđa viši stupanj empatije, više vremena provedenog u igranju računalnih igrica znači i bolju vršnjačku prihvaćenost i sl.), ali nema pri upotrebi interneta.

4.2. MOTIVACIJA ZA UPOTREBU INTERNETA DJECE I MLADIH

Internet je postao osnova današnje komunikacije, no unatoč prednostima, predstavlja i rizik za osobnu sigurnost i privatnost korisnika. Današnja djeca su djeca „digitalne generacije" jer se već od druge godine života koriste modernim uređajima za igru, gledanje videa i zabavu (Despotovic, Hossfeld, Kellerer, Lehrieder, Oechsner i Michel, 2011). Negativna je strana tog trenda mogućnost razvoja niza problema, pojave nasilja putem interneta, izolacije i problema s društvenom prilagodbom te ovisnosti o internetu. Kako odrastaju, djeca sve bolje razumiju suvremenu tehnologiju tako da im je lako manipulirati roditeljima glede svoje aktivnosti na internetu (Despotovic i sur., 2011).

Broj adolescenata koji imaju mobitel i pristup internetu svake je godine sve veći. Trećina djece Europske unije od 9 do 10 godina svakodnevno pristupaju internetu te to čini 80 % mladih u dobi od 15 do 16 godina (Livingstone, Haddon, Görzig i Ólafsson, 2011). Neka istraživanja pokazuju kako se 90 % mladih koristi internetom (Tokunaga, 2010). Tehnološka je oprema sve manja, brža, interaktivnija i sve prisutnija. Oko 87 % djece internetom se koristi kod kuće, a 63 % njih i u školi. Polovina djece koja se koristi internetom koristi se u svojoj spavaćoj sobi ili drugoj privatnoj sobi kod kuće, dok se 62 % djece koristi internetom u dnevnoj sobi ili drugoj javnoj sobi kod kuće. Adolescenti se češće koriste internetom u privatnim, a rjeđe u zajedničkim prostorijama u usporedbi s mlađom djecom. Djeca u prosjeku na internetu provedu sat vremena dnevno, a adolescenti dva sata dnevno (Livingstone i sur., 2011). Količina vremena koju djeca i mladi provode na internetu svakodnevno je u porastu, a izuzetno visoki postotak srednjoškolaca, njih 72,5 %, više puta dnevno kontaktira s prijateljima internetom (Đuraković i Klasnić, 2016). Prema istraživanju Lagator (2017) desetogodišnjaci se najčešće koriste internetom zbog igrica, (52,3 %), slušanja glazbe (60,3 %), dopisivanja s prijateljima (47,7 %) te traženja podataka koji im trebaju za školu (41,8 %). Kao motivaciju za pristupanjem internetu navode kako često traže zanimljive informacije (55,4 %), dok ih 36,3 % pristupa internetu iz želje za druženjem. Navedeno istraživanje pokazalo je kako dječaci provode više vremena na internetu i to najčešće u igranju igrica. Dječaci češće objavljuju sadržaje i traže zanimljive informacije nego djevojčice te internetu pristupaju uglavnom jer se ne žele razlikovati od drugih i kako bi izbjegli dosadu. Djevojčice češće pristupaju internetu zbog traženja informacija potrebnih za školu (Lagator, 2017).

Istraživanja pokazuju kako 63 % hrvatskih adolescenata rabi internet za komunikaciju s prijateljima, 61 % za preuzimanje raznih sadržaja, 47 % pretražuje sadržaje za školu i učenje, 42 % pretražuje bez posebnoga cilja, 20 % rabi internet za e-poštu, 18 % za socijalizaciju, 10 % piše blogove, a 9 % mladih sudjeluje u raspravama (Buljan

Flander, Ćosić i Profaca, 2009). Istraživanje Vejmelke, Strabića i Jazvo (2017) utvrdilo je kako djevojke provode više vremena na internetu od mladića na društvenim mrežama, u slušanju glazbe, razmjeni poruka, pretraživanju informacija za pisanje domaćih zadaća i medicinskih informacija te u kupovini. S druge strane, adolescenti značajno više od adolescentica provode vrijeme u igranju igara na interentu, pretraživanju sadržaja za odrasle, kockanju na internetu, u sobama za razgovor na internetu (engl. *chat*) i internetskim forumima.

Istraživanje Ercega (2015) utvrdilo je kako se djeca i adolescenti internetom koriste primarno zbog druženja i komunikacije te zabave, a rjeđe radi informiranja i samoostvarenja (čitanje vijesti, knjiga, učenja); također, dječaci se internetom češće koriste u svrhu zabave, a djevojčice u svrhu samoostvarenja, održavanja prijateljstava i informiranja. Različita istraživanja ukazuju kako su dječaci više motivirani od djevojčica u pogledu funkcionalnih i zabavnih aktivnosti na internetu, što uključuje pretraživanje internetskih stranica, igranje igrica te preuzimanje filmova i aplikacija (Lenhart, Madden i Hitlin, 2005; Livingstone i sur., 2011). Nasuprot tomu, djevojke se češće koriste internetom za obrazovne i socijalne aktivnosti, uključujući sobe za razgovor na internetu (engl. *chat*), društvene mreže, e-poštu i slušanje glazbe (Vlček, 2016). Izbjegavanje dosade jedan je od glavnih motiva upotrebe interneta kod djece. Vuletić, Jeličić i Karačić (2014) proveli su istraživanje kojim su utvrdili kako je kod 92 % sudionika glavna svrha upotrebe interneta razonoda, a tek kod 8 % sudionika škola ili posao.

Rezultati istraživanja pokazuju kako osobe koje postižu visoke rezultate na skalama neuroticizma na internetu uglavnom pretražuju zabavne sadržaje i koriste društvene mreže kako bi se opustile, smanjile razinu stresa te kao distrakciju od svojih problema (Wolfradt i Doll, 2001); osobe otvorene prema iskustvu internetom se uglavnom koriste instrumentalno (za traženje informacija) i za komunikaciju na društvenim mrežama, dok se ekstroverti internetom koriste ponajprije radi zabave i komunikacije (Hamburger i Ben-Artzi, 2000). Slabije obrazovane osobe te one nezadovoljnije svojim životom internetom se uglavnom koriste zbog osjećaja dosade pretražujući zabavne sadržaje i komunicirajući na društvenim mrežama, dok visoko obrazovani i oni zadovoljniji životom internetom se češće koriste u instrumentalne svrhe (radi traženja potrebnih informacija) (Kalmus, Realo i Siibak, 2011, Papacharissi i Ruben, 2000).

Druženje u virtualnom svijetu može predstavljati odmak od realnog okružja, bijeg u idiličan svijet bez obveza i odgovornosti koji nudi primamljive mogućnosti, ali i rizične situacije. Pretpostavlja se da je adolescentima jednostavnije komunicirati i sigurnije povjeriti se nekomu na internetu nego se izložiti mogućem nerazumijevanju i kritici prijatelja u stvarnom svijetu. Virtualna komunikacija ne mora uvijek biti ne-

gativna, već može pomoći mladima, osobito sramežljivima i niskog samopoštovanja (Bilić, 2010).

4.3. RIZIČNO PONAŠANJE DJECE I MLADIH NA INTERNETU

Uz brojne prednosti internet skriva i opasnosti, posebice za djecu i mlade. Često se ističu rizici nastanka ovisnosti, pretilosti uslijed smanjene tjelesne aktivnosti, mržnja, izloženost nasilju na internetu, narušavanje privatnosti te rizici izloženosti pornografskim sadržajima (Nikodem, Kudek Mirošević i Bunjevac Nikodem, 2014). Ybarra i Mitchell (2007) proveli su istraživanje o ponašanju adolescenata na internetu te su u rizike koji se mogu pojaviti njegovom uporabom uvrstili: otkrivanje osobnih informacija, agresivno ponašanje, razgovor s nepoznatim osobama, aktivnosti vezane uz seksualno ponašanje te preuzimanje materijala s interneta.

Karl, Peluchette i Schlaegel (2010) definiraju rizično ponašanje upotrebom interneta kao svako ponašanje koje uzrokuje zdravstvenu, profesionalnu, financijsku ili socijalnu štetu. Na internetu informacije i sadržaje može objavljivati bilo tko u bilo kojem trenutku bez ikakve odgovornosti i cenzure. Neprimjerene i neprovjerene informacije mogu biti štetne i ugrožavajuće za fizički i psihički integritet djece i mladih. Tzv. rizične stranice interneta upravo su djeci i mladima najzanimljivije (Đuraković, 2016). U znanstvenoj literaturi kao izrazito rizični sadržaji odnosno internetske stranice neprimjerene i štetne za djecu i mlade navode se one koje promoviraju kupnju i konzumiranje alkohola, narkotika i duhanskih proizvoda, pornografske stranice koje potiču seksualno neodgovorno ponašanje, stranice koje navode na kockanje i klađenje, koje potiču na objavljivanje osobnih podataka, stranice koje šire agresivnost, rasnu i nacionalnu netrpeljivost (Patchin i Hinduja, 2006). Opasnost predstavljaju i društvene mreže koje omogućavaju i izravnu komunikaciju s nepoznatim ljudima koji ih mogu nagovoriti i na osobni susret.

Livingstone i Helsper (2009) dijele rizike s kojima se djeca susreću na internetu na agresivne (nasilje, uhođenje), seksualne (pornografija, *seksting*, seksualno uznemiravanje ili iskorištavanje), vrijednosne (rasistički, ideološki sadržaji) i komercijalne (zloupotreba osobnih podataka, kockanje i zlouporaba autorskih prava).

Vejmelka, Strabić i Jazbo (2016) navode kako je kockanje na internetu aktivnost koja je vrlo rizična, ali i rjeđe pristupačna adolescentima jer zahtijeva posjedovanje kreditne kartice. Rezultati navedenog istraživanja pokazuju kako neki adolescenti ipak sudjeluju u internetskom kockanju, a utvrđena je i korelacija takve aktivnosti s počinjenjem nasilja internetom. Učenici koji čine nasilje na internetu pokazuju ten-

denciju rizičnoga ponašanja i u drugim aktivnostima, kao što su kockanje i pregledavanje pornografskoga sadržaja.

4.3.1. DJEČJE VJEŠTINE UPOTREBE INTERNETA

Većina djece u dobi od 11 do 16 godina može označiti internetsku stranicu (64 % djece), blokirati nečije poruke s kim ne žele biti u kontaktu (64 % djece) ili pronaći informacije o sigurnosti na internetu (63 % djece). Polovina djece može promijeniti postavke privatnosti na profilu društvene mreže, usporediti različite stranice za procjenu kvalitete informacija (56 % djece), izbrisati povijest pretraživanja (52 % djece) ili blokirati neželjenu poštu (51 % djece). Samo četvrtina može promijeniti filtar preferencije. Djeca od 9 do 12 godina (u usporedbi s djecom od 13 do 16 godina) manje će se koristiti internetom za gledanje ili objavljivanje videoisječaka, slanje poruka, čitanje ili gledanje vijesti, društvene mreže i e-poštu, preuzimanje glazbe ili filmova, odnosno manje su vješta u uporabi interneta u odnosu na adolescente (Livingstone i sur., 2011).

Djeca višeg socioekonomskog statusa i obrazovanijih roditelja imaju veći repertoar aktivnosti i bolje vještine uporabe interneta od djece nižeg socioekonomskog statusa te imaju veći pristup internetu. Dječaci su uključeni u više aktivnosti u odnosu na djevojčice. Također, dječaci i starija djeca samopouzdanija su po pitanju svojih vještina. Djeca nižeg socioekonomskog statusa svjesnija su kako njihovi roditelji imaju slabije razvijene vještine uporabe interneta (Livingstone i sur., 2011).

Oni koji više vremena provode na internetu i imaju razvijenije vještine, susretat će se s više rizika budući da će sudjelovati u više različitih aktivnosti (npr. pisanje bloga ili posjedovanje internetske stranice). Pozitivna iskustva i negativne posljedice interneta međusobno su povezane – što više prilika dijete dobije, to je više i izloženo rizicima (Livingstone i sur., 2011).

Djeca općenito precjenjuju svoje internetske vještine i procjenjuju se vještijima od roditelja što ponekad i jest slučaj, ali ponekad i nije. Mlađa djeca (9–10 godina) realnija su što se tiče osobnih internetskih vještina, procjenjuju ih nižima, te su svjesna kako su roditelji vještiji od njih, dok adolescenti svoje vještine uporabe interneta češće precjenjuju (Livingstone i sur., 2011).

4.3.2. RIZIČNA ISKUSTVA DJECE NA INTERNETU I ČIMBENICI KOJI IH PREDVIĐAJU: PRIKAZ REZULTATA EUROPSKIH ISTRAŽIVANJA

Prema istraživanju Livingstone i Bober (2006) mladi od 12 do 17 godina koji se koriste internetom najmanje jednom tjedno navode da:

- su se susreli s pornografskim sadržajem (reklame za pornografiju dok su radili nešto drugo) – 44 %
- su završili na pornografskoj stranici slučajno kada su tražili na internet nešto drugo – 41 %
- su primili pornografsku poštu – 28 %
- su dobili pornografski sadržaj od nekoga koga znaju – 9 % djece
- su posjetili pornografsku stranicu s namjerom – 9 % djece
- su dobili pornografski sadržaj od nekoga koga su upoznali na internetu – 3 %
- su slučajno završili na mjestu s nasilnim ili jezivim slikama – 27 %
- su posjetili takvu stranicu namjerno – 14 %
- su slučajno završili na internetskoj lokaciji koja širi neprijateljstvo ili mržnju prema skupini ljudi – 10 %
- su svojom voljom posjetili stranicu koja širi mržnju – 3 %
- su dali osobne podatke nekome upotrebom interneta – 46 %
- bi dali osobne podatke kako bi osvojili nagradu u kvizu – 72 %
- neke osobe poznaju samo na internetu i s njima razgovaraju – 36 %
- su se susreli s nekim licem u lice koga su upoznali na internet – 9 %
- su primili zlobne komentare na internetu – 33 %.

Rizični sadržaji ne moraju nužno od strane djece biti doživljeni kao štetni ili uznemirujući. Dakle, nešto što smatramo rizičnim sadržajem za dijete ne mora biti uznemirujuće i ne mora kod njega izazvati psihičku patnju. Primjerice, s gledanjem ili dobivanjem seksualnih slika susreće se svako osmo dijete, ali samo rijetki to doživljavaju uznemirujućim (Livingstone i sur., 2011).

Čak 12 % djece od 9 do 16 godina navodi kako je bilo uznemireno nečim na internetu (Livingstone i sur., 2011). Najmanje je vjerojatno da će nešto na internetu zasmetati najmlađoj djeci, u dobi od 9 do 10 godina (9 %), u usporedbi sa starijom djecom (11– 15 %) zbog toga što starija djeca sudjeluju u više aktivnosti na internetu te se susreću s više rizika. Ipak, djevojke i mlađa djeca će općenito vjerojatnije biti uzrujani kada se susretnu s rizičnim sadržajima (osjetljiviji su). Rizici se povećavaju s dobi, 14 % djece od 9 do 10 godina naišli su na jedan ili više rizika, što vrijedi za 33 % djece od 11 do 12 godina, 49 % djece od 13 do 14 godina i 63 % djece od 15 do 16 godina. Dakle, starija djeca susreću se s više rizika, ali su na njih otpornija (Livingstone i sur., 2011).

Čak 21 % djece od 11 do 16 godina bilo je izloženo jednom ili više vrsta potencijalno štetnim sadržajima na internetu: poticanju mržnje (12 %), promoviranju anoreksije (10 %), samoozljeđivanju (7 %), uzimanju droge (7 %) ili samoubojstvu (5 %) (Livingstone i sur., 2011).

Djevojčice će češće posjećivati širi spektar stranica – stranice povezane s pravima manjina (prava homoseksualaca, žena, djece itd.), političke stranice, peticije na internetu i sl. Susrest će se s manje pornografije, ali će se sa strancima koje upoznaju na internetu češće nalaziti uživo. Djevojke, osobito one u dobi od 14 do 16 godina, vjerojatnije će od dječaka vidjeti stranice koje podupiru anoreksiju ili bulimiju (19 % djevojaka u dobi od 14 do 16 godina) (Livingstone i sur., 2011). Dječaci više vremena provode na internetu, vjerojatnije će tražiti pornografske sadržaje, nasilne i rasističke sadržaje ili do njih doći slučajno (Livingstone i sur., 2011). Dječaci imaju veći pristup internetu i bolje vještine uporabe interneta pa se susreću s više rizičnih sadržaja, ali su otporniji od djevojčica, tj. izvještavaju o nižem stupnju uznemirenosti.

Čak 15 % djece u dobi od 11 do 16 godina dobilo je seksualnu poruku ili sliku od svojih vršnjaka, a 3 % djece izjavljuje kako je poslalo ili objavilo takve poruke ili slike (Livingstone i sur., 2011). Od onih koji su primili takve poruke, gotovo jedna četvrtina bila je njima uznemirena. Onima kojima je smetao *seksting*, u 40 % slučajeva blokirali su osobu koja je poslala poruke i/ili izbrisali neželjene seksualne poruke (38 %) (Livingstone i sur., 2011).

Djevojke će rjeđe vidjeti seksualne slike na internetu od dječaka (12 % u odnosu na 16 %), ali je veća vjerojatnost da će ih one zasmetati (Livingstone i sur., 2011). Više od polovine ispitane djece (53 %) u dobi od 9 do 16 godina bilo je uznemireno gledanjem seksualnih slika na internetu. Četvrtina (26 %) onih koji su bili uznemireni seksualnim slikama zauzeli su "pasivni" pristup nadajući se da će problem sam nestati, 22 % zauzelo je proaktivan pristup pokušavajući riješiti problem, dok ih je polovina nekome rekla što se dogodilo. Najčešća je reakcija na seksualne poruke brisanje poruka od onoga tko je poslao slike (26 %). Oko 25 % djece nakon uznemirujućih slika neko je vrijeme prestalo koristiti se internetom.

Čak 9 % djece od 11 do 16 godina doživjelo je zlouporabu osobnih podataka – zloupotrebu zaporke (7 %), osobnih podataka (4 %) ili je novčano prevareno (1 %) (Livingstone i sur., 2011).

Polovina ispitane djece (50 %) od 11 do 16 godina smatra da im je lakše razgovarati s ljudima na internetu nego kada se s njima sretnu licem u lice. Gotovo polovina ispitanih (45 %) izjavljuje da razgovara o drukčijim stvarima na internetu nego kada razgovara s ljudima licem u na lice. Trećina (32 %) izjavljuje da o privatnim stvarima o kojima govori na internetu ne govori licem u lice. Više dječaka (31 %)

od djevojaka (20 %) komunicira na internetu s ljudima koje pozna samo na internetu.

Postoje dobne razlike u komunikaciji s ljudima s kojima su se prvi put susreli na internetu (i s kojima nemaju drugu povezanost u životu): navedeno čini 19 % djece od 11 do 12 godina, 23 % djece od 13 do 14 godina i 33 % djece od 15 do 16 godina. Trećina djece (34 %) dodala je na neku društvenu mrežu kontakte koje ne poznaje, a polovina njih to čini nekoliko puta mjesečno (Livingstone i sur., 2011).

Čak 30 % djece uspostavilo je kontakt na internetu s nekim koga ne poznaje u stvarnom životu. Što je dijete starije, to će vjerojatnije kontaktirati nove ljude uporabom interneta. Samo 2 % djece od 9 do 10 godina i 4 % djece od 11 do 12 godina upoznalo se licem u lice s nekim koga su prvi put susreli na internetu. Međutim, 9 % djece od 13 do 14 godina i 16 % djece od 15 do 16 godina otišli su na takav sastanak. Većina djece nekomu je rekla kad je otišla na susret s nepoznatom osobom, a 70 % djece povelo je prijatelja sa sobom. Međutim, gotovo jedna trećina nije rekla nikome da planira otići na sastanak (Livingstone i sur., 2011).

Oko 6 % djece bilo je zlostavljano putem interneta, od čega je 31 % djece time bilo vrlo uzrujano, 24 % djece prilično uzrujano, 30 % djece malo uzrujano te 15 % djece izjavljuje kako nije uopće bilo uzrujano. Čini se da su djeca iz obitelji s nižim socioekonomskim statusom znatno više uzrujana. Djevojke (37 %) imaju veću vjerojatnost da će zbog zlostavljanja biti "vrlo uzrujane" u usporedbi s dječacima (23 %) (Livingstone i sur., 2011).

Najčešći odgovor na zlostavljanje putem interneta bio je proaktivan – 36 % djece pokušalo je riješiti problem zlostavljanja. Četvrtina (24 %) se nadala da će problem sam nestati. Četvero od petero (77 %) djece u dobi od 9 do 16 godina koji su doživjeli zlostavljanje razgovarali su s nekim o tome. Najčešća poduzeta akcija žrtve je blokiranje osobe koja je poslala zlobne poruke (46 %) ili brisanje zlobne poruke (41 %). Četvero od desetero djece odgovorilo je proaktivno, tj. 27 % djece pokušalo je riješiti problem. Međutim, više od petine (22 %) samo se nadalo da će problem nestati. Većina (60 %) je razgovarala s nekim o tome, najčešće je to bio prijatelj (38 %) ili roditelj (30 %).

Djeca koja koriste pasivne pristupe u suočavanju s uznemirujućim iskustvima na internetu mlađa su, niže samoefikasnosti, s više psiholoških teškoća, osjetljivija (ona koja se lakše uznemire) i rjeđe se koriste internetom. Oni koji pričaju o negativnim iskustvima češće su ženskog spola, mlađi, niže potrebe za traženjem uzbuđenja, oni koji se i inače lakše uznemire te oni skloniji komunikaciji. Proaktivni u suočavanju imaju visoku samoefikasnost i često koriste internet (Livingstone i sur., 2011).

Livingstone i sur. (2011) na temelju rezultata istraživanja u kojem su obuhvatili 25 000 djece Europske unije zaključili su kako je većinu djece moguće svrstati u jednu od šest kategorija.

1) Rijetki korisnici / korisnici usmjereni učenju – mlađa djeca (9–10 godina) koja se rijetko koriste internetom, sudjeluju u malom broju aktivnosti na internetu, rabe ga uglavnom za potrebe škole, rjeđe za gledanje videoisječaka i gledanje ili čitanje vijesti te su izložena vrlo malom broju potencijalnih rizika, ali doživljavaju najviše uznemirenosti ukoliko se susretnu s rizičnim sadržajem, npr. ukoliko upoznaju ljude putem interneta (najosjetljiviji su).

2) Rijetki korisnici / korisnici usmjereni društvenim mrežama – mlađa djeca kojoj nije toliko stalo do pretraživanja sadržaja vezanih za školu ili vijesti, već posjećuju društvene mreže. Potencijalni su rizici umjereni, a ta skupina upoznavat će mnoge ljude na internetu, ali neće biti uznemirena tim iskustvima.

3) Umjereni korisnici – u prosjeku stari 12 godina, provode više vremena na internetu i sudjeluju u većem broju aktivnosti. Svi su čimbenici rizika viši u odnosu na prve dvije skupine.

4) Skupina korisnika različitih i rizičnih aktivnosti – u prosjeku stari 13,5 godina, imaju najveći raspon aktivnosti, kao i rizičnih aktivnosti, često gledaju ili čitaju vijesti, preuzimaju filmove ili glazbu, šalju ili primaju e-poštu, igraju igrice i služe se web kamerom, provode vrijeme u virtualnim svjetovima i pišu blogove. Izloženi su najrizičnijim sadržajima i iskustvima, ali doživljavaju najmanje štete i uznemirenosti (otporni su).

5) Česti korisnici / korisnici usmjereni zabavi – u prosjeku stari 14 godina, uglavnom dječaci, dnevno provode najviše vremena na internetu, ali u manjem broju aktivnosti – uglavnom igraju igre ili gledaju videoisječke. Rijetko traže informacije koje se odnose na školu, vijesti ili pišu blog. Potencijalni su rizici visoki kao i opasnost od prekomjerne upotrebe interneta.

6) Korisnici usmjereni na socijalnu upotrebu interneta – najstariji, u prosjeku 14,2 godine, češće djevojke, često se koriste internetom i imaju velik raspon aktivnosti na internetu, ne igraju igrice, vrijeme provode na društvenim mrežama, dopisuju se, čitaju vijesti, pišu blogove, objavljuju glazbu ili slike. U poprilično su velikom riziku iako malo manjem u odnosu na prethodne dvije skupine, ali će biti poprilično uznemireni kada se susretnu s rizičnim sadržajima.

Djevojke će biti osjetljivije na seksualne sadržaje i nasilje putem interneta, dok po pitanju osjetljivosti od upoznavanja novih ljudi na internetu spol nema utjecaja. Djeca koja traže uzbuđenje bit će manje uznemirena po pitanju seksualnih sadržaja,

mlađi će biti uznemireniji po pitanju seksualnih sadržaja i upoznavanja novih ljudi na internetu od starijih, dok dob nema utjecaja na otpornost na nasilje na internetu. Nasilje na internetu uznemirit će najveći broj djece (86 % onih koji ga dožive). Djeca s teškoćama u razvoju, zlostavljana i zanemarena djeca, djeca niskog samopoštovanja, adolescenti koji zloupotrebljavaju alkohol i droge te odrastaju uz roditelje ovisnike podložnija su i osjetljivija na sve vrste rizika na internetu (Livingstone i sur., 2011).

4.3.3. RIZIČNA ISKUSTVA DJECE NA INTERNETU: REZULTATI NACIONALNIH ISTRAŽIVANJA

Prema istraživanju Poliklinike za zaštitu djece grada Zagreba i Hrabrog telefona iz 2013. godine 41 % djece izjavilo je da su im tijekom druženja i komunikacije na internetu bila postavljana intimna pitanja o njima, njihovom tijelu ili pitanja seksualnog karaktera (djevojčice, njih 43 %, bile su češće pitane o intimnim detaljima nego dječaci, njih 38 %). Na pitanje je li tko koga su upoznali na internetu tražio da se slikaju ili snimaju na seksualizirani način, 39 % djece navodi da je, ali to nisu učinili, dok 6 % djece navodi da su se slikali i poslali sliku. Čak 31 % djece navodi da im je osoba koju su upoznali na internetu poslala svoju sliku bez odjeće, a 14 % djece navodi da su otišli na sastanak i upoznavanje s internetskim prijateljem kojeg do tada nisu poznavali uživo. U 14 % slučajeva navode da su kao pratnja išli i roditelji, 49 % navodi da su išli s prijateljima, dok 37 % djece navodi da su otišli na sastanak sami. Čak 54 % djece i mladih izjavilo je da je naišlo na internetsku stranicu koja je sadržavala fotografije golih ljudi ili ljudi u spolnom odnosu, a da to nisu željeli, 24 % djece i mladih navelo je da su primili poruku elektroničkom poštom koja je oglašavala pornografske stranice ili je sadržavala poveznice za te stranice, a da to nisu željeli, a 28 % djece i mladih otvorilo je poruku ili poveznicu koja je sadržavala slike golih ljudi ili osoba u seksualnoj aktivnosti, a da to nisu željeli.

Otkrivanje osobnih podatka na internetu može se opisati kao neodgovorno ili opasno ponašanje jer potencijalni zlostavljači mogu iskoristiti te iste podatke u svrhu povrede druge osobe (Carević, Mihalić i Sklepić, 2014). Budući da je internet anoniman medij, omogućuje odraslim osobama da se pretvaraju da su djeca čime djeca, misleći da razmjenjuju informacije s drugom djecom, mogu pedofilu dati svoje osobne informacije o svojoj dobi, spolu, adresi i školi koju pohađaju, dok neki pedofili mogu biti samo promatrači razgovora i na taj način prikupljati informacije o djetetu. Većina korisnika nije svjesna te činjenice. Rezultati istraživanja Carević, Mihalić i Sklepić (2014) otkrivaju da se s tvrdnjom „Na internetu otkrivam svoje osobne podatke“ mali postotak srednjoškolaca u potpunosti slaže, njih 3,48 %, s tvrdnjom ih se slaže 15,42 %, a samo 37,81 % srednjoškolaca uopće se ne slaže s navedenom tvrdnjom. S

tvrdnjom „Na internetu razmjenjujem poruke s nepoznatim ljudima“, najveći postotak srednjoškolaca uopće se ne slaže (44,28 %), dok se malen broj učenika u potpunosti slaže (9,45 %). Također, istraživanje je utvrdilo kako postoji povezanost rizičnih oblika ponašanja učenika srednjih škola s brojem sati koje tjedno provode na internetu te kako postoji sukladan rast vrijednosti između vremena provedenog na internetu i zanemarivanja školskih obaveza.

4.3.4. UGROŽAVANJE INFORMACIJSKE SIGURNOSTI I PRIVATNOSTI

Adolescenti i mlađe odrasle osobe najčešći su korisnici društvenih mreža kao što su Facebook ili Twitter. Čak 59 % djece i mladih u dobi od 9 do 16 godina ima profil na društvenoj mreži – 58 % dječaka i 60 % djevojčica, uključujući 26 % djece u dobi od 9 do 10 godina, 49 % djece u dobi od 11 do 12 godina, 73 % djece u dobi od 13 do 14 godina i 82 % mladih u dobi od 15 do 16 godina (Livingstone i sur., 2011). Među korisnicima društvenih mreža 26 % djece ima javni profil, a 43 % djece zadržava profil privatnim, dok ostali nisu sigurni je li njihov profil javan ili privatan. Oko 9 % djece ima više od 300 kontakata na profilu, a 20 % djece ima između 100 i 300 kontakata. Djevojke i djeca iz obitelji s visokim socioekonomskim statusom češće imaju privatni profil. Razlike u socioekonomskom statusu vrlo su male (57 % privatnih profila u djece s niskim socioekonomskim statusom nasuprot 62 % privatnih profila u djece s visokim socioekonomskim statusom). Iznenađujuće je da stariji adolescenti češće imaju javni profil. S druge strane, moguće je da roditelji češće savjetuju mlađoj djeci da postavljaju svoje profile privatnima (Livingstone i sur., 2011).

Trećina roditelja izjavljuje kako je svojoj djeci zabranila biti na društvenim mrežama, petina kako se djeca smiju koristiti društvenim mrežama, ali samo uz njihov nadzor, dok polovina roditelja djeci nije postavila nikakva ograničenja s obzirom na upotrebu društvenih mreža (Livingstone i sur., 2011).

Nosko, Wood i Molema (2009) razlikuju tri kategorije otkrivanja osobnih informacija na Facebooku:

a) informacije o osobnom identitetu – spol, datum rođenja

b) osjetljive osobne informacije – slike, adresa e-pošte

c) potencijalno stigmatizirajuće informacije – seksualna orijentacija, interesi i sl.

Također, navedeni autori razlikuju namjeru, dubinu, količinu i iskrenost u otkrivanju osobnih informacija.

Prema istraživanju Brstilo, Batinić i Grgić (2014) provedenom među 1987 djece osnovnoškolske i srednjoškolske dobi u Republici Hrvatskoj oko 75 % djece i mladih objavljuje svoje ime na društvenim mrežama, dok 68 % njih objavljuje i svoje prezime,

a više od trećine djece i mladih objavljuje ime škole koju pohađa. Adresu e-pošte otkriva oko trećina djece i gotovo polovina adolescenata. Relativno mali postotak otkriva svoju kućnu adresu, samo 5 % djece odnosno 7 % adolescenata, broj telefona oko 12 % djece i oko 12 % adolescenata, datum rođenja otkriva oko 45 % djece i 63 % adolescenata. Svoje privatne fotografije objavljuje 34 % djece i 57 % adolescenata. Informacije iz privatnog života otkriva 35 % djece i 54 % adolescenata, a informacije o obitelji i prijateljima 17 % djece i gotovo trećina adolescenata. Rezultati ukazuju na to da su mladi skloniji dijeljenju informacija o sebi na društvenim mrežama od djece što može biti jedan od načina privlačenja pozornosti i stjecanja popularnosti. Oko trećina djece i gotovo polovina adolescenata šalje zahtjeve za prijateljstvom osobama koje nije upoznala uživo (Brstilo, Batinić i Grgić, 2012). Moguće je da nad internetskim aktivnostima mlađe djece roditelji imaju veću kontrolu pa djeca imaju manje mogućnosti stupanja u kontakt sa strancima. Postavlja se pitanje prihvaćaju li mladi prijateljstva s osobama koje ne poznaju zbog popularnosti koja se često mjeri brojem prijatelja na društvenim mrežama? Također, trebalo bi provjeriti jesu li svjesni mogućih opasnosti s obzirom da se radi o korisničkim profilima u čiju autentičnost ne mogu biti sigurni. Više od jedne četvrtine djece i mladih prihvaćalo je zahtjeve za prijateljstvom od stranaca (Brstilo, Batinić i Grgić, 2012). Može se zaključiti kako sudionici precjenjuju svoju povezanost s prijateljima na Facebooku i zbog toga se smatraju imunima na različite prijetnje privatnosti (Brstilo, Batinić i Grgić, 2012). Kada je riječ o mijenjanju početnih postavki privatnosti na stranicama društvenih mreža, mladi više nego djeca pridaju važnost tome i češće mijenjaju postavke privatnosti. Ipak, upitna je njihova osviještenost o problemima privatnosti na internetu. Zabrinjava i činjenica da svako treće dijete ne mijenja početne postavke privatnosti na stranicama društvenih mreža (Brstilo, Batinić i Grgić, 2012). Korisnici često ne vode računa o količini osobnih podataka koje objavljuju niti o broju ljudi kojima su njihovi osobni podaci dostupni. Mladi značajno češće od djece provjeravaju kako izgleda njihov profil, znatno im je važnije kakav dojam ostavljaju na druge. U čak 12,3 % slučajeva djeca i adolescenti provode na Facebooku više od 5 sati dnevno (Brstilo, Batinić i Grgić, 2012). Njih čak 86,16 % ne poznaje neko nadležno tijelo kojem bi se mogli obratiti u slučaju da netko ugrozi njihovu privatnosti**.** Manji broj njih navodi da poznaje neka, no dio onih koje su navodili uopće ne pripadaju kategoriji nadležnih tijela (Brstilo, Batinić i Grgić, 2012). Paradoks privatnosti pokazao je kako s osvještavanjem pitanja privatnosti ne raste korištenje postavki privatnosti niti poduzimanje mjera za zaštitu osobnih podataka na društvenim mrežama. Djeca i mladi dijele osobne informacije na Facebooku usprkos tomu što su svjesni da time ugrožavaju svoju privatnost (Brstilo, Batinić i Grgić, 2012).

Istraživanjem Poliklinike za zaštitu djece i mladih grada Zagreba (2013) utvrđeno je kako 93 % djece ima otvoren Facebook profil, 68 % njih otvore ga prije 13. go-

dine, a čak 78 % roditelja djeci nije postavilo nikakva pravila o korištenju Facebooka. S porastom dobi djeteta roditelji postavljaju sve manje ograničenja pa su najugroženija skupina za rizična ponašanja na internetu mladi u dobi od 15 do 16 godina.

Jedno od mogućih objašnjenja ponašanja djece i mladih na društvenim mrežama u kontekstu njihove otvorenosti prema dijeljenju osobnih podataka nalazimo kod Meada (2003) koji na osnovi simbola objašnjava socijalnu komunikaciju. Simbolima se izražavamo i pomoću njih komuniciramo s drugim ljudima. U komunikaciji svaka osoba preuzima određenu ulogu, a dojam o drugoj osobi stvaramo već u prvih nekoliko sekundi. U virtualnom okruženju profilna aplikacija predstavlja niz simbola pomoću kojih komuniciramo s drugima te ima zadatak socijalne prezentacije.

Također, rezultati istraživanja pokazuju kako se osoba koja je spremnija podijeliti informacije o sebi procjenjuje socijalno atraktivnijom, odnosno s takvom se osobom ljudi žele družiti i ostvariti prijateljski odnos. Livingstone i Helsper (2008) zaključuju kako objavljivanje sadržaja na društvenoj mreži za mnoge adolescente predstavlja stvaranje identiteta, životnog stila i socijalnih odnosa. Adolescenti dijele svoje privatne informacije kako bi održali prisnost s drugim ljudima. Potreba za komuniciranjem kod adolescenata jača je od osjećaja opreza i nepovjerenja prema nepoznatim osobama te adolescenti nekritički pristupaju takvim situacijama.

Djeca imaju poteškoće u razumijevanju privatnosti na internetu i implikacija gubitka te privatnosti. Svijest o gubitku kontrole i vlasništva nad sadržajem koji su postavili na Facebooku kod njih još uvijek nije razvijena. Često su impulzivni i djeluju bez razmišljanja pogotovo kada su na internetu i kada ne postoje neposredne društvene posljedice. Vještine donošenja odluka još nisu dovoljno razvijene u toj dobi što ih često čini ranjivima na rizično ponašanje. Kombinacija impulzivnosti, naivnosti i slabo razvijene vještine donošenja odluka djecu čini populacijom koja je u današnje vrijeme najviše izložena riziku, prijevarama, zlostavljanju, ponižavanju, uznemiravanju i neprimjerenim sadržajima na internetu (Kušić, 2010).

4.3.5. NEGATIVNE POSLJEDICE UPOTREBE INTERNETA

4.3.5.1. Posljedice upotrebe Facebooka

Facebook potiče socijalnu komparaciju, a time i zavist koja može dovesti do depresije (Chou i Edge, 2012, Nguyen Steers, Wickham i Acitelli, 2016). Usporedbom s drugima ljudi procjenjuju svoje sposobnosti i osobine ličnosti te pokušavaju povećati svoje samopouzdanje. Pri tome se mogu osjećati pozitivno ili negativno, a kako će se osjećati, ovisi o nekoliko čimbenika kao što su osobine ličnosti, ali i osoba s kojom se

pojedinac uspoređuje. Pregledavanje tuđih informacija, kao što su fotografije s godišnjih odmora, potiče osjećaj zavisti koji ima štetan utjecaj na zadovoljstvo životom (Chou i Edge, 2012, Ryan i Xenos, 2011). Pozitivno je raspoloženje negativno povezano s vremenom koje osoba aktivno provodi na Facebooku. Najviše se zavidi ljudima koji objavljuju slike s praznika i s prijateljima, koji dobivaju više čestitki i želja za rođendan. Osobe koje se češće koriste Facebookom osjećaju da je njihov život lošiji za razliku od osoba koje se rjeđe koriste Facebookom (Chou i Edge, 2012). Pojedinci koji provode više vremena na Facebooku više se uspoređuju s drugima. Jedan od kriterija usporedbe je i broj prijatelja na Facebooku. Oni korisnici koji duže vrijeme imaju otvoren račun na Facebooku izvještavaju kako vjeruju da drugi imaju bolji život i da su sretniji od njih (Chou i Edge, 2012). Nesigurnost u sebe pozitivno je povezana s frekvencijom socijalnih usporedbi na Facebooku (Nguyen Steers, Wickham i Acitelli, 2016).

Provodeći vrijeme na internetu i komunicirajući sa strancima na društvenim mrežama, pojedinci postaju sve više socijalno izolirani i odsječeni od svojih stvarnih socijalnih veza (Ryan i Xenos, 2011, Deters i Mehl, 2012). Što više provode vremena na društvenim mrežama, osobe imaju manju kvalitetu života odnosno razina njihovog zadovoljstva pada tijekom vremena. Ljudi su previše zaokupirani time da sve neprestance dokumentiraju i objavljuju na Facebooku, a provođenje vremena na internetu povezuje se s manje vremena provedenog sa svojom obitelji, smanjenim brojem prijatelja i povećanom depresijom i usamljenošću. Što više vremena djeca i adolescenti provode na internetu, osjećaju se usamljenijima (Puri i Sharma, 2016, Zeng, Ye, Hu i Ma, 2016).

Neka istraživanja sugeriraju da je aktivna komunikacija s prijateljima na Facebooku povezana s manjom razinom usamljenosti, dok je pasivno korištenje (npr. pretraga vijesti na Facebooku) povezano s većom razinom usamljenosti (Ryan i Xenos, 2011, Deters i Mehl, 2012). Djevojke izvještavaju o pozitivnijem stavu prema Facebooku te provode više vremena na Facebooku nego što to čine dječaci. Ipak, intenzivna uporaba Facebooka može značiti da korisnici više ulažu u odnose sa svojim prijateljima na Facebooku te stoga i pokazuju negativnije odgovore i odgovore s više ruminacije kada izgube jednog od tih prijatelja (kada ih prijatelj obriše s liste prijatelja). Adolescenti često kasne u školu jer provjeravaju Facebook, manje spavaju jer su do kasno na Facebooku, znatno vremena troše na Facebook zbog čega imaju manje vremena za učenje i izvršavanje drugih obaveza (Puri i Sharma, 2016). Vjerojatnost da osoba postane žrtva zlostavljanja na internetu viša je za one koji su više ovisni o internetu, za koje je vjerojatnije da će razgovarati sa starijim poznanicima na internetu ili one koje daju zaporke drugima i dijele osobne podatke na blogu ili Facebooku (Deters i Mehl, 2001).

Facebook može izazvati probleme u vezama povećanim osjećajem zavisti. Ljudi se često uspoređuju s potencijalnim ili bivšim partnerima svoje simpatije kao i s njezinim/njegovim prijateljima kako bi procijenili svoju atraktivnost. Nakon prekida veze, Facebook omogućava nezdravi nadzor nad bivšim partnerom i odgađa emocionalni oporavak (Nguyen Steers, Wickham i Acitelli, 2016).

Osjećaji koji se javljaju prilikom uporabe Facebooka su (Zeng i sur., 2016, Deters i Mehl, 2012):

1. *živciranje* – zbog stalnih negativnih objava loše raspoloženog prijatelja, stalnih obavijesti o postignućima u igricama
2. *šok* – kada pojedinci čuju važnu vijest od bliskog prijatelja na Facebooka ili kada prijatelj objavi neprimjeren post, komentar ili sliku
3. *zaprepaštenje* – kada čuju važnu vijest o sebi bliskim osobama, povrijeđeni su jer su tu vijest čuli koristeći se Facebookim a ne uživo
4. *gađenje* – kada vide neprikladan sadržaj koji su objavili njihovi prijatelji
5. *iritacija* – zbog sadržaja koji se stalno ponavljaju ili ih smatraju besmislenima.

Istraživanje Staksruda, Olafsson i Livingstone (2013) pokazalo je kako djeca koja češće koriste društvene mreže doživljavaju više rizičnih iskustava na internetu. Oni koji koriste društvene mreže i imaju bolje razvijene kompetencije upotrebe interneta, oni koji imaju više prijatelja i oni koji imaju javni profil također su u većem riziku doživljavanja neugodnih iskustava na internetu. Ipak, podržavajuće objave na Facebooku od strane vršnjaka mogu dovesti do više razine socijalne i psihološke dobrobiti, dok dijeljenje informacija te stalna akademska podrška mogu dovesti do boljeg uspjeha u školi (Zheng i Zhao, 2015). Dakle, društvene mreže same po sebi nisu niti loše niti dobre, već je bitan način na koji ih djeca rabe.

4.3.5.2. Emocionalne poteškoće povezane s rizičnim ponašanjem na internetu

Tijekom adolescencije povećava se potreba za povezivanjem s drugima, a internet nudi mogućnosti adolescentima da se uključe u potencijalno rizična ponašanja kao što su interakcije sa strancima. Interakcije na internetu uklanjaju inhibicije i povećavaju osjećaj intimnosti među ljudima. Gotovo 80 % roditelja izjavljuje da je vrlo zabrinuto da će se njihovo dijete susresti sa strancima upotrebom interneta (George i Odgers, 2015). Susret sa strancem kojeg upoznaju na internetu za djecu može biti opasan po život i rezultirati nizom negativnih posljedica. U istraživanjima provedenim u zemljama šdiljem svijeta postotak adolescenata koji se licem u lice

nalazi s ljudima s kojima su se upoznali na internetu iznosi od 7 % do 35 % (Baumgartner, Valkenburg i Peter, 2010, Liau, Khoo i Ang, 2005).

Malo se toga zna o mentalnom zdravlju adolescenata koji pokazuju rizično ponašanje upotrebom interneta (Livingstone i Haddon, 2008). Istraživanja sugeriraju da depresija i smanjeno samopouzdanje imaju utjecaj na uključivanje u rizična ponašanja upotrebom interneta (Ybarra, Alexander i Mitchell, 2005). Moguće objašnjenje zašto adolescenti komuniciraju s drugima na internetu nudi hipoteza *socijalne kompenzacije*. Prema toj hipotezi socijalno anksiozni i introvertirani adolescenti posebno se često koriste internetom zato što imaju poteškoća u razvijanju prijateljstva i komuniciranju u stvarnim životnim okruženjima (Valkenburg, Schouten i Peter, 2005). Adolescenti skloni depresivnosti mogu tražiti kontakte na internetu kako bi smanjili osjećaj usamljenosti i ostvarili socijalnu potporu. Približno 80 % adolescenata s depresivnom simptomatologijom razgovaralo je s neznancem na internetu u usporedbi sa 55 % adolescenata bez depresivne simptomatologije (Ybarra, Alexander i Mitchell, 2005). Istraživanja s obzirom na smjer odnosa između osjećaja depresije i formiranja odnosa upotrebom interneta nejednoznačna su. Jedno istraživanje otkrilo je kako povišena razina depresije predviđa povećanje sklonosti za društvene interakcije na internetu (Gamax-Guadix, 2014), dok je drugo istraživanje pokazalo kako komuniciranje sa strancima na internetu predviđa povećanje osjećaja depresivnosti (Bessiere, Kiesler, Kraut i Boneva, 2008). U istraživanju Dufrasnesove (2017) utvrđeno je kako adolescenti skloni depresivnosti češće stupaju u kontakt sa strancima na internetu, češće im odaju svoje osobne informacije, nalaze se s njima licem u lice te češće traže osobu za razgovor o seksualnim temama na internetu.

Tijekom 90-ih smatrano je kako oni koji provode više vremena na internetu imaju površnije odnose u stvarnom životu jer vrijeme koje provode na internetu skraćuje vrijeme provedeno s obitelji i prijateljima, ali i oni čiji su socijalni odnosi nezadovoljavajući kompenzaciju traže upotrebom interneta. Ipak, novija su istraživanja potvrdila kako komunikacija internetom u svrhu održavanja već postojećih prijateljstava povećava socijalnu povezanost i psihičku dobrobit, odnosno potvrdila su hipotezu stimulacije prema kojoj ekstroverti imaju više kontakata i u situacijama u stvarnom svijetu i na internetu (Valkenburg i Peter, 2007). Pozitivni učinci ne postoje ukoliko su osobe sklone komuniciranju sa strancima (Bessiere i sur., 2008). Hipoteza koja objašnjava povećanu psihičku dobrobit adolescenata koji komuniciraju s prijateljima upotrebom interneta pretpostavlja kako internet smanjuje inhibicije i sramežljivost koja je karakteristična za adolescente te im dozvoljava da se slobodno izraze. Također, budući da će uporabom interneta otkriti više o sebi, adolescenti će na taj način formirati snažnija, kvalitetnija i intimnija prijateljstva (Valkenburg i Peter, 2007). Budući da su socijalni odnosi zaštitni čimbenik utjecaja stresora, tako formi-

rana kvalitetna prijateljstva unaprijedit će psihičku dobrobit osobe. Dječaci imaju više koristi od prijateljstava koja se održavaju upotrebom interneta u usporedbi s djevojčicama (Valkenburg i Peter, 2007). Pozitivni učinci komunikacije internetom ostvaruju se kada adolescenti provode vrijeme s prijateljima u stvarnom životu te kada su ta prijateljstva kvalitetna (Valkenburg i Peter, 2007).

4.3.5.3. *Seksting* i rizična spolna ponašanja

Seksting podrazumijeva slanje i primanje samoproduciranih seksualno eksplicitnih tekstualnih poruka, slika ili videozapisa mobitelom, elektroničkom poštom, društvenim mrežama i drugim sličnim medijima (Döring, 2014). Prema Hudsonu (2011) postoje četiri oblika *sekstinga*: (1) dogovorni *seksting* u kojem obje strane žele sudjelovati bez pritiska, (2) *sextbullying* pri čemu je *seksting* sredstvo za uznemiravanje, prisilu i iskorištavanje, (3) ilegalni *seksting* među maloljetnicima ili između maloljetne i punoljetne osobe te (4) rizični *seksting* koji ima negativne posljedice poput viktimizacije, ponižavanja, gubitka posla, razvoda i slično (Hudson, 2011). Od 50 akademskih članaka na temu *sekstinga* napisanih između 2009. i 2013. 33/50 (66 %) označava *seksting* kao rizično ponašanje (Döring, 2014). Istraživanjem Crofts, Lee, McGovern i Milivojevic (2014) utvrđeno je kako je 38,4 % adolescenata od 13 do 15 godina i 49,6 % adolescenata u dobi od 16 do 18 godina poslalo seksualno sugestivnu sliku sebe, a 62 % adolescenata između 13 i 15 godina te 70,1 % između 16 i 18 godina primilo je takvu sliku. Rezultati su istraživanja spolnih razlika nejednoznačni, u nekim je istraživanja dobiveno kako adolescenti češće sudjeluju u *sekstingu* (Rice, Gibbs, Winetrobe, Rhoades, Plant, Montoya i Kordic, 2014), a u nekim nisu pronađene spolne razlike (Lenhart, 2009).

Seksting može biti povezan s brojnim rizičnim ponašanjima, posebno seksualno rizičnim ponašanjima. Neka su istraživanja pokazala kako adolescenti koji prakticiraju *seksting* također ranije počinju stupati u seksualne odnose te su seksualno aktivniji, imaju više seksualnih partnera, što ih čini podložnijima riziku neželjene trudnoće i oboljenju od spolno prenosivih bolesti (Ybara i Mitchell, 2014). Upuštanje u *seksting* povezuje se i s konzumacijom alkohola i opojnih sredstava (Ybarra i Mitchell, 2014). U istraživanju Kričkić, Šincek i Babić Čikeš (2017) pronađeno je kako su sudionici koji su se upuštali u *seksting* češće bili žrtve i počinitelji nasilja upotrebom interneta. Sklonost seksualno rizičnim ponašanjima na internetu pokazuju oni slabijeg obrazovanja, oni koji traže uzbuđenje, komuniciranju češće na internetu i dolaze iz obitelji koja je manje povezana (Baumgartner, Sumter, Peter i Valkenburg 2012).

4.3.6. KARAKTERISTIKE RIZIČNIH KORISNIKA INTERNETA

Istraživanje Livingstone i Helsper (2008) utvrdilo je kako su oni koji češće komuniciraju na internetu stariji adolescenti, djevojke, česti korisnici interneta, oni koji imaju više vještina uporabe interneta, koji traže uzbuđenje u svakodnevnom životu i koji cijene anonimnost koju nudi internet. Oni koji će se sastati sa strancem kojeg su upoznali na internetu bit će stariji adolescenti, koji provode manje vremena na internetu, ali izjavljuju da imaju više internetskih vještina. Oni su manje stidljivi i vjerojatnije će tražiti uzbuđenje u svakodnevnom živote te biti nezadovoljni svojim životom. Oni koji se osjećaju sigurnijima u komuniciraju na internetu nego u stvarnim životnim situacija i cijene anonimnost interneta, vjerojatno će se susresti sa strancem kojeg upoznaju na internetu. Odavanje osobnih podataka češće je među starijim adolescentima iako nije povezano sa spolom ili socioekonomskim statusom. Te su aktivnosti također karakterističnije za one koji su nezadovoljni svojim životom, ali imaju dobre vještine uporabe interneta i cijene anonimnost koju nudi komunikacija internetom. Nadalje, traženje savjeta na internetu tipično je za one koji se rjeđe koriste internetom, vjerojatno zbog toga što je njihova upotreba interneta instrumentalna, motivirana potrebom koja je uspostavljena u stvarnom životu. Značajno je da će mladi koji odaju osobne podatke na internetu imati više rezultate na skalama traženjem uzbuđenja. Rezultati su pokazali da socijalna i psihološka obilježja djece imaju utjecaj na njihovu komunikaciju na internetu. Biti sramežljiv u stvarnom životu znači biti sramežljiv i kada se koristiš internetom, dakle sramežljivost smanjuje vjerojatnost sastanaka sa strancima. Međutim, nezadovoljstvo životom važno je iako nije povezano s češćom komunikacijom na internetu, povećava vjerojatnost rizične komunikacije što sugerira da mladi na internetu na neki način nadoknađuju nedostatke iz stvarnog života. Takvo nezadovoljstvo, kao i potreba za traženjem uzbuđenja, stoga su povezani s češćim komuniciranjem na internetu, odlascima na sastanke sa strancima, traženjem osobnih savjeta na internetu i davanjem osobnih podataka na internetu. Nedostatak otvorene komunikacije s roditeljima povećava traženje savjeta i intimnosti na internetu (Livingstone i Helsper, 2008).

Motiv za održavanjem postojećih prijateljstava na internetu nije jednak kao i motiv za upoznavanjem novih ljudi na internetu. Pretpostavlja se da će oni koji imaju nedostatak socijalnih vještina češće upoznavati nove ljude na internetu. Istraživanje Petera, Valkenburga i Schoutena (2006) potvrdilo je tu pretpostavku, međutim riječ je o vrlo niskoj povezanosti. Pretpostavlja se da će djevojke te mlađi adolescenti češće upoznavati nove ljude na internetu jer više vremena provode u komunikaciji internetom i izjavljuju kako im je ona važnija. Međutim, rezultati nekih istraživanja (npr. Peter, Valkenburg i Schouten, 2006) pokazuju kako nema razlike u navedenoj varijabli u funkciji spola, ali ima u funkciji dobi – mlađi češće razgovaraju s nepoznatima.

Pretpostavlja se kako će introverti te oni koji se internetom češće koriste također biti skloniji komunikaciji internetom, međutim neka istraživanja (npr. Peter, Valkenburg i Schouten, 2006) pokazuju kako nema povezanosti između introverzije i komunikacije sa strancima. Oni koji češće komuniciraju internetom, rjeđe će komunicirati sa strancima jer će komunikaciju internetom koristiti kako bi održavali svoja postojeća prijateljstva. Oni koji komunikaciju internetom rabe za održavanje postojećih prijateljstava vjerojatnije će se susretati s pozitivnim komentarima koji će pozitivno djelovati na njihovo samopoštovanje. Međutim, oni koji se koriste internetom kompulzivno i prekomjerno ne doživljavaju navedene pozitivne posljedice (Valkenburg i Peter, 2011).

Istraživanja pokazuju povezanost između različitih vrsta rizičnih ponašanja upotrebom interneta – oni koji odaju više osobnih informacija na društvenim mrežama ili prekomjerno/kompulzivno rabe internet ponašaju se rizičnije i u drugim situacijama (Karl, Peluchette i Schlaegel, 2010). Emocionalno stabilni, savjesni i ugodni pojedinci ponašaju se opreznije na internetu (Karl, Peluchette i Schlaegel, 2010). Također, otkrivanje osobnih informacija na internetu povezano je s otkrivanjem osobnih informacija u interakcijama licem u lice (Cho, 2007). Muški su sudionici iskreniji u otkrivanju osobnih informacija i pokazuju više seksualno rizičnih ponašanja nego ženski sudionici (Cho, 2007). Kliničke varijable poput narcisoidnosti, histrionskih oblika ponašanja, impulzivnosti i ovisnosti o drugima povezane su s rizičnijim ponašanjima na internetu (Campbell, Goodie i Foster, 2004).

4.3.7. ČIMBENICI KOJI PREDVIĐAJU PREKOMJERNU UPOTREBU INTERNETA

Ovisnost o internetu predstavlja stanje u kojemu pojedinac gubi kontrolu nad upotrebom interneta i rabi ga prekomjerno što utječe na kvalitetu njegova života (Young, 1998). Internetski ovisnici provode 40 do 80 sati tjedno na internetu (Young, 1998). Osobe koje pokazuju znakove ovisnosti o internetu doživljavaju poteškoće u akademskom, međuljudskom, financijskom, profesionalnom i fizičkom funkcioniranju. Za razliku od dijagnoze ovisnosti o psihoaktivnim tvarima, dijagnoza ovisnosti o internetu znatno je kompleksnija s obzirom na to da je, za razliku od alkohola i droga, internet dio našeg osobnog i profesionalnog života te je samim time znakove ovisnosti lakše opravdati.

Istraživanja karakteristika osoba koje se prekomjerno koriste internetom pokazala su kako su to osobe sklone fantaziranju, stidljive, socijalno anksiozne, sniženog samopoštovanja, fobične i nezadovoljne svojim socijalnim statusom (Hamburger, Ben-Artzi, 2003). Hamburger i Ben-Artzi (2000) utvrdili su kako su ekstraverzija i

neuroticizam značajni prediktori prekomjerne upotrebe interneta. Navedeni autori smatraju kako se ekstroverti češće koriste internetom zbog želje za druženjem, dok Hinić (2008) navodi kako introvertirane osobe, kao i one s neurotskim crtama ličnosti, vide mogućnost iskazivanja svoga „pravog ja" isključivo u zajednicama na internetu. Rakić-Bajić i Hedrih (2012) navode kako se pregledom literature može zaključiti kako su istraživanja kvalitete života i upotrebe interneta nejednoznačna, a veza između zadovoljstva životom i prekomjerne upotrebe interneta ostvaruje se posredno savjesnošću. Savjesni pojedinci rjeđe se koriste internetom i u manjoj su mjeri o njemu ovisni. Navedeni autori pokazali su kako muški sudionici pokazuju viši stupanj prekomjerne upotrebe interneta u odnosu na sudionice. Razlog tomu može biti što su muškarci u našoj kulturi još uvijek više upućeni na upotrebu računala pa se samim tim i više koriste internetom nego žene. Sudionici sa srednjom stručnom spremom skloniji su većem pretjerivanjem u uporabi interneta nego sudionici s visokom stručnom spremom.

Čak 30 % djece od 11 do 16 godina prijavljuje jedno ili više iskustava glede prekomjerne uporabe interneta (npr. zanemarivanje prijatelja, školskog rada ili nedostatni san), dok 17 % djece izjavljuje kako su zanemarili hranu i san zbog interneta – 5 % izjavljuje da se to događa često ili vrlo često. Razlike u dobi velike su, 23 % djece od 11 do 12 godina te 36 % djece od 15 do 16 godina suočavaju se s posljedicama pretjerane upotrebe interneta. Pretjerana upotreba interneta nije povezana sa socioekonomskim statusom, ali je sa spolom – dječaci su nešto neumjereniji u upotrebi interneta. Prekomjerna upotreba interneta povezana je s traženjem uzbuđenja (kao crtom ličnosti), psihološkim poteškoćama (depresivnošću, hiperaktivnošću, poremećajem ophođenja i problemima u vršnjačkim odnosima), rizičnim iskustvima na internetu, slanjem seksualnih poruka, činjenjem nasilja u tradicionalnom obliku i na internetu (Livingstone i sur., 2011).

Zabrinjavajući podatak je da čak 16,5 % srednjoškolaca više od 5 sati dnevno provede služeći se internetom (Đuraković i Klasnić, 2016). Istraživanje Vejmelke, Starbića i Jazbo (2017) pokazalo je kako čak trećina srednjoškolaca pokazuje umjerene do teške znakove ovisnosti o internetu. Istraživanje Poliklinike za zaštitu djece grada Zagreba iz 2013. godine pokazalo je da djeca koja imaju manju kontrolu nad upotrebom interneta (primjerice, teže im je otići s interneta, češće razmišljaju o internetu kad se njime ne koriste, više zanemaruju svoje obveze zbog interneta i sl.) imaju lošiju sliku o sebi, tjeskobnija su, pokazuju više simptoma depresivnosti te su sklonija neprihvatljivom ponašanju. Ovisnost o medijima pokazala se pozitivnim prediktorom niza rizičnih ponašanja adolescenata (seksualno rizično ponašanje, konzumacija alkohola, nasilje na internetu) (Livazović, 2012). Istraživanje Livazovića (2012) također je pokazalo kako oni koji više vremena provode u potrazi za obrazovnim

sadržajima imaju manju vjerojatnost stvaranja ovisnosti o internetu u odnosu na one koji se internetom uglavnom koriste za zabavu. Adolescenti skloniji obrazovnim sadržajima medijski su kompetentniji i pismeniji (gimnazijalci i djeca visokoobrazovanih roditelja, stariji adolescenti, sudionici koji su manje agresivni te izvještavaju i o kvalitetnijim vršnjačkim odnosima i slobodnovremenskim aktivnostima). Možda obrazovni sadržaji (te obrazovaniji roditelji) osim veće količine i kvalitete informacija koju donose, utječu na kritičnost koja se smatra jednom od osnovnih sastavnica medijske kompetencije. Zabavni sadržaji pozitivan su prediktor rizičnom seksualnom ponašanju, ovisnosti o medijima i strahu od okoline. Moguće je kako su zabavni sadržaji, dakle glazbeni spotovi, humoristične serije za mlade, *reality* emisije, reklame, komedije prepuni različitih seksualno ambivalentnih, stereotipno profiliranih poruka. Istraživanje Livazovića (2012) pokazalo je kako gimnazijalci više vremena na internetu provode u pregledavanju obrazovnih sadržaja, dok učenici trogodišnjih i četverogodišnjih strukovnih škola više vremena provode u pregledavanju zabavnih sadržaja.

Rezultati istraživanja Livazovića (2012) pokazuju i kako je strah od okoline povezan s ovisnošću o medijima. Navedeno se može objasniti time da mladi sa strahom od okoline rjeđe izlaze pa stoga više vremena provode koristeći se medijima. Međutim, možda upravo vrijeme i značaj koji pridaju medijima, kao i informacijama kojima su izloženi, uzrokuje povećano nepovjerenje i strah od okoline. Također, mladi koji pokazuju blagu, umjerenu ili visoku razinu ovisnosti o internetu značajno češće čine nasilje na internetu od mladih kod kojih ne postoje znakovi ovisnosti.

4.3.8. SIGURNOST PODATAKA DJECE I MLADIH NA INTERNETU - ZNANJE O RIZICIMA I RIZIČNA PONAŠANJA

Elektornički kriminal (engl. *cyber*) predstavlja oblik kriminalnog ponašanja kod kojeg se uz pomoć kompjutorske tehnologije i interneta čini kazneno djelo (Symantec, 2010). Na internetu postoje razne kriminalne aktivnosti, npr. kršenje autorskih prava, ilegalno preuzimanje glazbe, filmova, knjiga, igrica, trgovina oružjem, ljudima, identitetima, ljudskim organima, prostitucija, krađa novca s bankovnih računa i sl. Šteta koja nastaje kao posljedica elektroničkog kriminala psihološka je i često neopipljiva što otežava pravni postupak protiv počinitelja čak i ukoliko se zna njegov identitet. Najpoznatiji način prijevare takozvano je „pecanje“ (engl. *phishing*), a predstavlja krađu identiteta u kojem pošiljatelj navodi žrtvu da otkrije osobne informacije (obično financijske) na lažnoj internetskoj stranici. Poruka koja predstavlja „udicu“ (engl. *hook*) može izgledati kao obavijest iz banke, zahtjev policije, internetske trgovine i sl., a navodi žrtvu da klikne na poveznicu. Naravno, djeca su ugroženija populacija jer su lakovjerna i sklinija su biti žrtvom prijevare. Za smanjenje rizika od

elektroničkog kriminala potrebno je povećati svijest korisnika o potencijalnim prijetnjama na internetu te usvajanje znanja, tj. informatičke pismenosti. Korisnici interneta često nisu svjesni rizika koji postoje te se ponašaju neoprezno. Osobne podatke potrebno je zaštititi na odgovarajući način, pravilno ih pohraniti te drugim osobama ograničiti pristup vlastitim podacima (Symantec, 2010).

U istraživanju Velki, Šolića i Nenadića (2015) dobivene su pozitivne povezanosti između različitih oblika rizičnog ponašanja računalnih korisnika i blažeg rizičnog i delikventnog ponašanja. Osobe koje su sklonije blažim oblicima rizičnog i delikventnog ponašanja sklonije su i uobičajenim rizičnim ponašanjima pri uporabi računala, neodržavanju računalnih sustava i posuđivanju pristupnih podataka drugim osobama.

Istraživanje Velki, Šolića, Gorjanac i Nenadića (2017) pokazalo je kako kod adolescenata postoji povezanost između uključenosti u nasilje internetom i rizičnog ponašanja na internetu, posuđivanja pristupnih podataka te neredovitog održavanja računalnih sustava. Navedeno istraživanje pokazalo je kako će velik broj sudionika otkriti svoju zaporku e-pošte ako to od njih traže istraživači. Učenici srednjih škola češće otkrivaju svoje zaporke u odnosu na odrasle osobe (77 % naprama 51 %). Također, općenito su neopreznji i smatraju pojedine aktivnosti na internetu sigurnijima od odraslih. Osobe koje većem broju ljudi daju svoju zaporku pokazuju rizična ponašanja u vidu slabog održavanja računalnih sustava, smatraju kako je internetska komunikacija sigurna te ne znaju kako pravilno pohraniti i čuvati računalne podatke. Znanje o informacijskoj sigurnosti ne razlikuje se kod sudionika koji su odali i onih koji nisu odali svoju zaporku. Štoviše, učenici koji su svjesniji opasnosti na internetu ponašaju se rizičnije. Rezultati govore u prilog tezi da, iako većina osoba ima određena znanja, prijenos tih znanja u područje sigurnosnih ponašanja pri upotrebi računala očito nije uspješan (Velki i sur., 2017) .

Muškarci za razliku od žena smatraju da je komunikacija računalom sigurnija (Velki, Šolić i Nenadić, 2015). Također, žene smatraju da postoji veća vjerojatnost da će im netko ukrasti osobne podatke. Srednjoškolke redovitije održavaju računalne sustave od srednjoškolaca, no nema razlike u rizičnim ponašanjima na internetu u funkciji spola (Velki i sur., 2017). U istraživanju Velki i Romstein (2018) dobivene su značajne interakcije između spola i dobi, žene s godinama postaju opreznije u ponašanju, dok su muškarci oprezniji u adolescenciji i starijoj dobi, a najrizičniju skupinu predstavljaju muški studenti.

Savjesnost, otvorenost prema iskustvu i ugodnost pozitivni su prediktori slijeđenja sigurnosnih pravila glede zaštite osobnih podataka i svijesti o važnosti zaštite osobnih podataka (McCormac i sur., 2016). Ovisnost o internetu i impulzivnost prediktori su rizičnom ponašanju na internetu. Osobe koje su staloženije i imaju veću

kontrolu nad svojim emocijama češće će brisati te neće otvarati sumnjivu e-poštu (Welk, Hong, Zielinska, Tembe, Murphy-Hill i Mayhorn, 2015).

Istraživanje Reynsa (2013) utvrdilo je kako su osobe starije životne dobi, muškog spola te boljeg materijalnog statusa češće žrtve krađe osobnih podataka na internetu. Ti su pojedinci i svjesniji da postoji mogućnost krađe podataka. Autor ističe kako postoji velika razlika između ponašajnih namjera i samog ponašanja glede sigurnosti osobnih podataka. Oni koji češće koriste e-poštu, instant poruke, kupnju internetom te uporabu interneta u svrhu preuzimanja sadržaja i bankovnih transakcija, u većem su riziku od krađe podataka što je u skladu s teorijom rutinskih aktivnosti. Teorija rutinskih aktivnosti objašnjava kako svakodnevne rutinske situacije stvaraju prilike da pojedinci postanu žrtve prevare na internetu (Bossler i Holt, 2010). Navedena teorija pretpostavlja kako se svakodnevnom upotrebom interneta, u kojoj su prisutni elementi motiviranoga „počinitelja" (osobe sklone vršenju namjernih neprihvatljivih radnji), prikladne „mete" (osobe koja je iz perspektive „počinitelja" percipirana kao ranjiva ili pogodna „žrtva") te kod djece i adolescenata često i odsutnost skrbnika povećavaju vjerojatnost krađe podataka ili prevare na internetu.

Chibnall, Wallace, Leicht i Lunghofer (2006) zaključili su kako su se programi o sigurnosti na internetu pokazali učinkovitima za povećanje znanja o sigurnim strategijama na internetu, međutim nisu smanjili rizična ponašanja na internetu. Nepostojanje razlike u otkrivanju podataka na društvenim mrežama prije i poslije intervencije može se objasniti time da učenici, unatoč primjeni programa osvještavanja problema sigurnosti na internetu, sigurnosne strategije teško primjenjuju. Kako bismo razumjeli zašto se adolescenti upuštaju u rizična ponašanja i otkrivaju podatke o sebi na internetu i nakon edukacije o rizičnosti takvih ponašanja, trebalo bi uzeti u obzir njihova razmišljanja i motive koje se odnose na društvene mreže.

4.4. SAVJETI ZA SIGURNIJU UPORABU INTERNETA

4.4.1. RODITELJSKI NADZOR NAD DJEČJOM UPOTREBOM INTERNETA

Nathanson (2001) razlikuje tri roditeljske strategije regulacije koje se odnose na medijske sadržaje:

1) Aktivno posredovanje (razgovor o medijima) koje može imati poželjne posljedice usmjeravajući djecu da postaju skeptičniji prema medijskom sadržaju i razviju veća znanja o posljedicama, kao i smanjiti vjerojatnost nasilnog ponašanja ili stavova.

2) Zajedničko korištenje (npr. djeca i roditelji zajedno se koriste medijima) pokazalo se čak učinkovitijim, ali samo u nekim okolnostima.

3) Ograničavajuće posredovanje (zadavanje pravila – koliko i kojim se medijima koristiti, u kojim situacijama, bez objašnjenja pravila) koje varira u djelotvornosti, a neki autori smatraju kako ne umanjuje rizik kojim su izložena djeca (npr. Livingstone i Helsper, 2008).

Na temelju Nathansonove kategorizacije Livingstone i Helsper (2008) utvrdili su pet vrsta roditeljskih medijacija koje se mogu javiti prilikom dječje upotrebe interneta:

1) aktivno posredovanje (roditelji su prisutni i pomažu djetetu kada se koristi internetom)

2) posredovanje koje uključuje poticanje djece na sigurnu upotrebu interneta (raspravljaju o sigurnom ponašanju, pružaju savjete i podučavaju kako se ponašati na internetu)

3) posredovanje uspostavljanjem granica ponašanja (roditelji postavljaju određena pravila i ograničenja)

4) praćenje (stalna provjera internetskih stranica koja djeca posjećuju)

5) postavljanje tehničkih ograničenja (blokiranje i filtriranje internetskih stranica, praćenje posjećenih internetskih stranica ili postavljanje vremenskog ograničenja).

Od 24 medijacije ponuđene u istraživanju Livingstone i sur. (2011) rezultati pokazuju kako roditelji u prosjeku implementiraju sedam do osam medijacija. Aktivno posredovanje prilično je raširena strategija (Livingstone i sur., 2011), dvije trećine roditelja razgovara s djetetom o upotrebi interneta, gotovo polovina prati zaslon dok je dijete na internetu, a trećina je u blizini kada je njihovo dijete na internetu. Oni roditelji koji se koriste aktivnim posredovanjem, imaju djecu razvijenijih vještina služenja internetom (Livingstone i sur., 2011). Nadalje, neki roditelji primjenjuju različita ograničenja, zabranjujući im e-poštu (43 %), preuzimanje sadržaja (17 %) ili komunikaciju u sobama za razgovor na internetu (13 %). Tehnička ograničenja također provodi 33 % roditelja koji imaju instaliran softver za filtriranje, međutim 20 % nije znalo ili nije bilo sigurno imaju li instaliran filtar što ukazuje na ograničenja roditeljskih vještina uporabe interneta. Neki prate računalo nakon što je dijete završilo s upotrebom, 30 % pregledava stranice koje je dijete posjetilo, a 17 % provjerava dječju e-poštu. Ipak, čini se da je aktivno posredovanje najčešća strategija koju roditelji primjenjuju u praćenju dječjih aktivnosti, dok je uobičajeno i ograničavanje aktivnosti. Također, roditelji znatno više pravila zadaju mlađoj djeci u odnosu na starije. Roditelji višeg socioekonomskog statusa zadaju više pravila. Istraživanje Eastina, Greenberga i Hofschirea (2006) pokazuje kako se autoritarni roditelji najčešće koriste strategijama

restriktivne medijacije. Neka istraživanja pokazuju kako djevojčice percipiraju više kontrole od strane roditelja (Livingstone i sur., 2011), neka su utvrdila kako roditelji s boljim vještinama služenja internetom bolje nadgledaju dječju upotrebu interneta (npr. Livingstone, 2011), dok druga (npr. Lou, Ru-Chu, Hung-Tzu, Yuan-Chang i Kuo-Hung., 2010) sugeriraju kako roditelji koji su medijski pismeniji više vjeruju svojoj djeci, manje ograničavaju njihovu upotrebu interneta te su manje svjesni rizika koji se mogu javiti na internetu.

Skup roditeljskih postupaka ili ponašanja kojim roditelji prate aktivnosti djece naziva se roditeljski nadzor (Borawski, Ievers-Landis, Lovegreen i Trapl, 2003). Roditeljski nadzor važan je čimbenik koji može utjecati na različita ponašanja. Roditeljski nadzor nad dječjom upotrebom interneta ima zaštitno djelovanje na djecu kada se ona susretnu s uznemirujućim sadržajem (Livingstone i sur., 2011). Uključenost roditelja može smanjiti rizik od nasilja na internetu od strane vršnjaka. Dijete koje dijeli svoje brige s roditeljima i traži savjete oko ponašanja na internetu roditelji mogu obeshrabriti u druženju s nasilnim vršnjacima (Ybarra i Mitchell, 2007). Istraživanja pokazuju da djeca i mladi skloni činjenju nasilja često dolaze iz obitelji u kojima nedostaje emocionalnosti i uključenosti roditelja (Ybarra i Mitchell, 2004) te obitelji pretjerano kontrolirajućeg ponašanja (Kuterovac-Jagodić i Keresteš, 1997). Istraživanja su pokazala da djeca s niskom samoregulacijom, slabim vodstvom i roditeljskim nadzorom češće imaju javne, a manje privatne profile na Facebooku (Livingstone i sur., 2011).

Postoje određeni izazovi za procjenu valjanosti konstrukta roditeljskog nadzora budući da neki autori tvrde kako je to ustvari mjera „roditeljskog znanja", a ne aktivnih nastojana roditelja da prate aktivnost svoga djeteta. Istraživanja (npr. Kerr, Stattin i Burk, 2010) su pokazala da je roditeljsko znanje (a ne ograničenja) povezano s manje rizičnih ponašanja djece. Valcke, Bonte, De Wever i Rots (2010) definiraju roditeljske internetske stilove po uzoru na klasičnu podjelu roditeljskih stilova te osim roditeljskog nadzora govore i o roditeljskoj toplini, tj. emocionalnosti. Emocionalnost je dimenzija roditeljskog ponašanja koja se odnosi na emocije ljubavi i privrženosti prisutne u interakciji s djetetom. *Permisivni stil roditeljstva* imaju roditelji koji nemaju jasno postavljene granice oko upotrebe interneta, nastoje djeci udovoljiti te se suzdržavaju od svađe s djecom. *Ravnodušni stil* odražava nisku razinu nadzora i nisku razinu uključenosti (topline) te se odnosi na roditelje koji ne pokazuju pravilno podržavanje niti ograničavanje djece kada je riječ o upotrebi interneta. *Autoritativni stil roditeljstva* odnosi se na roditelje koji određuju jasna pravila, s djecom otvoreno razgovaraju o tim pravilima te pružaju podršku svom djetetu. *Autoritarni stil roditeljstva* karakterizira provedba pravila bez objašnjenja i diskusije.

Istraživanja pokazuju kako su podržavajući oblici odgoja s odgovarajućom kontrolom povezani s manje rizičnih ponašanja te manjom razinom depresivnosti

adolescenata (Aquilino i Supple, 2001). Također, rizična ponašanja na internetu povezana su sa slabijim nadzorom roditelja, nižom emocionalnosti roditelja, nižim posredovanjem prilikom upotrebe interneta djece, većim provođenjem vremena djeteta za računalom te slabim druženjem roditelj – dijete (Ybarra i Mitchell, 2004).

Podaci dobiveni u nacionalnom istraživanju o upotrebi informacijsko-komunikacijskih tehnologija djece i mladih u Republici Hrvatskoj koje je financirala Europska unija u okviru projekta „Safer Internet Centre Croatia – Making internet a good and safe place" utvrdilo je kako 62,6 % desetogodišnje djece navodi kako roditelji ograničavaju njihovu upotrebu interneta, kako 51,3 % djece razgovara s roditeljima o sadržaju koji objavljuju, no 54,9 % njih navodi kako roditelji ne nadgledaju njihovu upotrebu društvenih mreža (Lagator, Šincek i Duvnjak, 2018). Čak 90,2 % djece iskazuje kako poštuje pravila koja roditelji postave o upotrebi interneta. Djeca koja percipiraju visoku razinu roditeljskog nadzora provode više vremena dnevno u dopisivanju s prijateljima nego što to čine oni koji percipiraju nisku razinu nadzora. Djeca koja percipiraju visoku razinu nadzora češće pronalaze motivaciju za pristupanje internetu u svrhu traženja informacija koje se odnose na školske obveze. Više osobnih podataka objavljuju oni koji percipiraju viši nadzor. Djeca koja percipiraju visoku i ona koja percipiraju nisku razinu nadzora ne razlikuju se u vremenu koje utroše dnevno na aktivnosti na internetu. Desetogodišnji dječaci i djevojčice ne razlikuju se u percepciji roditeljskog nadzora ponašanja na internetu (Lagator i sur., 2018).

Moguće je razlikovati pozitivnu roditeljsku regulaciju (poticanje određenih aktivnosti) i negativnu roditeljsku regulaciju (zabranjivanje i onemogućavanje određenih aktivnosti) (Livingstone i Helsper, 2008). Istraživanja pokazuju kako roditelji najčešće koriste kombinaciju navedenih strategija, od otvorenog, nedirektivnog pristupa do kontrolirajućeg i restriktivnog. Neki autori taj pristup smatraju pristupom koji je previše orijentiran na roditelja i zanemaruje potrebe i interese djeteta koje je aktivno u odnosu na internetske sadržaje. Neka istraživanja pokazuju kako se roditeljske zabrane poput zabrane upotrebe e-pošte, komunikacije u sobama za razgovor na internetu ili odavanja osobnih informacija ne pokazuju uspješnima (Livingstone i Helsper, 2008, Livingstone i Bober, 2006), dok druga istraživanja pokazuju kako su tehnička ograničenja roditelja (filtriranje stranica i sl.) povezana s manjim doživljavanjem rizičnih iskustava i osjećaja uznemirenosti djece na internetu (Livingstone i sur., 2011). Istraživanje Fleminga i sur. (2006) utvrdilo je kako roditeljsko instaliranje softwarea za blokiranje određenih stranica ne umanjuju izloženost djece tim stranicama, dok je razgovor roditelja s djecom pozitivan prediktor sigurnijem ponašanju djeteta na internetu.

Djeca i roditelji u određenoj mjeri smatraju da je roditeljsko posredovanje pri uporabi interneta korisno (Livingstone i sur., 2011). Djeca koja su bile žrtve nasilja na

internetu, kojima su poslane seksualne poruke ili koja su se susrela s osobom koju su upoznali na internetu te doživjela neugodno iskustvo često izjavljuju kako ih „nitko nije pitao pravo pitanje kada je za to bilo vrijeme“, odnosno njihova iskustva svjedoče o nedostatku uključenosti i potpore roditelja ili skrbnika (Livingstone i sur., 2011). Više od dvije trećine djece izjavljuje kako im roditeljski savjeti mnogo ili malo pomažu. Djeca od 9 do 12 godina pozitivnija su što možda odražava njihov relativni nedostatak vještina, za njih je roditeljsko posredovanje korisnije. Adolescenti (13–16 godina) nešto su kritičniji od svojih roditelja (38 % ih izjavljuje da im roditeljski savjeti ne pomažu, u usporedbi sa 30 % roditelja koji se slažu s navedenim). Čak 29 % djece izjavljuje kako djelomice ignorira roditeljske savjete i pravila, a 7 % djece izjavljuje kako to čini često. Ipak, 15 % djece voljelo bi da su njihovi roditelji uključeniji u njihovu upotrebu interneta, dok 12 % djece želi da su roditelji manje uključeni.

Podizanje svijesti o postojanju problema jedan je od prvih koraka u bilo kojem programu prevencije (Buljan Flander, 2008). Istraživanja pokazuju da se najveći broj ponašanja karakteriziranih kao nasilje i izlaganje neprimjerenim sadržajima na internetu dogodio dok odrasli nisu obraćali pozornost na ono što djeca rade. Iz tog razloga osobno računalo trebalo bi biti u dnevnoj sobi gdje je lakše nadzirati aktivnosti djece (Buljan Flander, 2008). Važno je razlikovati roditeljski nadzor od pojma roditeljske kontrole (bihevioralne i psihološke) koji podrazumijeva nametljivo roditeljsko ponašanje, prisilu, strogo kažnjavanje i agresiju te je povezano s češćim činjenjem i doživljavanjem kako tradicionalnog tako i nasilja na internetu (Kuterovac-Jagodić i Keresteš, 1997, Buljan, Dugić i Handabaka, 2015).

4.4.2. MIŠLJENJA RODITELJA I DJECE O RIZICIMA NA INTERNETU

Istraživanja provedena u 25 zemalja Europske unije (Livingstone i sur., 2011) pokazuju kako roditelji podcjenjuju rizike kojima su djeca izložena na internetu (npr. samo 5 % roditelja smatra da je dijete odalo određenu osobnu informaciju, dok u stvarnosti to čini gotovo 50 % djece). Samo 7 % roditelja misli kako se njihovo dijete susrelo sa seksualnim komentarima na internetu, a samo 4 % roditelja misli kako je njihovo dijete bilo zlostavljano na internetu (izjave djece o navedenim događajima dvostruko su češće). Možda su uzroci tih razlika metodološki – „seksualni komentari“ ili „nasilje na internetu“ možda imaju drukčije značenje roditeljima i djeci. Roditelji najviše podcjenjuju probleme koje doživljava najstarija dobna skupina (Livingstone i Bober, 2006).

Samo 42 % djece izjavljuje kako su im roditelji uspostavili pravila o tome koliko dugo smiju biti na internetu (Livingstone i Bober, 2006), a 43 % roditelja izjavljuje isto. Međutim, 20 % djece izjavljuje kako ne smiju ispunjavati ankete na internetu,

dok 57 % roditelja smatra da su zadali djeci takvo pravilo, 40 % djece svjesno je pravila da ne smije koristiti sobe za razgovor na internetu, dok 62 % roditelja smatra kako su navedeno zabranili djeci. Samo 33 % djece izjavljuje kako su ih roditelji upozorili kako nisu sve informacije koje se nađu na internetu pouzdane, dok 41 % roditelja izjavljuje da je to učinilo i kako su sigurni da njihova djeca to znaju učiniti. Očito postoje određena nerazumijevanja između djece i roditelja oko uspostavljenih pravila, odnosno nekoj djeci uspostavljena pravila nisu dovoljno jasna (Livingstone i Bober, 2006). Roditelji često pretpostavljaju da se njihovo pravilo poštuje, što nije uvijek slučaj te kako pravila ponekad nisu bi potrebna.

Trećina djece od 9 do 17 godina izjavljuje kako im roditelji pomažu u upotrebi interneta i sugeriraju koje stranice posjetiti, također trećina ih izjavljuje kako roditelji nadgledaju njihovu upotrebu interneta, međutim samo kod petine djece roditelji ostaju u istoj sobi kao i dijete kada je na internetu. Čak 81 % roditelja izjavljuje kako znaju što im djeca pretražuju na internetu, 51 % njih kako pomažu djeci na internetu, a 50 % da su prisutni u sobi zajedno s djetetom kada je ono na internetu. Kada se ista pitanja postave roditeljima i djeci, očito je kako se njihovi odgovori ne podudaraju u potpunosti (Livingstone i Bober, 2006).

Roditeljima je ponekad vrlo teško pratiti aktivnost djeteta na internetu, mnogo teže nego što je pratiti sadržaje koje dijete gleda na televiziji budući da je danas internet dostupan svuda – u školi, knjižnici, na mobilnim uređajima itd. (Livingstone i Bober, 2006). Djeca također izražavaju svoje nezadovoljstvo roditeljskom kontrolom i pretjeranom stigmatizacijom interneta i medija općenito kao izvorima velike opasnosti. Sloboda i neovisnost mladih ljudi u sukobu je s nastojanjima roditelja da ih prate i provjeravaju. Nije rijedak slučaj da što više roditelji pokušavaju ograničiti i kontrolirati aktivnost svoje djece na internetu, djeca se sve više trude izmaći kontroli. Više od trećine djece izjavljuje kako je obrisalo e-poštu kako ju roditelji ne bi vidjeli, a 17 % djece obrisalo je povijest svojih pretraživanja (Livingstone i Bober, 2006).

Čak 44 % djece izjavljuje da je od prijatelja dobilo neke smjernice za sigurnu uporabu interneta, a 35 % djece izjavljuje kako je pružilo takav savjet svojim prijateljima (Livingstone i sur., 2011). Oko polovine djece misli da su njihovi učitelji angažirani u osvješćivanju pravila sigurne upotrebe interneta, 73 % djece izjavljuje kako su njihovi učitelji proveli barem jedan od oblika aktivnog posredovanja. Usporedbom svih izvora sigurnosnih savjeta može se zaključiti kako je većina savjeta primljena od roditelja (63 %), zatim nastavnika (58 %) i vršnjaka (44 %). Na subjektivni dječji osjećaj uznemirenosti i štete uzrokovane aktivnostima na internetu najviše utječu roditeljske medijacije, dok medijacije prijatelja i nastavnika imaju vrlo skroman, gotovo zanemariv utjecaj. Ako na dijete utječe roditelj, najvjerojatnije će se i utjecaj nastavnika pokazati značajnim (Livingstone i sur., 2011).

Samo oko 9 % roditelja izjavljuje kako ne žele dodatne informacije o internetskoj sigurnosti. Roditelji bi najradije dobili informacije o internetskoj sigurnosti u djetetovoj školi tako da je potrebno poticati škole da se uključe u informiranje roditelja glede internetske sigurnosti (Livingstone i sur., 2011).

4.4.3. PREPORUKE ZA ZAŠTITU DJECE I SIGURNU UPOTREBU ELEKTRONIČKIH MEDIJA

U monografiji Preporuke za zaštitu djece i sigurnu uporabu elektroničkih medija (2016) autorice Kuterovac Jagodić, Štulhofer i Lebedina Manzoni ukazuju na važnost roditeljskih medijacija prilikom uporabe medija te navode brojne praktične savjete za roditelje ukratko opisane u nastavku.

Aktivno posredovanje prilikom uporabe audiovizualnih sadržaja podrazumijeva različite aktivnosti u kojima roditelji s djecom razgovaraju o sadržajima koje će gledati i zašto, odnosno o sadržajima koji nisu primjereni za gledanje i zašto te o sadržajima koje su gledali i kako su ih razumjeli. Važno je da roditelji s djecom interpretiraju sadržaje, pojašnjavaju ih, raspravljaju i daju svoja mišljenja o njima. Dijete treba pitati što mu je u medijskim sadržajima zanimljivo, kako si tumače određene događaje i postupke likova, što misle o nekim temama, kakve osjećaje određeni sadržaji u njima bude i sl. Djetetu je potrebno pomoći pronaći alternativna objašnjenja, ukazati na neprimjerenost nekih tvrdnji, scena i postupaka likova. Potrebno je razgovarati o drugim, nenasilnim načinima rješavanja određenih situacija. Djeca čiji roditelji negativno komentiraju nasilne scene i agresivna ponašanja likova lakše ga prepoznaju i na njega reagiraju u stvarnome životu.

Ako dijete i vidi neke potencijalno štetne, neprimjerne i uznemirujuće sadržaje, ne bi trebali preko njih samo prijeći šutnjom već o njima raspraviti s djetetom. Djecu je potrebno upozoriti na opasna ponašanja i protumačiti im zašto ih ona ne bi trebala činiti i kako bi ih mogla dovesti u opasnost. Osobito je važno razgovarati o uznemirujućim vijestima o nesrećama i drugim opasnostima kojih se djeca mogu bojati.

Trebamo poticati dijete na kritičnost kod biranja sadržaja, ali i na kritičko analiziranje i vrednovanje kvalitete viđenog medijskog sadržaja, iznesenih ponašanja, postupaka, stavova, mišljenja. Korisno je ukazati adolescentima kako mediji mogu utjecati na njihovo samopoštovanje i sliku svijeta. Dobro je ukazati i na sadržaje koji potiču spolnu, seksualnu, dobnu, rasnu, nacionalnu diskriminaciju te koji potiču izgradnju kulta tijela, stereotipe, konzumerizam, odnosno na sadržaje koji promoviraju određeni neprimjereni stil života i neprimjerene vrijednosti, neprihvatljiva ponašanja, rasizam, nacizam, kriminal i sl.

Roditelji bi trebali donijeti obiteljsko pravilo da se televizor i druge medijske platforme ne uključuju niti gledaju dok nisu izvršene školske i druge obveze, ne dopustiti djetetu da gleda neprimjerene sadržaje, osobito one s nasiljem i seksualnim sadržajima. Potrebno je osigurati dovoljno vremena za djetetove druge aktivnosti: igru, druženje s vršnjacima i obitelji, učenje, tjelesne i ostale aktivnosti izvan kuće. Roditelji svojoj djeci trebaju biti dobar uzor u restriktivnom pristupu korištenju televizije i medijskih platformi i razmišljanju o kvaliteti sadržaja. Roditelji bi se trebali držati pravila koja su zajednički donijeli, posebice da se mediji ne koriste tijekom obiteljskih aktivnosti. Također, trebaju se informirati o mogućnosti tehničke zaštite djece od štetnih sadržaja pinovima ili kodovima, posebnim prekidačima i programatorima vremena, filterima, ključevimaa za električne kabele i sl.

Roditelji trebaju potaknuti dijete da gleda obrazovne, dokumentarne i kvalitetne programe te s njim razgovarati o viđenome. Djetetu treba pokazati da nam je stalo do njihovih interesa pa se trebamo upoznati sa sadržajima koje ono voli.

4.5. LITERATURA

Anderson, C. A. i Bushman, B. J. (2001). Effects of violent video games on aggressive behaviour, aggressive behaviour, aggressive cognition, aggressive affect, psychological arousal, and prosocial behaviour: A Meta-Analytic Review of the Scientific Literature. *American Psychological Society*, *12*(5), 353-359.

Aquilino, W. S. i Supple, A. J. (2001). Long-term Effects of Parenting Practice during Adolescence on Wellbeing: Outcomes in Young Adulthood. *Journal of Family Issues*, *22*(3), 289-308.

Bandura, A. (1986). *Social foundations of thought and action: A socialcognitive theory*. Englewood Cliffs, NJ: Prentice-Hall.

Berkowitz, L. (1993). *Aggression: Its causes, consequences, and control*. New York: McGraw Hill.

Bargh, J. A. i McKenna, K. Y. A. (2004). The Internet and Social Life. *Annual Review of Psychology, 55*, 573-590.

Baumgartner, S. E., Valkenburg, P. M. i Peter, J. (2010). Unwanted online sexual solicitation and risky sexual online behavior across the lifespan. *Journal of Applied Developmental Psychology, 31*(6), 439-447.

Baumgartner, S. E., Sumter, S. R., Peter, J. i Valkenburg, P. M. (2012). Identifying Teens at Risk: Developmental Pathways of Online and Offline Sexual Risk Behavior. *Pediatrics, 130*(6), 1489-1496.

Bessiere, K., Kiesler, S., Kraut, R. i Boneva, B. S. (2008). Effects of Internet use and social resources on changes in depression. *Information, Communication & Society, 11*(1), 47-70.

Bilić, V. (2010). Povezanosti medijskog nasilja s agresivnim ponašanjem prema vršnjacima. *Odgojne znanosti,12*(2), 263-281.

Borawski, E. A., Ievers-Landis, C. E., Lovegreen, L. D., i Trapl, E. S. (2003). Parental monitoring, negotiated unsupervised time, and parental trust: The role of perceived parenting practices in adolescent health risk behaviors. *Journal of Adolescent Health*, *33*(2), 60-70.

Bossler, A. M. i Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, *38*(3), 227 -236.

Brstilo, I., Batinić, L. i Grgić, S. (2014). Navike djece i mladih kod objavljivanja osobnih podataka na društvenim mrežama. *Sociološka luča, 8*(2), 105-121.

Buljan Flander, G. (2008). Internet i djeca – trebamo li brinuti? (Internet and children – should we be worried?). *Proceedings from third conference on violence "Violence among and against children"*, Croatia, 13-22.

Buljan Flander, G., Ćosić, I. i Profaca, B. (2009). Exposure of children to sexual content on the Internet in Croatia. *Child Abuse & Neglect*, *33*(12), 849-856.

Buljan Flander, G., Dugić, S. i Handabaka, I. (2015). Odnos elektroničkog nasilja, samopoštovanja i roditeljskih čimbenika kod adolescenata. *Klinička psihologija, 8*(2), 167-186.

Campbell, K., Goodie, A. S. i Foster, J. D. (2004). Narcissism, confidence, and risk attitude. *Journal of Behavioral Decision Marketing, 17*(4), 297-311.

Carević, N., Mihalić, M. i Sklepić, M. (2013). Ovisnost o internetu među srednjoškolcima. *Socijalna politika i socijalni rad, 2*(1), 64-81.

Catalano, R., Kosterman, R., Hawkins, J. D., Newcomb, M. i Abbott, R. (1996). Modeling the etiology of adolescent substance use: A test of the social development model. *Journal of Drug Issue, 26*(2), 429-455.

Chibnall, S., Wallace, M., Leicht, C. i Lunghofer, L. (2006). *I-safe evaluation. Final report.* Faiffax: Caliber Assotiation.

Cho, S. H. (2007). Effects of motivations and gender on adolescents' self-disclosure in online hatting. *CyberPsychology & Behavior, 10*(3), 339-345.

Chou, H.T i Edge, N. (2012). They are happier and having better lives than I am: the impact of using Facebook on pereception of others lives. *Cyberpsychology, Behaviour and Social Networking, 15*(2), 117-121.

Crofts, T., Lee, M., Mc Govern, A. i Milivojevic, S. (2014). Sexting and young people. *Legaldate, 26*(4), 2-4.

Despotovic, Z. O., Hossfeld T. O., Kellerer, W. O., Lehrieder, F. R., Oechsner, S. I. i Michel, M. A. (2011). Mitigating Unfairness In Locality-Aware Peer-To-Peer Networks. *International Journal Of Network Management*, *21* (1), 3-20.

Deters, F. i Mehl, M.R. (2012). Does Posting Facebook Status Updates Increase or Decrease Loneliness? An Online Social Networking Experiment. *Social Psychological and Personality Science, 5*(4), 579-586.

Döring, N. (2014). Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting? *Cyberpsychology Journal of Psychosocial Research in cyberspace, 8*(1), article 9. doi: 10.5817/CP2014-1-9.

Dufrasnes, C. (2017). *Online Risk Behavior and Depression in Adolescence*. Faculty of Social Sciences, Utrecht University.

Đuraković, M. i Klasnić, I. (2016). Povezanost školskog uspjeha i rizičnih ponašanja srednjoškolaca na internetu. *Napredak, 157*(3), 263–281.

Eastin, M.S., Greenberg, B.S. i Hofschire, L. (2006). Parenting the Internet. *Journal of Communication, 56*(3), 486–504.

Erceg, M. (2015). *Sadržaji interneta i slobodno vrijeme djece i mladeži osnovnoškolske dobi* (neobjavljeni diplomski rad). Prirodoslovno-matematički fakultet Sveučilišta u Splitu.

Fleming, M. J., Greentree, S., Cocotti-Muller, D., Elias, K. A. i Morrison S. (2006). Safety in Cyberspace: Adolescents' Safety and Exposure Online. *Youth & Society, 38*(2), 135-154.

Gámex-Guadix, M. (2014). Depressive symptoms and problematic Internet use among adolescents: Analysis of the longitudinal relationships from the cognitive-behavioral model. *Cyberpsychology, Behavior, and Social Networking, 17*(1), 714-719.

George, M. J. i Odgers, C. L. (2015). Seven fears and the science of how mobile technologies may be influencing adolescents in the digital age. *Perspectives on Psychological Science, 10*(6), 832-851.

Hamburger, Y. i Ben-Artzi, E. (2000). The relationship between extraversion and neuroticism and the different uses of the Internet. *Computers in Human Behavior, 16*(4), 441–449.

Hamer, A., Konijn, E. A. i Keijer, M. G. (2014). Cyberbullying Behavior and Adolescents' Use of Media with Antisocial Content: A Cyclic Process Model. *Cyberpsychology, Behavior, and Social Networking, 17*(2), 74-81.

Hinić, D. (2008). Simptomi i dijagnostička klasifikacija internet zavisnosti u Srbiji. *Primenjena psihologija, 2*(1), 43-59.

Hudson, H. K. (2011). *Factors affecting sexting behaviors among selected undergraduate students. A dissertation submitted in partial fulfillment of the requirements for the doctor philosophy in Education degree with a concentration in Health education.* Southern Illinois University Carbondale: Department of Health Education and Recreation in the Graduate School.

Huesmann, L. R. i Eron, L. D. (1986). *Television and the aggressive child: A cross-national comparison.* Hillsdale, NJ: Lawrence Erlbaum.

Jackson, L., Biocca, F., von Eye, A., Barbatsis, G., Zhao, Y. i Fitzgerald, H. (2004). Children's internet use: Findings from the HomeNetToo Project. U: L. Cantoni i C. McLoughlin (Ur.), *Proceedings of EdMedia: World conference on educational media and technology 2004* (str. 4763-4769). Lugano, Switzerland: Association for the Advancement of Computing in Education (AACE).

Kalmus, V., Realo, A. i Siibak, A. (2011). Motives for internet use and their relationships with personality traits and socio-demographic factors. *Trames: Journal* of *the Humanities and Social Sciences, 15*(4), 385–403.

Karl, K., Peluchette, J. i Schlaegel, C. (2010). Who's posting Facebook faux-pas? A cross-cultural examination of personality differences. *International Journal of Selection and Assessment, 18*(2), 174-186.

Kerr, M., Stattin, H. i Burk, W. J. (2010). A reinterpretation of parental monitoring in longitudinal perspective. *Journal of Research on Adolescence*, *20*(1), 39-64.

Kričkić, D., Šincek, D. i Babić Čikeš, A. (2017). Sexting, cyber-violence and sexually risk behaviour among college students. *Kriminologija & socijalna integracija, 25*(2), 15-28. https://doi.org/10.31299/ksi.25.2.2

Kušić, S. (2010). Online društvene mreže i društveno umrežavanje kod učenika osnovne škole: navike Facebook generacije. *Život i škola*, *24*(2), 103 – 125.

Kuterovac Jagodić, G., Štulhofer, A. i Lebedina Manzoni, M. (2016). *Preporuke za zaštitu djece i sigurno korištenje elektroničkih medija.* Zagreb: Agencija za elektroničke medije.

Kuterovac Jagodić, G. i Keresteš, G. (1997). Perception of parental acceptance-rejection and some personality variables in young adults. *Društvena istraživanja, 30-31*(4-5), 477-491.

Lagator, I. (2017). *Odnos roditeljskog nadzora i ponašanja na internetu* (neobjavljeni diplomski rad). Filozofski fakultet, Osijek.

Lagator, I., Šincek, D. i Duvnjak, I. (2018). Roditeljski nadzor i ponašanje djevojčica i dječaka na internetu. *Život i škola, 64*(1), 89-103. https://doi.org/10.32903/zs.64.1.7

Lenhart, A. (2009). *Teens and sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging.* Pew Internet & American life project.

Liau, A. K., Khoo, A. i Ang, P. H. (2005). Factors influencing adolescents engagement in risky Internet behavior. *Cyberpsychology & Behavior*, *8*(6), 513–520.

Livazović, G. (2009). Teorijsko-metodološke značajke utjecaja medija na adolescente. *Život i škola, 57*(21), 108-115.

Livazović, G. (2011). *Utjecaj medija na poremećaje u ponašanju adolescenata* (doktorska disertacija). Zagreb: Filozofski fakultet Sveučilišta u Zagrebu.

Livazović, G. (2012). Povezanost medija i rizičnih ponašanja adolescenata. *Kriminologija i Socijalna Integracija, 20*(1), 1-22.

Livingstone, S. (1998). Relationships between media and audiences: Prospects for future audience reception studies. U: T. Liebes i J. Curran (Ur.), *Media, ritual and identity: Essays in honor of Elihu Katz* (str. 237–255). London, England: Routledge.

Livingstone, S. i Bober, M. (2006). Regulating the internet at home: Contrasting the perspectives of children and parents. U: D. Buckingham i R. Willett (Ur.), *Digital Generations* (str. 93-113). Mahwah, NJ: Erlbaum.

Livingstone, S. i Helsper, E. J. (2008). Parental mediation of children's internet use. *Journal of Broadcasting & Electronic Media*, *52*(4), 581-599.

Livingstone, S. i Millwood Hargrave, A. (2006). *Harm and Offence in Media Content: A review of the evidence,* Intellect Books, ISBS, Portland, Oregon.

Livingstone, S., Haddon, L., Görzig, A., i Ólafsson, K. (2011). *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries. EU Kids Online, Deliverable D4*. EU Kids Online Network, London, UK.

Lou, S. J., Ru-Chu. S., Hung-Tzu, L., Yuan-Chang, G. i Kuo-Hung, T. (2010). The Influences of the Sixth Graders' Parents' Internet Literacy and Parenting Style on Internet Parenting. *Turkish Online Journal of Educational Technology - TOJET*, *9*(4), 173-184.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. i Pattinson, M. (2016). Individual differences and Information Security Awareness. *Computer in Human Behavior*, *69*(3), 151–156.

McDonald, D. G. (2009). Media use and the social environment. U: R. L. Nabi i M. B. Oliver (Ur.), *Media processes and effects* (str. 251-268). Los Angeles, CA: Sage.

Mead, G. H. (2003). *Um, osoba i društvo sa stajališta socijalnog biheviorista*. Zagreb: Jesenski i Turk, Hrvatsko sociološko društvo.

Nathanson, A. I. (2001). Parent and child perspectives on the presence and meaning of parental television mediation. *Journal of Broadcasting & Electronic Media*, *45*(2), 201—220.

Nguyen Steers, M., Wickham, R. E. i Acitelli, L. K. (2014). Seeing Everyone Else's Highlight Reels: How Facebook Usage Is Linked to Depressive Symptoms. *Journal of Social and Clinical Psychology, 33*(8), 701-731.

Nikodem, K., Kudek Mirošević, J. i Bunjevac Nikodem, S. (2014). Internet i svakodnevne obaveze djece. *Socijalna ekolologija, 23*(3), 211-235.

Nosko, A., Wood, E. i Molema, S. (2009). All about me: Disclosure in online social networking profiles: The case of Facebook. *Computers in Human Behavior, 26*(3), 406-418.

Papacharissi, Z. i Rubin, A.M. (2000). Predictors of Internet Use. *Journal of Broadcasting & Electronic Media*, *44*(2), 175-196, doi: 10.1207/s15506878jobem4402_2

Patchin, J. W. i Hinduja, S. (2006). Bullies Move Beyond the Schoolyard: A Preliminary Implications for adolescent health. *Journal of Adolescent Health*, *41*(2), 189-195.

Poliklinika za zaštitu djece i mladih grada Zagreba (2013). http://www.poliklinika-djeca.hr/istrazivanja/istrazivanje-o-iskustvima-i-ponasanjima-djece-na-internetu-i-na-drustvenoj-mrezifacebook-2/, pristupljeno 19.11.2018.

Puri, A. i Sharma, R. (2016). Internet usage, depression, social isolation and loneliness amongst adolescents. *Indian Journal of Health & Wellbeing*, 7(10), 996-1003.

Rakić-Bajić, G. i Hedrih, V. (2012). Prekomjerna upotreba interneta, zadovoljstvo životom i osobine ličnosti, *Suvremena psihologija, 15*(1), 119-131.

Reyns, B. W. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses, *Journal of Research in Crime and Delinquency*, *50*(2), 216-238.

Rice, E., Gibbs, J., Winetrobe, H., Rhoades, H., Plant, A., Montoya, J. i Kordic, T. (2014). Sexting and sexual behavor among middle school students. *Pediatrics, 134*(1), 21-28.

Ryan, T. i Xenos, S. (2011). Who uses Facebook? An investigation into the relationship between the Big Five, shyness, narcissism, loneliness, and Facebook usage. *Computers in Human Behavior, 27*(5), 1658-1664.

Schultz, D., Izard, C., Ackerman, B. i Youngstrom, E. (2001). Emotion knowledge in economically disadvantaged children: Self-regulatory antecedents and relations to social difficulties and withdrawal. *Development and Psychopathology*, *13*(1), 53–67.

Shaw, L.H. i Gant, L.M. (2002). In defense of the internet: The relationship between internet communication and depression, loneliness, self-esteem, and perceived social support. *Cyber Psychology & Behavior, 5*(2), 157-171.

Staksrud, E., Ólafsson, K. i Livingstone, S. (2013). Does the use of social networking sites increase children's risk of harm?. *Computers in Human Behavior, 29*(1), 40-50.

Symantec (2010). *State of spam & phishing – A monthly report*. Preuzeto s http://www.symantec.com/content/en/us/enterprise/other_resources/b-state_of_spam_and_phishing_report_12-2010.en-us.pdf.

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behaviour, 26*(3), 277-287.

Tomkins, S. (1987). *Script Theory. The Emergence of Personality*. New York: Springer Publishing Company.

Valcke, M., Bonte, S., De Wever, B. i Rots, I. (2010). Internet parenting styles and the impact on Internet use of primary school children. *Computers & Education*, *55*(2), 454-464.

Valkenburg, P. M. i Peter, J. (2011). Online Comunication Among Adolescents: An Integrated Model of its Attraction, Opportunities and Risks. *Journal of Adolescents Health*, *48* (2), 121-127.

Valkenburg, P. M., Schouten, A. P. i Peter, J. (2005). Adolescents' identity experiments on the Internet. *New Media & Society, 7* (3), 383-402.

Valkenburg, P. M. i Cantor, J. (2000). Children's likes and dislikes in entertainment programs. U: D. Zillmann i P. Vorderer (Ur.), *Media entertainment: The psychology of its appeal* (str. 135-152). Mahwah, NJ: Erlbaum.

Valkenburg, P. M. i Peter, J. (2007). Online communication and adolescents' well-being: Testing the Stimulation versus the displacement hypothesis. *Journal of Computer-Mediated Communication, 12*(4), 1169-1182.

Valkenburg, P. M. i Peter, J. (2013). The differential susceptibility to media effects model. *Journal of Communication*, *63*(2), 221-243.

Vejmelka, L., Strabić, N. i Jazvo, M. (2017). Online aktivnosti i rizična ponašanja adolescenata u virtualnom okruženju. *Društvena istraživanja, 26*(1), 59-78.

Velki, T. (2012). Uloga nekih obiteljskih čimbenika u pojavi nasilja među djecom. *Psihologijske teme*, *21*(1), 29-60.

Velki, T. i Duvnjak, I. (2017). Efekti socijalnog konteksta na povezanost uporabe medija s nekim aspektima razvoja djece. *Psihologijske teme, 26*(3), 481 – 508.

Velki, T., Šolić, K. i Nenandić, K. (2015). Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK). *Psihologijske teme, 24*(3), 401-424.

Velki, T., Šolic, K., Gorjanac, V. i Nenadic, K. (2017). Empirical study on the risky behavior and security awareness among secondary school- validation and preliminary results. *Hrvatska udruga za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku – MIPRO proceedings,* 1280-1284.

Velki, T. i Romstein, K. (2018). Nacionalno istraživanje rizičnog ponašanja i znanja računalnih korisnika, U: Šolić, K. i Velki, T. (Ur.), *Priručnik za informacijsku sigurnost i zaštitu privatnosti* (str. 37-68), Fakultet za odgojne i obrazovne znanosti Sveučilište Josipa Jurja Strossmayera u Osijeku.

Vuletić, S., Jeličić, A. i Karačić, S. (2014). Bioetičke konotacije interneta. *Diacovensia, 22*(4), 525-558.

Welk, A.K., Hong, K.W., Zielinska, O.A., Tembe, R., Murphy-Hill, E. i Mayhorn, C.B., (2015). Will the Phisher-Men Reel You In? *International Journal of Cyber Behavior Psychology and Learning*, *5*(4), 1–17.

Wolfradt, U. i Doll, J. (2001). Motives of adolescents to use the Internet as a function of personality traits, personal and social factors. *Journal od Educational Computing Research*, *24*(1) 13–27.

Ybarra, M. i Mitchell, K. (2007). Prevalence & frequency of Internet harassment instigation: Look at Cyberbullying. *Youth Violence and Juvenile Justice, 4*(2), 148-169.

Ybarra, M. L., Alexander, C. i Mitchell, K. J. (2005). Depressive symptomatology, youth Internet use, and online interactions: a national survey. *Journal of Adolescent Health, 36*(1), 9-18.

Ybarra, M. L. i Mitchell, K. J. (2004). Youth engaging in online harassment: associations with caregiver–child relationships, Internet use, and personal characteristics. *Journal of Adolescence*, *27*(3), 319–336.

Young, K. (1998). Internet addiction: The emergence of the new clinical disorder. *Cyber Psychology and Behavior, 1* (3), 237-242.

Zeng, W., Ye, K., Hu, Y. i Ma, Z. W. (2016). Explicit Self-Esteem, Loneliness, and Pathological Internet use among Chinese Adolescents. *Social Behavior & Personality: an International Journal, 44(*6), 965-972.

Zheng, X. i Zhao, W. (2015). Relationship between Internet altruistic behavior and hope of middle-school students: The mediating role of self-efficacy and self-esteem. *Psychological Development and Education*, *31*(4), 428–436.

Zloković, J. i Vrcelj, S. (2010). Rizična ponašanja djece i mladih. *Odgojne znanosti, 12*(1), 197-213.

Ivana Duvnjak, asistentica psihologije
Filozofski fakultet Sveučilišta Josipa Jurja Strossmayera u Osijeku
izv. prof. dr. sc. Daniela Šincek
Filozofski fakultet Sveučilišta Josipa Jurja Strossmayera u Osijeku

5. VRŠNJAČKO NASILJE U DIGITALNOM SVIJETU

Sažetak

U današnje vrijeme internet je postao dio svakodnevnice većine ljudi i broj aktivnih korisnika svakim danom sve je veći. Internet pruža velike mogućnosti, no u ovakvoj globalnoj ekspanziji javljaju se i negativni primjeri poput nasilja na internetu i različitih oblika rizičnih ponašanja. Za nasilje na internetu specifično je to što se za razliku od tradicionalnih oblika nasilja može odvijati neprestano tijekom cijelog dana te ono pruža anonimnost. Uslijed uporabe interneta moguće je javljanje različitih psiholoških i bihevioralnih problema te ono ima značajan utjecaj na psihički i emocionalni razvoj djece i mladih. Neke od mogućih posljedica su: pojava depresije, anksioznosti, sniženog samopouzdanja, slabijeg obrazovnog uspjeha kod žrtvi te nedostatak empatije kod onih koji čine nasilje na internetu.

5.1. UVOD

Pojava interneta krajem 20. stoljeća donijela je globalnu promjenu u načinu i brzini komunikacije među ljudima. Prvotna namjena bila je olakšavanje razmjene informacija u svrhu dobrobiti svih ljudi. Tehnologija je do sada napredovala u tolikoj mjeri da se odražava i u pojavi nasilja na internetu. Vremena su se promijenila, no djeca i mladi drže korak s promjenama puno lakše nego odrasli. Premda se tradicionalno vršnjačko nasilje još uvijek redovito javlja, današnja djeca i mladi doživljavaju i nasilje tehnološkim napretkom, na pametnim telefonima i na internetu. Način upotrebe interneta određuje i moguće posljedice, pa je tako prednost da internetom možemo širiti spoznaje i upotpunjavati znanje, dopisivati se s drugima, doznati novosti i slično (Robotić, 2015). S druge strane, nemaju svi korisnici interneta dobre namjere pa se tako neki koriste internetom kako bi naštetili drugima. Posebno ranjiva skupina su djeca i mladi koji o elektroničkim uređajima znaju u pravilu znatno više od roditelja.

Unatoč većoj medijskoj posvećenosti temi nasilja na internetu, mnogi još uvijek nisu upoznati s tim pojmom. Danas se za takva ponašanja koriste i pojmovi kao što su elektroničko nasilje, nasilje na nternetu, e-nasilje i slično. Ono predstavlja nasilje koje se odvija instant porukama (IM), mrežnim stranicama, digitalnim porukama ili fotografijama koje se šalju pametnim telefonima ili računalima. Unatoč sličnostima s tradicionalnim nasilje, nasilje na nternetu predstavlja pojavu koja je izazvala zanimanje javnosti i medija a također i znanstvenika. Osim što je nasilje na internetu različito od tradicionalnog nasilja, ono dovodi do jedinstvenih izazova u suočavanju s njegovom pojavom, posebno za roditelje, obrazovne djelatnike i sve odrasle koji su u interakciji s djecom.

U Republici Hrvatskoj prema podacima Državnog zavoda za statistiku upotreba je računala i interneta u porastu u svim dobnim skupinama (Zoroja Milić i Markuš, 2018), a najviše među mladima u dobi između 16 i 24 godine. Otprilike 90 % adolescenata redovito se koristi društvenim mrežama, dok 70 % ima korisnički profil na najmanje jednoj društvenoj mreži (Subrahmanyam, Garcia, Harsono, Li i Lipana, 2009). Društvene mreže sve su više prepoznate kao često sredstvo iskazivanja i doživljavanja nasilnog ponašanja. U digitalnom svijetu, posebice na društvenim mrežama, često se iskazuju i doživljavaju nasilna ponašanja poput slanja uvredljivih ili prijetećih poruka, širenja tračeva, otkrivanja tuđih osobnih informacija, objavljivanja neprikladnih fotografija ili isključivanja drugih za vrijeme komunikacije interentom (Upton Patton i sur., 2014).

5.2. NASILJE NA INTERNETU

Pri definiranju pojma nasilja na internetu javljaju se određena pitanja glede pojmovnog određenja, odnosno koji se elementi trebaju pojavljivati da bi se govorilo o nasilju na internetu. Nasilje na internetu definira se kao namjeran pokušaj nanošenja štete vršnjaku ili vršnjacima kroz manipulaciju ili narušavanje odnosa s drugima uporabom interneta ili mobitela (Cetin, Yaman i Peker, 2011). Različitim medijima svakodnevno nasilje širi se i na digitalni svijet stvarajući nasilje na internetu (Strabić i Tokić Milaković, 2016). Patchin i Hinduja (2006, p.152) definiraju nasilje na nternetu kao „namjerno i ponavljano nanošenje štete uzrokovano elektroničkim tekstom". Tokunaga (2010) definira nasilje na internetu kao „bilo koje ponašanje koje osoba ili grupa osoba vrši kroz elektroničke medije, a kojim opetovano komuniciraju neprijateljske ili agresivne poruke čija je svrha nanošenje štete ili neugode drugima." Nadalje, O'Keeffe i Clacke-Pearson (2011) definiraju nasilje na internetu kao namjernu upotrebu digitalnih medija za komunikaciju lažnih, sramotnih ili hostilnih informacija o drugoj osobi. Definicija proizišla iz kvalitativnog istraživanja (Vandebosch i Van Cleemput, 2008) načina na koji djeca i mladi u dobi od 10 do 18 godina definiranju nasilje na internetu pomoću modernih tehnoloških uređaja uključuje sljedeće aspekte: a) namjeru da se nekoga povrijedi, b) dio je ponavljajućeg uzorka negativnih radnji i c) dovodi se u vezu koju karakterizira neravnoteža snage.

Stručnjaci u tom području opisuju tri glavne motivacije za nasilje na internetu do kojih su došli istraživanjem na studentima (Rafferty i Vander Ven, 2014). Prva motivacija je sankcioniranje prema kojoj pojedinci na društvenim mrežama sankcioniraju nepoželjna ponašanja prijatelja ili poznanika, najčešće javnim vrijeđanjem (na primjer, javnim objavana na društvenim mrežama). Stoga se takva motivacija smatra metodom indirektne socijalne kontrole. Sram je ovdje ključna komponenta budući da je sankcioniranje javno, a svrha je posramiti osobu zbog nekog ponašanja. Kada se dogodi posramljivanje u pravilu izostaju intervencije što može dovesti do stvaranja normi prema kojima je prihvatljivo i dopušteno ponižavati i uznemiravati druge (Larkin, 2013). Druga motivacija je borba moći koja se odnosi na pokušaje povrjeđivanja i ponižavanja drugih ili utjecanja na njihovo ponašanje kako bi dobili pristup vrijednim resursima. Kod borbe moći najčešće se ističu romantične veze, a čest je slučaj nasilja nad bivšim partnerima ili njihovim novim partnerima. Posljednja motivacija je zabava („trolanje") kojoj je svrha isprovocirati žrtvu te dobiti emocionalnu reakciju koja služi osobnoj zabavi. Ključna je komponenta anonimnost i često podrazumijeva otvaranje lažnih profila. Karakteristično je za te osobe da, nakon što ih je netko pokušao zaustaviti, one nastavljaju ili intenziviraju svoje provokacije.

5.2.1. OBLICI NASILJA NA INTERNETU

Nasilje na internetu može poput tradicionalnog nasilja poprimiti direktni i indirektni oblik. Direktan oblik nasilja na internetu je onaj u kojem se poruke šalju direktno drugoj djeci ili mladima. Nasilje na internetu pomoću posrednika odnosi se na ponašanje u kojem drugi vrše nasilje nad žrtvom, odnosno pronalaska nekoga tko čini nasilje umjesto nasilnika (Kowalski, Limber i Agatston, 2008). Često ti posrednici nisu svjesni i ne znaju da ih se koristi za činjenje takvog oblika nasilja na internetu.

Potrebno je razlikovati načine preko kojih se odvija (različitih sustava za dopisivanje, društvenih mreža itd.) i vrstu ponašanja koja se prenosi na određene načine, a dovode do nasilja na internetu. Nancy Willard (2006) opisala je sedam ponašanja koja predstavljaju nasilje na internetu.

- *Izazivanje sukoba (flaming, „potpaljivanje")* odnosi se na kratku i „usijanu" raspravu koja se odvija između dviju ili više osoba uporabom bilo koje komunikacijske tehnologije. Obično se odvija javno pred drugima, u raspravama ili različitim grupama, a započinje razmjenom niza uvreda. Isprva se može činiti kako se takvo potpaljivanje odvija između dviju osoba koje se podjednako vrijeđaju, no neočekivani agresivni postupci jednog pojedinca mogu stvoriti neravnotežu u grupnoj raspravi koja postaje sve veća. Flaming uključuje namjerno započinjanje rasprave pomoću objavljivanja uvredljivih i provokativnih poruka, poput upotrebe neprijateljskog izražavanja, psovki, pogrdnih imena, prijetnji i seksualno neprimjerenih komentara (Lapidot-Lefler i Barak, 2012). Stoga se i opisuje kao hostilna i vulgarna komunikacija o najčešće kontroverznim temama (politika, religija).
- *Uznemiravanje* predstavlja jedinstveni oblik nasilja na internetu koji podrazumijeva ponavljajuće uvredljive poruke poslane nekoj osobi. Najčešće se događa u privatnoj komunikaciji između dviju osoba, ali se takve uznemirujuće poruke mogu pojaviti i u javnim raspravama i grupama. Jedan oblik uznemiravanja koji se odnosi na stvaranje tzv. tekstualnih ratova uključuje jednog ili više počinitelja nasilja i jednu žrtvu. Nasilnik ili nasilnici u tom slučaju šalju stotine ili tisuće tekstualnih poruka putem interneta (Kowalski i sur., 2008). Uznemiravanje se razlikuje od izazivanja sukoba po tome što uznemiravanje traje duže i jednsotranije je, odnosno sudjeluju najmanje jedan nasilnik i jedna žrtva. S druge strane, kod izazivanja sukoba postoji međusobna razmjena uvreda između uključenih sudionika. Uznemiravanje se također pojavljuje i među grupama nasilnika poznatih pod nazivom „griefers". To su oni pojedinci koji namjerno uznemiravaju druge igrače u višeigračkim igricama na internetu. Njih ne zanima pobjeda u igrici, nego pokušavaju uništiti iskustvo igranja drugim igračima,

na primjer ubijanjem suigrača ili ometanjem ciljeva cijelog tima (Adrian, 2010).

- *Klevetanje* se odnosi na slanje ili objavljivanje informacije o drugoj osobi koje su pogrdne i neistinite s namjerom ugrožavanja njezine reputacije ili prijateljstva. Informacije se mogu objaviti na internetskim stranicama ili se mogu proslijediti drugima preko e-pošte ili izravne razmjene poruka. U tu kategoriju pripada objavljivanje ili slanje digitalno izmijenjenih fotografija neke osobe, posebice na seksualiziran ili štetan način. Jedan od oblika takvog nasilja su „elektronske knjige" (engl. *slam books*) kojima je cilj ponižavanje i ismijavanje drugih, najčešće vršnjaka. Učenici izrade mrežnu stranicu na kojoj se mogu pisati nepristojni i zlonamjerni komentari. Slično tomu su i glasanja ili izbori na internetu pri čemu se vršnjaci mogu izjasniti u vezi sa specifičnim pitanjem (npr. tko je najružniji u razredu ili školi?). Na takav se način formiraju liste s mnoštvom uvredljivih i zlobnih komentara.
- *Lažno predstavljanje* događa se kada se osoba koja čini nasilje predstavlja kao žrtva koristeći njezinu lozinku kako bi pristupila njezinim računima i profilima na internetu te tada komunicirala s drugima na neprikladan način praveći se da izražava mišljenje osobe čiji je profil preuzela. Takva osoba može također mijenjati profil osobe i objavljivati ponižavajuće ili provokativne informacije. Nadalje, može slati uznemirujuće poruke drugima pretvarajući se da je osoba čiji profil koristi i pisati javno u ime te osobe u grupama te objavljivati osobne informacije žrtve (adresu, broj telefona). Sva ta ponašanja mogu narušiti ugled i prijateljstva žrtve.
- *Nedozvoljeno objavljivanje i obmanjivanje* odnosi se na javno objavljivanje ili prosljeđivanje tuđih privatnih i često sramotnih fotografija onim osobama kojima te informacije nisu bile namijenjene. Najčešće je riječ o distribuciji fotografija koje su ponižavajuće ili seksualne prirode te razgovorima koji sadrže povjerljive informacije. Takve prijevare odnose se na zavaravanje drugih kako bi im otkrili osobne informacije o sebi i kako bi ih onda dalje dijelili s drugima. Osoba koja čine takvo nasilje koristi trikove i obmane kako bi saznala privatne informacije o drugima. Može se odvijati i na način da se na mobitelu drugima pokazuju tuđe poruke ili fotografije.
- *Isključivanje na internetu* odnosi se na indirektan način nasilja kojim se namjerno isključuje neku osobu iz grupe na internetu ili zajednice. Kod žrtava dolazi do pada samopoštovanja. Osobe koje su žrtve takvog nasilja spremnije se uključuju u druge grupe, potpuno nove i drugačije od one koja ih je isključila. To čine kako bi ponovno osjetile povezanost s drugima. Uključivanje u druge

grupe može pomoći ublažiti negativne posljedice isključivanja, a ponekad može doprinijeti tomu da se žrtva osnaži za osvetu grupi koja ju je isključila.

- *Uhođenje na internetu* odnosi se na upotrebu elektroničke komunikacije za uhođenje druge osobe ponavljajućom, uznemirujućom i prijetećom komunikacijom. Uključuje potajno slijeđenje i praćenje u svrhu uznemiravanja te više prijetnji nego čisto uznemiravanje. Kod žrtava se javlja uvjerenje kako će uhođenje na internetu postati i fizičko te se javlja strah za vlastitu sigurnost budući da se prijetnje odnose na povrjeđivanje, zastrašivanje i neugodne komentare.
- *Snimanje i objavljivanje napada* (engl. *happy slapping*) predstavlja jedan od oblika nasilja na internetu koji se pojavio u Engleskoj u vlakovima podzemne željeznice. Takvo ponašanje najčešće čine adolescenti pri čemu priđu nepoznatoj osobi i ošamare ju, dok drugi vršnjak snima događaj nasilja koji se potom javno objavi na internetu. Mladi navode kako se radi o šali i načinu zabave. Međutim, često uključuje više od "šamara" i često predstavlja izravni tjelesni napad (tzv. "hoppin"). Žrtve mogu biti poznate ili nepoznate osobe počiniteljima takvog nasilja.

5.3. TRADICIONALNO NASILJE I NASILJE NA INTERNETU

Govoreći općenito, nasilje predstavlja agresivno namjero ponašanje koje uključuje neravnotežu moći i snage (Olweus, 1993). Ponekad se ta neravnoteža odnosi na fizičku snagu između djece, a često je obilježena razlikama u socijalnoj moći ili statusu. Zbog takve neravnoteže djetetu koje je žrtva nasilja teško se obraniti. Vršnjačko nasilje ne javlja se samo jednom ili dvaput, nego se opetovano ponavlja tijekom vremena. Ponekad je odraslima vrlo teško znati ponavlja li se takvo ponašanje budući da djeca često uspješno skrivaju nasilje i nevoljko prijavljuju nasilje koje doživljavaju ili kojem svjedoče. Međutim, važno je utvrditi je li se nasilno ponašanje dogodilo jednom ili je dio obrasca ponašanja koje se ponavlja. Oblici tradicionalnog vršnjačkog nasilja uključuju direktna ponašanja poput udaranja, ruganja, zlonamjernog zadirkivanja ili nazivanja pogrdnim imenima, ali i indirektna ponašanja koja su često manje očita, poput širenja glasina, socijalne izolacije, izbjegavanja ili manipulacije prijateljstvima (npr. ucjene da se neće družiti s nekim ukoliko se ono druži sa žrtvom). Najčešći oblici vršnjačkog nasilja uključuju nazivanje ružnim i pogrdnim imenima, zlobno zadirkivanje ili verbalno izrugivanje o nečijem izgledu ili načinu govora (Nansel i sur., 2001).

Samo definiranje nasilja na internetu složeno je iz više razloga. Jedan je od razloga taj što se nasilje na internetu može smatrati posebnim fenomenom ili podvrstom

nasilnog ponašanja u digitalnom svijetu ili nastavkom tradicionalnog nasilja (Strabić i Tokić Milaković, 2016). Ukoliko je nasilje na internetu podvrsta nasilnog ponašanja, trebao bi se javljati zajedno s tradicionalnim nasiljem. Rezultati istraživanja (Li, 2007) pokazali su kako oni koji čine nasilje na internetu čine i nasilje u tradicionalnom smislu te oko 30 % adolescenata koji su uključeni u tradicionalno nasilje čine nasilje i u digitalnom okruženju.

Ono što je zajedničko tradicionalnom nasilju i internetskom nasilju je to da uključuju namjeru da se povrijedi drugu osobu, ponavljanje agresivnog ponašanja te neravnotežu moći između nasilnika i žrtve (Kowalski i sur., 2008). Unatoč konceptualnom preklapanju između tradicionalnog nasilja i nasilja na internetu, nasilje na internetu razlikuje se od tradicionalnog nasilja na način da ponižavajući materijali, kao što su poruke, slike i ostali sadržaji, mogu biti trajni i dostupni svima. Tradicionalno nasilje karakterizira fizička dominantnost nasilnika, dok kod internetskog nasilja fizička dominantnost nije nužna. Međutim, nasilnici mogu biti dominantni nad žrtvom znanjem o upotrebi interneta, anonimnošću i žrtvinoj ograničenoj mogućnosti obrane i bijega (Perren i sur., 2012). Stoga, internestko nasilje donosi neke nove socijalne i psihološke implikacije.

Internetsko nasilje u odnosu na tradicionalno nasilje omogućuje veći stupanj invazivnosti, veću publiku, anonimnost nasilnika te veći raspon varijabiliteta nasilja u digitalnom svijetu. Udaljenost između žrtve i nasilnika veća je kod internetskog nasilja, što zajedno s anonimnošću onoga koji čini nasilje olakšava pojavu nasilja, povećava stupanj izloženosti nasilju i intenzitet povrede. Smith i suradnici (2008) na temelju istraživanja na djeci i mladima u dobi od 11 do 16 godina utvrdili su kako je nasilje internetsko nasilje manje učestalo od tradicionalnog nasilja, da prevladava nasilje tekstualnim porukama i pozivima, da i nasilje na mobitelu ima značajan negativni učinak iako se rjeđe javlja, da nasilje najčešće čini jedan do tri učenika koji su većinom iz iste grupe te da žrtve tradicionalnog nasilja često postaju oni koji čine nasilje na internetu.

Za razliku od tradicionalnog nasilja, internetsko nasilje može se događati u bilo koje vrijeme, na bilo kojoj ili s bilo koje lokacije i može biti u potpunosti anonimno. Ono se može događati bilo kada u danu i tijekom svakog dana, a od takvih se nasilnih ponašanja teško sakriti (Steffgen, Kőnig, Pfetsch i Melzer, 2011). Neka istraživanja potvrđuju kako se tradicionalno nasilje prenosi u digitalni svijet (Espelage, Rao i Craven, 2012). Tako, primjerice, promatrač fizičkog nasilja može snimiti neki nasilan događaj i objaviti ga na internetu te na takav način postati počinitelj nasilja u digitalnom svijetu (Vejmelka i Majdak, 2014). Stoga se može zaključiti kako je vjerojatnije da će oni koji izravno sudjeluju u činjenju i doživljavanju tradicionalnog nasilja biti uključeni i u doživljavanje i činjenje nasilja na internetu.

Digitalno okruženje omogućuje anonimnost i rezultira drugačijim problemima od tradicionalnog nasilja (Kowalski i sur., 2008). Anonimnost omogućava osjećaj sigurnosti za nasilnika i smanjuje osjećaj straha da će biti uhvaćen. Oni koji čine nasilje vjerojatnije su manje emocionalno inhibirani zbog svijesti o anonimnosti, uključujući negativne emocije poput ljutnje (Erdur-Baker, 2010). U usporedbi s tradicionalnim nasiljem, oni koji čine nasilje na internetu manje su svjesni ili uopće nisu svjesni posljedica koje uzrokuju njihova ponašanja. Budući da nemaju povratne informacije, nemaju ni priliku za empatiju prema žrtvi. Počinitelji nasilja na internetu često su okrutniji nego što bi bili izvan digitalnog svijeta te je manje vjerojatno da će doživjeti krivnju, a to ih dodatno potiče da i dalje čine takva ponašanja.

Istraživanja (David-Ferdon i Hertz, 2007) pokazuju kako je tradicionalno nasilje i dalje učestalije nego internetsko nasilje, no s povećanjem zainteresiranosti djece i mladih za društvene mreže nasilje u digitalnom svijetu sve je češći i istaknutiji problem. Čest je slučaj da su pojedinci istodobno i žrtve i nasilnici, a najveću grupu uključenu u nasilje čine svjedoci odnosno opažači (Lenhart i sur., 2011). Pokazalo se kako česta izloženost nasilničkim ponašanjima na društvenim mrežama ima štetan psihološki učinak na žrtve, ali i na nasilnike i opažače. Stoga, mladi koji čine nasilje na internetu skloniji su vjerovati da je nasilje prema vršnjacima normativno ponašanje (Upton Patton i sur., 2014).

5.3.1. PREVALENCIJA I SPOLNE RAZLIKE U DOŽIVLJAVANJU NASILJA NA INTERNETU

Prevalencija nasilja na internetu varira ovisno o načinu na koji je nasilje definirano te ovisno o dobi i kulturi koja je uključena u istraživanje. Prevalencija činjenja i doživljavanja nasilja na internetu uglavnom se kreće u rasponu od 20 % do 40 % (Tokunga, 2010). Slični rezultati dobiveni su i na hrvatskim srednjoškolcima (Šincek, 2014) pa je tako na jednom uzorku prevalencija činjenja nasilja na internetu 27,7 %, dok je prevalencija doživljavanja 24,9 %, a na drugom uzorku srednjoškolaca prevalencija činjenja iznosi 17,7 % i doživljavanja 16,5 %. Prevalencija doživljavanja nasilja na društvenim mrežama u proteklih godinu dana u istraživanju Whittaker i Kowalski (2015) iznosi 18,2 % te gotovo 12 % onih koji su činili nasilje na internetu. U slučajevima kada su bili žrtve, nasilnik je u većini slučajeva bio prijatelj (50 %), drugi učenik iz škole (54,3 %) te stranac (30,6 %). Neka istraživanja navode kako je 80 % adolescenata uključeno u nasilje na internetu (Lianos i McGrath, 2018).

Istraživanja pokazuju kako se djeca i mladi koriste internetom za različite aktivnosti, pa se tako dječaci koriste internetom zbog igranja igrica i gledanja videa, a djevojčice zbog dopisivanja i komuniciranja s drugima (Snell i Englander, 2010). S

obzirom na različite motive upotrebe interneta, potrebno je razmotriti spolne razlike u nasilju na internetu. Istraživanje koje je proveo Deniz (2015) u Turskoj na uzorku od 760 djece u dobi od 11 do 15 godina pokazalo je kako dječaci češće sudjeluju u činjenju internetskog nasilja te su mu više i izloženi u usporedbi s djevojčicama. Suprotno tim nalazima su rezultati dobiveni u istraživanju koje su proveli Kowalski i Limber (2007) u SAD-u na uzorku od 3 767 djece u dobi od 11 do 14 godine koje je pokazalo kako su djevojčice sklonije činiti nasilje na internetu. Unatoč suprotnim nalazima pokazuje se kako su dob i spol značajni prediktori doživljavanja nasilja na internetu (Lianos i McGrath, 2018) te kako su djevojčice češće žrtve nasilja (Hinduja i Patchin, 2008). Također se razlikuju i oblici internetskog nasilja s obzirom na spol nasilnik pa tako djevojčice češće šire glasine i ogovaraju, a dječaci češće objavljuju sramotne fotografije i videozapise (Tarablus, Heiman i Olenik-Shemesh, 2015).

Istraživanja tradicionalnog nasilja pokazuju kako opažači reagiraju različito s obzirom na spol (Obermann, 2011), a istraživanja internetskog nasilja daju nekonzistentne rezultate. Tako u nekima nije utvrđen utjecaj spola na suportivno ponašanje prema žrtvi (Macháčková, Dedkova, Sevickova i Cerna, 2013), dok je u drugima utvrđeno kako su djevojčice sklonije pomoći žrtvi, dok su dječaci skloniji pridružiti se nasilju (Van Cleemput, Vandebosch i Pabian, 2014). U istraživanju nasilja na društvenim mrežama utvrđeno je kako su djevojčice imale više bihevioralne namjere da utješe žrtvu i daju joj savjete, dok su dječaci imali više bihevioralne namjere da podrže nasilnika (Bastiaensens i sur., 2014).

5.3.2. POSLJEDICE NASILJA NA INTERNETU

Doživljavanje nasilja na internetu može imati brojne posljedice i utjecaj na psihički i emocionalni razvoj djece i mladih. Kowalski i Limber (2013) proveli su istraživanje u kojem se pokazalo kako najčešće negativne posljedice internetskog nasilja uključuju depresiju, anksioznost, nisko samopoštovanje, probleme sa zdravljem (Feinberg i Robey, 2009), izostajanje iz škole, lošiji školski uspjeh i socijalnu anksioznost (Ortega i sur, 2012) pri čemu se pokazalo kako su ti učinci posebice izraženi kod mladića koji su žrtve nasilja. Pronađeno je kako i nasilnici izvješćuju o višim razinama emocionalnog stresa, suicidalnih misli te agresije u odnosu na vršnjake (Schenk i Fremouw, 2012). S druge strane, Kowalski i Limber (2013) ističu kako su razine anksioznosti i depresije kod mladića nasilnika bile slične razinama kod mladića koji nisu nasilnici. S druge strane, razine anksioznosti i depresije kod djevojaka nasilnica bile su više u odnosu na djevojke koje nisu nasilnice. Što se tiče depresivnosti, postoji recipročna povezanost između depresivnih simptoma i internetskog nasilja (Gámez-Guadix, Orue, Smith i Calvete, 2013). Nadalje, mladi koji su žrtve internetskog nasilja

vjerojatnije će izbjegavati školu i imati slabiji akademski uspjeh, a češće će konzumirati drogu i alkohol (Benzmiller, 2013). Pokazalo se kako i žrtve i osobe koje čine nasilje na internetu pokazuju veću sklonost suicidu. U istraživanju koje su proveli Price i Dalgleish (2010) 3 % sudionika izvijestilo je o suicidalnim mislima nakon što su doživjeli nasilje na interneta, a 2 % ih se samoozlijedilo nakon doživljenog nasilja.

Navodi se da posljedice internetskog nasilja mogu biti štetnije od tradicionalnog vršnjačkog nasilja zbog prisutnosti javnog objavljivanja uvredljivih komentara i veće publike koja svjedoči nasilju, anonimnosti zlostavljača, trajnosti i snage pisane riječi ili objavljene fotografije, mogućnosti da se žrtvu zlostavlja neprestano tijekom cijelog dana kao i nemogućnost bijega žrtve (Dredge, Gleeson i De la Piedad Garcia, 2014). Neki od znakova koji mogu upućivati na pojavu internetskog nasilja odnose se na izbjegavanje uporabe osobnog računala, mobitela i drugih tehnologija, pojavu stresnih reakcija kada pristigne poruka, povlačenje iz interpersonalnih odnosa, izbjegavanje odlaska u školu, izbjegavanje razgovora o uporabi računala, često izražavanje negativnih emocija, uključujući tugu, ljutnju, frustraciju, smanjenu toleranciju i brigu, pad u akademskom uspjehu te smetnje u spavanju i hranjenju.

Nalazi pokazuju kako internestko nasilje ima negativan učinak na razvoj u adolescenciji u kojem je razvoj identiteta iznimno bitan. Tako su Patchin i Hinduja (2010) u svom istraživanju došli do nalaza kako su žrtve i počinitelji internetskog nasilja postizali niže rezultate na mjeri globalnog samopoštovanja od onih koji nisu uključeni u nasilje. Objašnjenje je takvim nalazima da iskustvo viktimizacije narušava samopoštovanje ili da je vjerojatnije da će osobe nižeg samopoštovanja postati žrtve. Također se i u drugim istraživanima pokazalo kako nasilnici imaju nisko samopoštovanje (Kowalski i Limber, 2013). Budući da je samopoštovanje prediktor raznih problema u adolescenciji koji mogu na izravan ili neizravan način utjecati na školsko funkcioniranje, pokazalo se kako postoji slaba do umjerena povezanost između samopoštovanja i akademskog uspjeha, izostajanja iz škole i lošeg zdravlja i kriminalnih ponašanja (Patchin i Hinduja, 2010). Osim žrtvi i počinitelja nasilja potrebno je uzeti u obzir i one koji istodobno doživljavaju, ali i čine nasilje na internetu budući da se pokazalo kako upravo ta skupina djece i mladih pokazuje najviše razine depresije, stresa i anksioznosti te smanjeno samopoštovanje (Šincek, Duvnjak i Milić, 2017). Nadalje, oni koji i doživljavaju i čine nasilje na internetu skupina je koja je najviše izložena riziku od nastanka psihosocijalnih problema. Navedeno potvrđuju i rezultati drugih istraživanja (Ybarra i Mitchell, 2004) prema kojima oni koji pripadaju skupini koja je istodobno i žrtva i nasilnik na internetu imaju najviše depresivnih simptoma, anksioznost te percipirane razine stresa u odnosu na druge grupe, žrtve, nasilnike i neuključene u internetsko nasilje, a također i da imaju najveći rizik za razvoj depresivnih

simptoma u usporedbi s ostalima (Ybarra i Mitchell, 2004; Gámez-Guadix i sur., 2013).

5.3.3. PERCEPCIJA INTERNETA - DJECA I RODITELJI

Roditeljima nije lako pratiti i nadgledati ponašanje djece na internetu s obzirom na veliku mobilnost, ali i nedostatak tehnološkog znanja (Palfrey i Gasser, 2008). Stoga oni koriste različite strategije nadgledanja i kontroliranja ponašanja djece na internetu, poput aktivnog i restriktivnog posredovanja te zajedničke upotrebe interneta (Shin, 2015). Aktivno posredovanje odnosi se na interaktivni razgovor između roditelja i djeteta o prikladnom ponašanju na internetu, potencijalnim rizicima i negativnim posljedicama upotrebe interneta. Restriktivno posredovanje odnosi se na postavljanje pravila s ciljem kontroliranja djetetove upotrebe interneta, a može se odnositi na vremensko ograničenje, ograničenje sadržaja i slično. Zajednička upotreba interneta odnosi se na roditeljsko dijeljenje vlastitih iskustva na internetu sa svojom djecom bez neke specifične svrhe i cilja. Najučinkovitijom strategijom pokazalo se aktivno posredovanje, a njezina učinkovitost proizlazi iz toga da je vjerojatnije da će djeca biti responzivnija na roditeljske zahtjeve te će bolje internalizirati njihova očekivanja kroz razgovore o upotrebi interneta. Dodatna dobit od uporabe navedene strategije je razvijanje vještina kritičkog razmišljanja kod djece.

Što se tiče socijalne podrške, pokazalo se kako žrtve imaju sniženu percepciju podrške odraslih u smislu da roditelji i nastavnici ne interveniraju kako bi spriječili ili zaustavili nasilje ili se žrtve ne obraćaju odraslima za podršku i pomoć (Smokowski, Evans i Cotter, 2014). Takav nedostatak podrške može predstavljati dodatan faktor za žrtve koji može dovesti do socijalnog isključenja (Weber, Ziegele i Schnauber, 2013)

Roditelji su barem u početku internet smatrali korisnim sredstvom koje će pomoći njihovoj djeci pri učenju i domaćim zadaćama. Slično tomu, roditelji na mobitele gledaju kao na sredstvo namijenjeno djeci kako bi se mogla javiti u hitnim slučajevima. Za većinu roditelja pojava tehnologije nešto je novo s čime se susreću te im je strana i stoga prema njihovom mišljenju djeca i mladi trebaju biti oprezni pri uporabi. Mnogi roditelji iskreno priznaju kako su ih djeca naučila većini toga što znaju o internetu i općenito tehnologiji.

S druge strane, djeca i mladi smatrajuiInternet, mobitele i ostalu tehnologiju ključnim sredstvima za socijali život. Takva sredstva komunikacije prisutna su cijeli njihov život i mladi se osjećaju ugodno glede tehnologije što može njihovim roditeljima biti nepoznato. Ono što mladi danas čine nije toliko drugačije od onoga što su činili njihovi roditelji, no način na koji to čine drugačiji je. Mediji koji djeca i mladi danas koriste predstavljaju međutim neke jedinstvene izazove s kojim se nisu susretala

djeca prije nekoliko desetljeća. U tradicionalnom smislu poruke su se prenosile između pojedinaca, često u razredu skrivajući od nastavnika i drugih učenika. U današnje vrijeme šalju se istovremene trenutačne poruke (engl. *instant messaging*) znatno široj publici.

Bilo bolje ili gore, tehnologija je sveprisutna i spaja današnje živote djece i adolescenata. Mladi navode kako im je internet prilika za istraživanje svijeta odraslih bez nadzora (Wing, 2005).

5.4. ZAKLJUČAK

Razvojem novih tehnologija omogućeno je lakše pristupanje internetu i mogućnostima koje se nude. Internet omogućuje lakše načine komuniciranja, brže dolaženje do informacija, lakše održavanje odnosa, no također omogućuje i izražavanje agresivnog, nasilnog i manipulirajućeg ponašanja. Stoga se javlja i internetsko nasilje kojim se opetovano komuniciraju neprijateljske ili agresivne poruke čija je svrha nanošenje štete ili neugode drugima. Usporedbom s tradicionalnim nasiljem, pokazuje se kako su posljedice internetskog nasilja često veće jer žrtva doživljava javno poniženje i sramotu koja se odvija pred brojnom publikom. S razvojem tehnologije razvijaju se i novi načini i oblici nasilja koji prije nisu postojali. Takav trend zahtjeva suradnju stručnjaka i znanstvenika različitih struka kako bi što bolje razumjeli ponašanja i posljedice koje se odnose na pojavu nasilja na internetu, ali i kako bi poticali sigurnu uporabu informacijsko-komunikacijske tehnologije i stvarali što sigurnije okruženje za djecu i mlade.

5.5. PREPORUKE

Stručnjaci i svi oni koji rade s djecom i mladima imaju za cilj osvijestiti prednosti, ali i rizike upotrebe interneta, a također ih i podučiti o različitim oblicima nasilja te posljedicama vlastitog ponašanja. Stoga se daju različite preporuke djeci i mladima pri upotrebi interneta:

- ukoliko netko vrijeđa, govori ružne stvari, naziva pogrdnim imenima i slično, tada čini nasilje na internetu
- nasilje na internetu može se zabilježiti na način da se fotografiraju ili sačuvaju objave i poruke kojima se čini nasilje na internetu
- potrebno je potražiti pomoć ukoliko se takva ponašanja ponavljaju

- koristiti dostupne alate pa tako većina društvenih mreža ima mogućnosti blokiranja drugih (u slučaju uznemiravanja slanjem aplikacija i poruka, komentiranjem objava ili objavljivanjem fotografija)
- zaštiti svoje račune i profile – preporuča se ne otkrivati ni dijeliti svoje lozinke s drugima kao i zaštititi svoj mobitel kako se netko ne bi mogao lažno predstavljati ukoliko mu je dostupan nečiji mobitel
- ukoliko imamo saznanja da netko doživljava nasilje na internet, trebamo pružiti podršku toj osobi. Ukoliko se ne možemo suprotstaviti osobi koja čini nasilje, možemo saslušati osobu koja doživljava nasilje i biti joj podrška te vidjeti na koji joj način možemo pomoći. Zajedno s osobom koja doživljava nasilje prijaviti nasilje koje se događa.

Budući da i roditelji imaju važnu ulogu u pojavi internetskog nasilja i općenito ponašanja djece na internetu, daju se smjernice i roditeljima kako postupati s djecom i mladima:

- ukoliko dijete traži savjet i pomoć roditelja, to predstavlja dobar pokazatelj budući da se većina mladih ne povjerava roditeljima kada je riječ o vršnjačkom nasilju
- podučavati djecu i mlade da ne prosljeđuju, ne dijele i ne doprinose aktivnostima koji se odnose na internetsko nasilje koje čini netko drugi
- djeca i mladi odrastaju na društvenim mrežama na kojima se odvija i socijalizacija i učenje. To se događa svugdje i takve se interakcije događaju i na internetu i izvan njega, kod kuće i u školi te različitim medijima i uređajima. Uklanjanje uređaja ili društvenih mreža neće ukloniti interakciju budući da se ona odvija u vršnjačkim skupinama i socijalnim događajima u školi
- društveni mediji dodatno su mjesto na kojem djeca i mladi stječu prijatelje. Zabranjivanje upotrebe popularnih društvenih mreža djeci i mladima može dovesti do izolacije od strane vršnjaka, bilo da ih vršnjaci namjerno ne uključuju ili zato što nisu prisutni
- kada se zabrani uporaba društvenih mreža i željenih aktivnosti na internetu, nepoželjno se ponašanje samo premješta nekud dalje, kao što su stranice ili aplikacije kojima roditelji nemaju pristup ili im nisu poznate ili izvan interneta.

5.6. LITERATURA

Adrian, A. (2010). Beyond griefing: Virtual crime. *Computer law & Security review*, *26*(6), 640-648.

Bastiaensens, S. Vandebosch, H., Poels, K., Van Cleemput, K., DeSmet, A. i De Bourdeaudhuij, I. (2014). Cyberbullying on social network sites. An experimental study into bystanders' behavioural intentions to help the victim or reinforce the bully. *Computers in Human Behavior, 31*, 259-271.

Benzmiller, H. (2013). Notes & Comments. The cyber-Samaritans: exploring criminal liability for the "innocent" bystanders of cyberbullying. *Northwestern University Law Review*, *107*(*2*), 927-962.

Çetin, B., Yaman, E. i Peker, A. (2011). Cyber victim and bullying scale: A study of validity and reliability. *Computers & Education*, *57*(4), 2261-2271.

David-Ferdon, C. i Hertz, M. F. (2007). Electronic media, violence, and adolescents: An emerging public health problem. *Journal of Adolescent Health*, *41*(6), S1-S5.

Deniz, M. (2015). A study on primary school students' being cyber bullies and victims according to gender, grade, and socioeconomic status. *Croatian Journal of Education: Hrvatski časopis za odgoj i obrazovanje*, *17*(3), 659-680.

Dredge, R., Gleeson, J. F. M. i De la Piedad Garcia, X. (2014). Risk Factors Associated with Impact Severity of Cyberbullying Victimization: A Qualitative Study of Adolescent Online Social Networking. *Cyberpsychology, Behavior, and Social Networking*, *17*(*5*), 287-291.

Erdur-Baker, Ö. (2010). Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of Internet-mediated communication tools. *New Media & Society, 12*(1), 109-125.

Espelage, D. L., Rao, M. A. i Craven, R. G. (2012). Theories of cyberbullying. *Principles of cyberbullying research: Definitions, measures, and methodology*, 49-67.

Feinberg, T. i Robey, N. (2009). Cyberbullying: School leaders cannot ignore cyberbullying but rather must understand its legal and psychological ramifications. *Principal leadership*, *9*, 26-31.

Gámez-Guadix, M., Orue, I., Smith, P. K. i Calvete, E. (2013) Longitudinal and Reciprocal Relations of Cyberbullying With Depression, Substance Use, and Problematic Internet Use Among Adolescents, *Journal of Adolescent Health, 53*(4), 446–452.

Hinduja, S. i Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant behavior*, *29*(2), 129-156.

Kowalski, R. M. i Limber, S. P. (2007). Electronic bullying among middle school students. *Journal of adolescent health*, *41*(6), S22-S30.

Kowalski, R.M. i Limber, S.P. (2013). Psychological, physical and academic correlates of cyberbullying and traditional bullying. *Journal of Adolescent Health, 53*, 13-20.

Kowalski, R.M., Limber, S.P. i Agatston, P.W. (2008). *Cyber bullying: bullying in the digital age*. Blackwell Publishing.

Lapidot-Lefler, N. i Barak, A. (2012). Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. *Computers in Human Behavior*, 28, 434–443.

Larkin, R. W. (2013). Legitimated adolescent violence: Lessons from Columbine. U: *School Shootings* (str. 159-176). Springer, New York, NY.

Lenhart, A., Madden, M., Smith, A., Purcell, K., Zickuhr, K. i Rainie, L. (2011). Teens, Kindness and Cruelty on Social Network Sites: How American Teens Navigate the New World of" Digital Citizenship". *Pew Internet & American Life Project*.

Li, Q. (2007). Bullying in the new playground: Research into cyberbullying and cyber victimization. *Australasian Journal of Educational Technology*, 23(4), 435-454.

Lianos, H. i McGrath, A. (2018). Can the general theory of crime and general strain theory explain cyberbullying perpetration?. *Crime & Delinquency*, *64*(5), 674-700.

Macháčková, H., Dedkova, L., Sevcikova, A. i Cerna, A. (2013). Bystanders' Support of Cyberbullied Schoolmates. *Journal of Community & Applied Social Psychology*, *23*(1), 25–36.

Nansel, T. R., Overpeck, M. D., Pilla, R. S., Ruan, W. J., Simmons-Morton, B. i Scheidt, P. (2001). Bullying behavior among U.S. youth: Prevalence and association with psychosocial adjustment. *Journal of the American Medical Association, 285*, 2094–2100.

Obermann, M.-L. (2011). Moral Disengagement Among Bystanders to School Bullying. *Journal of School Violence*, *10*(3), 239–257.

O'Keeffe, G. S. i Clarke-Pearson, K. (2011). The impact of social media on children, adolescents, and families. *Pediatrics*, *127*(4), 800-804.

Olweus, D. (1993). *Bullying at school: What we know and what we can do*. New York: Blackwell.

Ortega, R., Elipe, P., Mora-Merchan, J. A., Genta, M. L., Brighi, A., Guarini, A., Smith, P. K., Thompson, F. i Tippett, N. (2012). The Emotional Impact of Bullying and Cyberbullying on Victims: A European Cross-National Study. *Aggressive behavior*, *38*(5), 342-356.

Palfrey, J. G. i Gasser, U. (2008). *Born digital: Understanding the first generation of digital natives*. New York: Basic Books.

Patchin, J. W. i Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth violence and juvenile justice*, *4*(2), 148-169.

Patchin, J. W. i Hinduja, S. (2010). Cyberbullying and self-esteem. *Journal of school health*, *80*(12), 614-621.

Perren, S., Corcoran, L., Mc Guckin, C., Cowie, H., Dehue, F., Völlink, T., ... i Tsatsou, P. (2012). Tackling cyberbullying: Review of empirical evidence regarding successful responses by students, parents, and schools.

Price, M. i Dalgleish, J. (2010). Cyberbullying: Experiences, impacts and coping strategies as described by Australian young people. *Youth Studies Australia*, *29*(2), 51.

Rafferty, R. i Vander Ven, T. (2014). „I Hate Everything About You": A Qualitative Examination of Cyberbullying and On-Line Aggression in a College Sample. *Deviant Behavior, 35*, 364-377.

Robotić, P. (2015). Zamke virtualnog svijeta: zaštita djece i mladih na Internetu i prevencija ovisnosti. *Časopis za primijenjene zdravstvene znanosti*, *1*(2), 81-96.

Schenk, A. M. i Fremouw, W. J. (2012). Prevalence, psychological impact, andcoping of cyberbully victims among college students. *Journal of School Violence, 11*, 21-37.

Shin, W. (2015). Parental socialization of children's Internet use: A qualitative approach. New media & society, *17*(5), 649-665.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. i Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of child psychology and psychiatry*, *49*(4), 376-385.

Smokowski, P. R., Evans, C. B. R. i Cotter, K. L. (2014). The Differential Impacts of Episodic, Chronic, and Cumulative Physical Bullying and Cyberbullying: The Effects of Victimization on the School Experiences, Social Support, and Mental Health of Rural Adolescents. *Violence and Victims*, *29*(6), 1029-1046.

Snell, P. A. i Englander, E. (2010). Cyberbullying victimization and behaviors among girls: Applying research findings in the field. *Journal of Social Sciences, 6(4),* 510-514.

Steffgen, G., König, A., Pfetsch, J. i Melzer, A. (2011). Are Cyberbullies Less Empathic? Adolescents' Cyberbullying Behavoir and Empathic Responsiveness. *Cyberpsychology, Behavior, and Social Networking, 14*(11), 643-648

Strabić, N. i Tokić Milaković, A. (2016). Elektroničko nasilje među djecom i njegova usporedba s klasičnim oblicima vršnjačkog nasilja. *Kriminologija & socijalna integracija: časopis za kriminologiju, penologiju i poremećaje u ponašanju*, *24*(2), 166-183.

Subrahmanyam, K., Garcia, E., Harsono, L. S., Li, J. S. i Lipana, L. (2009). In their words: Connecting on-line weblogs to developmental processes. *British Journal of Developmental Psychology*, *27*(1), 219-245.

Šincek, D. (2014). Gender differences in cyber-bullying. *Conference proceedings SGEM – SEGM conference on psychology and psychiatry, sociology and healthcare, education:* Vol 2. *International Multidisciplinary Scientific Conference Social Sciences and Arts* (str. 195-202). Sofija: Technology Ltd.

Šincek, D., Duvnjak, I. i Milić, M. (2017). Psychological Outcomes of Cyber-Violence on Victims, Perpetrators and Perpetrators/Victims. *Hrvatska revija za rehabilitacijska istraživanja*, *53*(2), 98-110.

Tarablus, T., Heiman, T. i Olenik-Shemesh, D. (2015). Traditional Bullying, and Socioemotional Functioning. *Journal of Aggression, Maltreatment & Trauma*, *24*(6), 707-720.

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in human behavior*, *26*(3), 277-287.

Upton Patton, D., Sung Hong, J., Ranney, M., Patel, S., Kelley, C., Eschmann, R. i Washington, T. (2014). Social media as a vector for youth violence: A review of the literature. *Computers in Human Behavior, 35*, 548-553.

Van Cleemput, K., Vandebosch, H. i Pabian, S. (2014). Personal characteristics and contextual factors that determine "helping,""joining in," and "doing nothing" when witnessing cyberbullying. *Aggressive behavior*, *40*(5), 383-396.

Vandebosch, H. i Van Cleemput, K. (2008). Defining cyberbullying: A qualitative research into the perceptions of youngsters. *CyberPsychology & Behavior*, *11*(4), 499-503.

Vejmelka, L. i Majdak, M. (2014). Specifičnosti nasilja kod djece smještene u domovima za djecu. U: Majdak, M., Vejmelka, L., Radat, K. i Vuga, A. (Ur.) Nemoj napraviti ništa u virtualnom svijetu, što ne činiš u stvarnom. Zbornik radova konferencije Nasilje na Internetu među i nad djecom i mladima (str. 51-73). Zagreb: Društvo za socijalnu podršku.

Weber, M., Ziegele, M. i Schnauber, A. (2013). Blaming the Victim: The Effects of Extraversion and Information Disclosure on Guilt Attributions in Cyberbullying. *Cyberpsychology, Behavior, and Social Networking*, *16*(4), 254-259.

Whittaker, E. i Kowalski, R.M. (2015). Cyberbullying Via Social Media. *Journal of School Violence, 14*(1), 11-29.

Willard, N. (2006). *Cyber bullying and cyberthreats: Responding to the challenge of online social cruelty, threats, and distress.* Eugene, OR: Center for Safe and Responsible Internet Use.

Wing, C. (2005). Young Canadians in a wired world. *Erin: Media Awareness Network*.

Ybarra, M. L. i Mitchell, K. J. (2004). Online aggressor/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry, 45*, 1308–1316.

Zoroja Milić, I. i Markuš, Z. (2018). Primjena informacijskih i komunikacijskih tehnologija (IKT) u kućanstvima i kod pojedinaca u 2018., prvi rezultati. *Državni zavod za statistiku.* Preuzeto s https://www.dzs.hr/Hrv_Eng/publication/2018/02-03-02_01_2018.htm 25.05.2019.

dr. sc. Valentina Ružić, prof. psihologije
Zagreb

6. RAČUNALNE IGRE

Sažetak

Neslužbenim početkom razvoja računalnih igara smatra se 1970. godina kad je u upotrebu puštena jedna od prvih igara. Od tada njihova popularnost sve više raste, a danas se smatraju jednim od najpopularnijih načina zabave djece i odraslih. U ovom trenutku diljem svijeta postoji na tisuće različitih računalnih igara čiji je sadržaj prilično raznolik. Primarna im je svrha zabava i opuštanje, ali postaju i sve većim dijelom akademskog, društvenog i emocionalnog života, a uključene su u gotovo sve sfere svakodnevnog života. Mogućnosti njihove upotrebe ograničene su samo maštom i trenutačnom razinom tehnološkog razvoja koja se iz dana u dan mijenja.

Sve se veća važnost pridaje razumijevanju učinaka igranja računalnih igara, kako pozitivnih tako i negativnih. Učinci se mogu zabilježiti u svim dijelovima života pojedinca, od kognitivnog funkcioniranja i zdravlja do društvenog života i regulacije emocija. U ovom poglavlju dan je pregled osnovnih karakteristika računalnih igara i rezultata dosadašnjih istraživanja kako bi se potaknulo razmatranje učinaka igara u širem kontekstu.

S obzirom na to da se velik broj igara može igrati i internetski u suradnji ili u natjecanju s drugim igračima, važno je imati na umu potencijalne opasnosti koje internetsko okruženje sa sobom nosi. Na kraju su poglavlja ukratko dane preporuke korisnicima, djeci i odraslima koje im mogu pomoći u odabiru prikladnih igara i zaštiti na internetu kako bi se iskustvo igranja učinilo što boljim i pozitivnijim.

6.1. UVOD

Fizičar William Higinbotham 1958. godine razvio je prvu računalnu igru koja se zvala *Pong*. Igra je služila za uvježbavanje stolnog tenisa, a u upotrebu je puštena 70-ih godina prošlog stoljeća. Njezin se izlazak smatra početkom razvoja i popularizacije te vrste zabave za svu životnu dob. Od tada se računalne igre ubrzano razvijaju, postaju sve složenije i tehnički zahtjevnije, a njihova popularnost sve više raste.

Podaci iz 2009. godine pokazuju da u Americi 88 % mladeži u dobi od 8 do 18 godina barem povremeno igra računalne igre, u trajanju od prosječno 13 sati tjedno (Groves i Anderson, 2015). Noviji podaci pokazuju da je 2018. godine prosječna dob osoba koje igraju računalne igre 34 godine, s time da je više od 70 % onih koji igraju takve igre starije od 18 godina (Entertainment Software Association, 2018). Drugim riječima, računalne igre postale su široko prihvaćene od strane svih dobnih skupina i toliko se „uvukle" u svakodnevne živote da većina ljudi svakodnevno odvaja barem sat vremena za njihovo igranje. Podaci istraživanja u Republici Hrvatskoj pokazuju da je 2017. godine svako četvrto dijete u dobi od 9 do 17 godina gotovo svakodnevno ili svakodnevno igralo neku računalnu igru (EU Kids Online Hrvatska, 2017).

Milijuni igrača diljem svijeta svaki dan igraju računalne igre, a igranje (samostalno ili s drugim igračima) postalo je jedna od najčešćih aktivnosti kojom se bave djeca, mladi i odrasli.

6.1.1. ZAŠTO SU RAČUNALNE IGRE TAKO POPULARNE?

Primarna svrha računalnih igara je zabava za igrača koja pomaže pri oslobođenju od stresa u svakodnevnom životu. Osim što omogućuju odmor od svakodnevnice i predstavljaju razbibrigu, računalne igre sadrže mnogo različitih podražaja koji privlače pozornost i koji su visokostimulativni pa zato korisnici mogu provesti sate igrajući ih.

Uz to, imaju jasnu strukturu i cilj, jasna i nepromjenjiva pravila te uključuju zadatke koje većina igrača uz manje ili više truda može riješiti. Time se igračima omogućava doživljaj uspjeha koji ih motivira za daljnje igranje.

Dodatna je privlačnost računalnih igara u njihovoj strukturi i činjenici da igrači u većini slučajeva mogu sami kontrolirati situaciju i brzinu svog napredovanja u igri. Većinom se započinje s laganijim, manje izazovnim razinama koje se zatim postupno otežavaju. Prolaskom nižih razinae igrači uvježbavaju potrebne vještine i odlučuju žele li se na tim razinama zadržati ili žele napredovati, tj. prijeći na zahtjevniju i složeniju razinu. Tijekom igre dobiva se trenutačna povratna informacija o uspjehu, a uspjeh je uvijek praćen nagradom (dodatnim bodovima, životima, prelaskom na

nove razine). S druge strane, u slučaju neuspjeha, igrač ima mogućnost ponavljanja i uvježbavanja igre koliko god je puta potrebno. Takva situacija nije karakteristična za stvarni život (u kojem su posljedice neuspjeha znatno složenije) pa su iz tog razloga igrači visoko motivirani za ostanak u virtualnom, sigurnom okruženju.

Privlačnost računalnih igara povećava se upotrebom realističnih slika i zvukova, točnih lokacija i geografskih pozicija, a vrlo često i stvarnih događaja iz povijesti ili čak aktualnih događanja. To povećava realističnost igara i uživljenost igrača, a sprečava osjećaj dosade (Eskasasnanda, 2017). Bogost i Poremba (2008) navode da su mnoge računalne igre popularne upravo zato što im je okosnica priča temeljena na stvarnim događajima ili sadržajima filmova, zbog čega se igrači lako familijariziraju s igrom. Ta realističnost stvara prostor za učenje kod igrača jer igranjem dobro osmišljene računalne igre mogu mnogo naučiti o povijesnim osobama i događajima, zemljopisnim lokacijama i mjestima, čitanju karata, navigaciji, arhitekturi određenog mjesta ili povijesnog razdoblja, fizičkim zakonima svemira i slično.

Iz tog razloga računalne igre mogu biti vrijedan i koristan alat za podučavanje te djelovati kao vrlo uspješni učitelji koji motiviraju, uključuju i razvijaju igrače i njihove vještine. Pojedine se računalne igre već godinama vrlo uspješno koriste u podučavanju školskih predmeta (npr. matematike, biologije, fotografiranja, kompjutorskog programiranja), u podučavanju sportskih vještina (poput golfa i tenisa), u podučavanju osoba s teškoćama, u uvježbavanju specifičnih vještina potrebnih za određena zanimanja (npr. vještina potrebnih za obavljanje posla kirurga, vojnika, mornara, pilota i slično), u različitim tvrtkama i organizacijama za trening novih i/ili postojećih zaposlenika, u podučavanju zdravstvenih navika (npr. djece s dijabetesom, kroničnim bolestima) te u razne druge svrhe. Smatra se da su učinkovitije čak od „običnog" televizijskog programa jer su interaktivnije i pružaju mogućnost sudjelovanja igrača, a ne samo pasivnu izloženost sadržajima.

U novije vrijeme sve su popularnije igre na internetu koje pružaju mogućnost suradnje ili natjecanja s igračima iz cijelog svijeta, upoznavanje s drugim krajevima i zemljama, kulturama i običajima te igraču omogućuju osjećaj pripadnosti skupini, stjecanje novih iskustava, a potencijalno i novih prijatelja.

6.2. VRSTE RAČUNALNIH IGARA

S obzirom na sve veći broj novih igara različitih vrsta, teško je napraviti jednu sveobuhvatnu klasifikaciju. Računalne igre možemo razlikovati ovisno o tome koja im je primarna funkcija (zabava ili neki oblik edukacije), jesu li namijenjene za jednog

igrača ili više njih, igraju li se u suradnji ili natjecanju s drugima. Također razlikujemo način njihova igranja – igraju li se na računalu ili mobitelu, uz pomoć igraće konzole ili bez, igraju li se na internetu, društvenim mrežama ili su, pak, instalirane na lokalnom računalu. Računalne igre i konzole (videoigre) prema svojim su karakteristikama relativno slične, dok igre na mobilnim aparatima predstavljaju drugačije iskustvo i najčešće traju kraće.

Jedna od mogućih podjela računalnih igara ona je koju predlaže Herz (1997) koji ih dijeli na akcije, avanture, borbe, puzzle, igranje uloga i simulacije. Slijedi opis navedenih kategorija i njihovih osnovnih karakteristika.

6.2.1. AKCIJE

Ove igre u sebi kao primarnu karakteristiku sadrže intenzivnu akciju. Za njihovo su igranje potrebni brzi refleksi, a predstavljaju možda najjednostavniju i jednu od najstarijih vrsta igara. Najpoznatija igra ovog tipa je *Super Mario*. Prvotno su bile izrađivane u 2D okruženju, ali razvojem tehnologije prelaze u 3D. Iz njih se razvijaju brojne složenije igre pa tako razlikujemo pucačine, „platforme" i slično, a ovoj skupini pripadaju i mnoge sportske igre (iako se one mogu svrstati i u simulacije ili, pak, u zasebnu kategoriju). Među najpopularnijim su igrama ove vrste *Grand Theft Auto, Monsters Hunter World* i *Sonic.*

6.2.2. AVANTURE

U ovom tipu igara igrač je glavni lik priče. On tijekom igre nailazi na različite prepreke i zagonetke. Razvoj ove vrste igara počinje još 1970. godine kad je nastala igra *Colossal Cave Adventure*, kasnije poznata kao *Zork serijal*. Prvotno su bile tekstualne, a igrač je upravljao igrom tekstualnim putem (zadajući naredbe poput „idi naprijed", „stani", „skoči" i slično na koje je računalo ispisivalo reakcije). S razvojem grafike igrači prelaze s tekstualnih naredbi na naredbe mišem. Osnovne vještine potrebne za uspješno savladavanje avantura su: rasuđivanje, kreativnost i znatiželja. Njihova popularnost u posljednjim dvama desetljećima pomalo slabi, ali i dalje su popularne igre poput *Batman, Harry Potter, Scherlock Holmes* i slične.

6.2.3. IGRE BORBE

Ove igre uključuju likove koji se međusobno bore pri čemu likove mogu kontrolirati drugi igrači ili računalo. Često se igraju borbe nastale iz filmskih serijala poput *Mortal Kombat*.

6.2.4. PUZZLE

Ova vrsta igara najčešće je zanimljiva starijim igračima, a u njih ubrajamo poznate igre poput *Tetris*, *Minesweeper, Pipe Mania* i slično. Odlične su za razvoj spacijalne inteligencije.

6.2.5. IGRE IGRANJA ULOGA (engl. *Role-Playing games - RPG*)

Ove igre omogućuju igraču preuzeti ulogu lika i igrati igru naracijom. Uključuju inovativne načine pričanja priča, a sam igrač ima potpunu kontrolu nad pričom koju stvara i osmišljava unapređujući likove. U igre ovoga tipa ubrajamo: *Final Fantasy, Diablo, Chrono Trigger, Star Ocean* i *South Park*

6.2.6. SIMULACIJE

Za ovu skupinu igara karakteristično je da je riječ o simulacijama situacija iz stvarnog života pri čemu ponovno proživljavanje tih situacija igraču pruža užitak. Relativno popularne igre ovog tipa su igre simulacija borbi ili automobilskih utrka. Također, u ovu skupinu pripadaju i simulacije socijalnih situacija, kao npr. u igri *Sims* u kojoj igrač simulira život likova različitim aktivnostima iz stvarnoga života ili *SimCity* u kojoj je cilj izgraditi grad svladavajući usput različite prepreke. Svakako jedna od najpopularnijih igara ovog tipa je *Minecraft*.

6.2.7. SPORTSKE IGRE

U ovu skupinu igara pripadaju igre koje simuliraju određenu vrstu sporta. Do sada su razvijene za gotovo sve vrste sportova, od timskih poput nogometa, rukometa i košarke do tenisa, kuglanja, lova, ribolova. Njihovoj popularnosti doprinosi to što uglavnom sve sadrže imena pravih igrača i timova, a redovito izlaze njihove nove ažurirane inačice. Najpoznatije igre ovog tipa su: *FIFA Soccer, NBA Live, NHL, Tiger Woods* i *PES*.

6.2.8. STRATEGIJE

Ove igre nazivaju se još i RTS strategije u realnom vremenu (engl. *Real-Time Strategy*). Novije igre ovog tipa oslanjaju se na samu priču i njezinu razradu, poput predvođenja vojske u nekoj povijesnoj borbi ili ratu. Najveću je popularnost postigao *Warcraft* serijal, a još su popularne igre ove vrste i *Starcraft, Dungeon Keeper, Command & Conquer* i *Age of Empires*.

Posebnu skupinu predstavljaju tzv. **arkade** koje se igraju na određenim strojevima uz pomoć žetona ili novca kojim se dobiva određen broj bodova i života. Često ih se može naći u zabavnim parkovima, kafićima i ostalim mjestima koje posjećuje velik broj ljudi u potrazi za zabavom. Najpoznatije igre ovog tipa su: poker, fliper, pikado i slično.

Postoje igre koje ne pripadaju ni jednoj od navedenih kategorija, ali i one koje se mogu svrstati u više kategorija jer obuhvaćaju i objedinjuju karakteristike više njih, što je slučaj s većinom novijih računalnih igara. Također, prema nekim podjelama posebnu skupinu računalnih igara predstavljaju **edukativne igre** odnosno edukativni programi/aplikacije, koji se koriste kao pomoć u učenju, a cilj im je učiniti učenje zabavnim i interaktivnim. Iako sliče one nisu igrice u pravom smislu riječi jer im glavni cilj nije zabava već podučavanje pa se zapravo radi o „igrolikim aktivnostima" koje olakšavaju učenje (Velki, 2018). Tako postoje aplikacije koje se usmjeravaju na učenje stranih jezika, uvježbavanje čitanja, gramatike i pravopisa, računanja, snalaženja na karti svijeta i slično.

Međutim, gotovo svaka se igra u nekoj mjeri može smatrati edukativnom jer se igranjem bilo koje igre mogu naučiti i uvježbati određena ponašanja i sposobnosti pri čemu učinkovitost same igre ovisi isključivo o igračima i njihovim karakteristikama.

6.2.9. MASIVNO VIŠEIGRAČKA IGRA IGRANJA ULOGA

U novije je vrijeme sve popularniji novi način igranja računalnih igara nazvan MMORPG (engl. *Massive Multiplayer Online Role-Playing Game*) ili Masivno višeigračka igra igranja uloga. Radi se o igrama na internetu koje omogućuju zajedničko istodobno igranje tisućama igrača. Nastale su oko 1997. godine i odmah postale masovno popularne pa se razdoblje od 1997. do 2001. godine često naziva „zlatno doba MMORPG-a". Kada je 2004. godine razvijena igra *World of Warcraft*, postala je toliki hit da je zauvijek promijenila svijet računalnih igara (Wolf, 2008). Danas je to jedna od najpopularnijih MMORPG igara koja ima više od 12 milijuna igrača/pratitelja diljem svijeta.

MMORPG igra omogućuje stvaranje lika (*avatara*) kojeg igrač sam osmišljava i daje mu karakteristike koje želi. To ovu vrstu igara čini posebno privlačnima jer igrači avataru mogu dati osobine koje ga čine sličnim njima samima ili, pak, osobine koje bi sami željeli imati u stvarnom životu. Stone (1991) smatra da na taj način igrači mogu ukloniti ograničenja vlastitog fizičkog izgleda i postati bilo tko. Pomoću avatara muškarac može postati žena, siromašan čovjek bogataš, a dijete odrasla osoba.

Najčešće se za ovakve igre plaća mjesečna pretplata iako postoje i one besplatne. Preko avatara igrači neprestano komuniciraju, što olakšava stvaranje računalnog

identiteta, uključenost u igru i disocijaciju od stvarnog svijeta (Talarn i Carbonell, 2009).

Svi su igrači u međusobnoj interakciji, pa jedan igrač svakim svojim potezom utječe na sve druge igrače. U ovim igrama i najmanja greška može biti kobna pa svaki igrač uči otkriti tragove koje ostavljaju drugi igrači, misliti unaprijed (planirati) te uči kako grupa funkcionira kao cjelina. Za uspješno igranje MMORPG igara često je nužna brzina jer su ograničenog vremena za ispunjenje određenog zadatka, dobra okulomotorna koordinacija za upravljanje likom u igri, sposobnost rješavanja zagonetki te sposobnost analitičkog mišljenja za otkrivanje dijelova i zadataka koji nas vode krajnjem cilju. U ovakvim igrama često dolazi do situacija u kojima je opstanak grupe ili većeg dijela članova ugrožen zbog čega dolazi do potrebe za zajedničkim akcijama. U takvim situacijama često pojedini igrači spase cijelu grupu, a da ni sami ne znaju kako su to učinili. Planiranje i odvijanje ovakvih akcija koristan je način učenja jer uključuje razmatranje širokog raspona mogućih akcija i posljedica takvih akcija.

U posljednjih nekoliko godina sve su popularnije igre u kojima se više igrača, koji mogu biti iz različitih dijelova svijeta, natječu kako bi ostali posljednji preživjeli. Igre ovog tipa nazivaju se Kraljevske bitke (engl. *Battle Royal*). Igrači započinju bez ikakvih pomagala, a tijekom igre osvajaju pomagala i resurse koji im omogućuju pobijediti ostale igrače. U igri je samo jedan pobjednik, a igračima je omogućeno i međusobno razgovaranje, stvaranje timova i udruživanje. Najpoznatija igra ovog tipa, a ujedno i najpopularnija igra današnjice, je *Fortnite* koja je krajem 2018. godine imala oko 200 milijuna aktivnih igrača.

6.3. POSLJEDICE IGRANJA RAČUNALNIH IGARA

Osim što su zabavne, računalne igre omogućuju učenje i/ili uvježbavanje mnogih kompliciranih ponašanja i vještina. Također, sudjeluju u stvaranju i razvijanju stavova igrača prema temama koje prikazuju te djeluju na očekivanja i vjerovanja igrača. Česta ponavljanja dovode do učvršćivanja usvojenih obrazaca i stavova, a obrazac koji je jednom naučen može određivati način interpretacije sličnih situacija u stvarnom životu. Upravo ta mogućnost prenošenja stavova, emocija i ponašanja iz virtualnog u stvarni svijet, tj. u stvarne svakodnevne situacije predstavlja mogući razlog za zabrinutost glede igranja računalnih igara.

Iako istraživači računalnih igara često izjavljuju da „ne možemo pobrojati sve njihove utjecaje kao što ne možemo pobrojati niti utjecaje hrane“ (Bavelier i sur., 2011, str. 763), slijedi kratak pregled najčešće istraživanih i spominjanih posljedica

igranja računalnih igara u nekoliko područja života (kognitivni razvoj, emocionalni razvoj, društveni život, akademsko postignuće i zdravlje).

6.3.1. SPOSOBNOSTI I VJEŠTINE

Uvriježeno je mišljenje da je igranje računalnih igara intelektualno zatupljujuće, no sve više istraživanja pokazuje da ono potiče razvoj različitih kognitivnih vještina (Granic, Lobel i Engels, 2014). Igranje igara poboljšava okulomotornu koordinaciju i finu motoriku te omogućuje uvježbavanje simultanog obavljanja više aktivnosti (engl. *multitasking*) uz veću točnost i preciznost pokreta. Zbog zahtjevnosti igara i nužnosti simultanog praćenja različitih podražaja, igrači njihovim igranjem vježbaju i razvijaju vještine vidnog procesiranja, mentalne rotacije, spacijalne vizualizacije i 2D/3D manipulacije u prostoru. Istraživači pretpostavljaju da su računalne igre izuzetno uspješan način razvijanja vještina rješavanja problema (Prensky, 2012) jer je vrlo često za uspješan prolazak pojedine razine potrebno riješiti zagonetku, otkriti rješenje problema ili povezati određene znakove koji se pojavljuju.

U današnje vrijeme, umjesto učenja eksplicitnim uputama (npr. čitanjem uputa/priručnika) mnogi pojedinci probleme rješavaju metodom pokušaja i pogrešaka, odnosno stalnim testiranjem hipoteza koje se eksperimentiranjem potvrđuju ili odbacuju (Granic i sur., 2014). Upravo je ta strategija sveprisutna u računalnim igrama.

Potrebna su daljnja istraživanja kako bi se detaljnije razjasnilo uče li upravo računalne igre igrače vještinama rješavanja problema ili zapravo računalne igre više privlače one pojedince koji su u tome uspješniji.

Važno je naglasiti da takvi učinci nisu zabilježeni kod svih vrsta igara što upućuje na to da su oni vjerojatno posljedica visokih zahtjeva igre i trodimenzionalnog prostora u kojem je potrebno vrlo brzo donošenje odluka i pozornost u nepredvidivim kontekstima (Green i Bavelier, 2012). Možda najbolje potkrepljenje toj tvrdnji pružaju mnogobrojna istraživanja igara *akcije* i usporedba njihovih učinaka s učincima drugih vrsta igara. Taj tip istraživanja najčešće se provodi s pojedincima koji nemaju gotovo nikakvo iskustvo igranja računalnih igara i to na način da ih se podijeli u dvije skupine, pri čemu jedna skupina igra igre *akcije*, a druga neku drugu vrstu računalnih igara (npr. *RPG* ili *puzzle*). Rezultati takvih istraživanja pokazuju da su igrači u prvoj skupini (nakon određenog vremena igranja) brže i točnije usmjeravali pozornost, imali bolju spacijalnu rezoluciju u vidnom procesiranju i poboljšane vještine mentalne rotacije od igrača u drugoj skupini (za pregled istraživanja navedene teme vidi Green i Bavelier, 2012).

Istraživanja koja koriste funkcionalnu magnetsku rezonanciju (fMRI) za ispitivanje učinkovitosti neuralnog procesiranja pokazuju da igrači igara *akcije* učinkovitije

usmjeravaju pozornost i učinkovitije filtriraju nevažne informacije iz okoline (Bavelier, Achtman, Mani i Föcker, 2012). Međutim, s obzirom na to da su računalne igre prepune podražaja koji lako privlače pozornost i održavaju interes igrača, realna je opasnost da kod igrača može doći do toga da im manje uzbudljivi podražaji (poput npr. slušanja predavanja) teže privlače pozornost (Prot, Anderson, Gentile, Brown i Swing, 2014). Uz to, možda su upravo djeca koja imaju probleme s održavanjem pozornosti više privučena igrama (Groves i Anderson, 2015) pa taj učinak još jače dolazi do izražaja.

Meta-analiza objavljena 2013. godine (Uttal i sur., 2012) pokazala je da je poboljšanje u vještinama vidnog procesiranja nakon igranja računalnih igara usporedivo s poboljšanjem do kojeg dovode formalni tečajevi (na srednjoškolskoj i visokoškolskoj razini) usmjereni upravo na poboljšanje tih vještina. Također se pokazalo da se te vještine mogu uvježbati u relativno kratkom vremenu, a učinci su dugoročni i prenose se izvan konteksta igara na druge prostorne zadatke.

Računalne igre zbog svoje konstrukcije i zahtjeva koje stavljaju pred igrače dovode do poboljšanja spacijalnih vještina. O važnosti tih vještina govore i rezultati longitudinalnog istraživanja (Wai, Lubinski, Benbow i Steiger, 2010) koje je trajalo 25 godina i pokazalo da su one vrlo dobar prediktor uspjeha u znanstvenom, STEM području, matematici, inžinjerstvu i tehnologiji – upravo područjima za koja se očekuje da će biti vrlo značajna u budućnosti.

Također, različita istraživanja (npr. Jackson i sur., 2012) pokazuju da je igranje bilo koje vrste računalnih igara pozitivno povezano s kreativnošću, što se nije pokazalo za uporabu ostalih oblika tehnologije poput računala, interneta ili mobitela. Međutim, opet ostaje nejasno radi li se o tome da igranje računalnih igara razvija kreativnost ili zapravo kreativnije osobe više igraju računalne igre (Granic i sur., 2014).

6.3.2. MOTIVACIJA I EMOCIJE

Računalne igre djeluju izrazito motivirajuće na igrače pa bismo mogli zaključiti da su oni koji ih osmišljavaju vrhunski stručnjaci u tome kako privući i zadržati pozornost te motivirati pojedinca za ulazak u virtualni svijet (Granic i sur., 2014). Zašto su zapravo igrači toliko motivirani za sve češće i sve duže igranje računalnih igara u kojima znatno češće doživljavaju poraz nego uspjeh?

Neposredna i konkretna povratna informacija koju igrači dobivaju igranjem zapravo je nagrada koja potkrepljuje igrača da nastavi dalje. Tajna je upravo u balansiranju optimalne razine izazova i frustracije s iskustvom doživljaja uspjeha i postignuća (Sweetser i Wyeth, 2005). Naime, računalne igre koriste neuspjeh kao motivator

omogućujući povremeno potkrepljenje (doživljaj uspjeha pri prolasku određene razine) što je najučinkovitiji obrazac za modificiranje ponašanja.

Računalne igre svojom strukturom i omogućavanjem ponovnog pokušaja prelaska pojedine razine stvaraju idealnu podlogu za vježbanje upornosti, razvijanje tolerancije na frustraciju zbog neuspjeha i za povećanje samopoštovanja zbog uspjeha. Vjerojatno igrači igranjem uče vrlo važnu poruku: upornost unatoč neuspjesima dovodi do vrijednih nagrada (Ventura, Shute i Zhao, 2013). Moguće je da se ta poruka prenosi na situacije u svakodnevnom životu iako je taj odnos potrebno detaljnije istražiti. Jedno je od rijetkih istraživanja ove teme ono koje su proveli Ventura i sur. (2013), a koje je pokazalo da je količina igranja prediktor količine pokušaja rješavanja teških zadataka/anagrama u svakodnevnom životu (izvan konteksta igara) što upućuje na to da zaista dolazi do prijenosa stečenih iskustava na svakodnevni život.

Također, istraživanja pokazuju da se igranje igara smatra jednim od učinkovitijih načina generiranja pozitivnih osjećaja (Ryan, Rigby i Przybylski, 2006). Nije rijetkost da igrači iznose da tijekom igranja doživljavaju *flow*, tj. osjećaj potpune uronjenosti u neku aktivnost uz zanemarivanje svega drugog (Sherry, 2004).

S obzirom na to da su igrači često izloženi neuspjehu, igranje računalnih igara također može dovesti do negativnih emocija poput frustracije, anksioznosti i tuge. S druge strane, upravo kontekst igranja računalnih igara omogućuje razvoj poželjnih strategija suočavanja s neuspjehom, poput prihvaćanja i ponovne procjene (Aldao, Nolen-Hoeksema i Schweizer, 2010). Strategije poput *ruminacije* vjerojatno neće biti nagrađene jer sputavaju igrača u brzom i fleksibilnom reagiranju na nove izazove.

6.3.2.1. Agresivnost

Jedno od najdetaljnije i najopširnije ispitivanih pitanja glede igranja računalnih igara je svakako njihova povezanost s agresivnim ponašanjem igrača. S obzirom na to da većina igara u sebi sadrži određenu količinu nasilja i agresije, nije čudno da je to pitanje najčešći razlog za zabrinutost i negativan stav prema igranju računalnih igara, osobito kad govorimo o djeci i mladima kao igračima. Posebno je zabrinjavajuća činjenica da se unutar igre vrlo često dobiva nagrada, tj. potkrepljenje za pojedine oblike agresivnog ponašanja, što može dovesti do formiranja stava o takvom ponašanju kao prihvatljivom i prikladnom načinu rješavanja problema.

Gentile, Lynch, Linder i Walsh (2004) navode da većina računalnih igara uključuje neki oblik nasilja. Igranje povećava učestalost agresivnog ponašanja, povećava pojavu emocija agresije, povećava znanje o agresiji i smanjuje vjerojatnost prosocijalnog ponašanja. Takvi rezultati pronađeni su kod muškaraca, žena, djece i odraslih.

Također, istraživanja pokazuju da je izloženost nasilju povezana s jačim vjerovanjem u to da je svijet opasno mjesto (Bryant, Carveth i Brown, 1981) te da igranje nasilnih igara desenzitizira pojedinca na nasilje što dovodi do smanjenja empatije (Anderson i sur., 2010) i prosocijalnog ponašanja (Greitemeyer i Mügge, 2014).

Današnje računalne igre izrazito su realistične, a igrač u njima preuzima poziciju lika kojim igra i time se na posredan način i sam agresivno ponaša. Pronađena je povezanost između igranja nasilnih igara i odobravajućih stavova prema nasilju (Funk, Bechtoldt-Baldacci, Pasold i Baumgartner, 2004) pri čemu ta veza dovodi do povećanja agresivnog ponašanja (Möller i Krahé, 2009).

Carnagey, Anderson, Bushman (2007) su po slučaju podijelili sudionike u dvije skupine koje su igrale nasilne i nenasilne igre u trajanju od 20 minuta. Po završetku igre svi su sudionici 10 minuta gledali snimku nasilja (stvarnu snimku iz svakodnevnog života) pri čemu je mjeren njihov puls i elektrodermalna reakcija kože (mjere fiziološke pobuđenosti). Rezultati su pokazali da su osobe koje su igrale nasilnu igru imale manju razinu pobuđenosti od onih koje su igrale nenasilnu igru. U sličnom su istraživanju Bartholow, Bushman i Sestir (2006) mjerili neurološki odgovor sudionika dok su gledali slike stvarnog nasilja. Pronašli su da je trajanje dugoročne izloženosti nasilju povezano sa smanjenjem neurološke pobuđenosti u dijelovima mozga koji su povezani s averzivnim sustavom motivacije, a to smanjenje pobuđenosti bilo je prediktor agresivnog ponašanja.

Kad smo suočeni s odlukom ponašati se na agresivan način, važan faktor je kakvim procjenjujemo sam čin koji planiramo, jer će pojedinci kojima agresivan čin izgleda neugodan vjerojatnije odabrati neki oblik neagresivnog odgovora (Bartholow i sur., 2006; Engelhardt, Bartholow, Kerr i Bushman, 2011).

O koliko se kompleksnom pitanju radi, najbolje pokazuju dvije meta-analize istraživanja agresivnog i nasilnog ponašanja (Anderson i sur., 2010 i Ferguson, 2007) koje su koristile gotovo jednake podatke u analizi, a dovele do prilično različitih zaključaka. Ferguson (2007) u svom radu navodi da su veličine učinaka koje se dobivaju u analizi premalene, da pružaju vrlo slabu moć predikcije i da je zbog različitih metodoloških nedostataka provedenih istraživanja gotovo nemoguće donositi bilo kakve zaključke. S druge strane, Anderson i sur. (2010) navode da su male veličine učinaka koje se dobivaju pouzdane čak i nakon kontroliranja faktora poput socioekonomskog statusa igrača, njihova IQ-a i prethodnog agresivnog ponašanja. Možda je najbolji zaključak koji možemo izvući iz ovih neslaganja istraživača taj da se radi o znatno širem i kompleksnijem pitanju nego što se na prvi pogled čini (Ferguson, 2013) te da ni jedna vrsta računalnih igara nije sama po sebi ni dobra ni loša. Vjerojatno se radi o tome da će kod igrača kod kojih su i prije igranja nasilnih igara postojala agresivna nastojanja igranjem ta nastojanja biti pojačana.

Istraživanja pokazuju da igranje računalnih igara može utjecati na razvoj mozga (Wallenius, Punamäki i Rimpelä, 2006) tako što se u mozgu pohranjuje velika količina informacija viđenih u igrama (npr. informacija koje se odnose na nasilje), što dovodi do toga da će igrači sve češće i lakše razmišljati o takvim načinima ponašanja. Igračima će biti potrebno uložiti manje napora prisjetiti se nasilja i vrste agresivnog reagiranja što će dovesti do toga da će se češće agresivno ponašati.

6.3.2.2. Sklonost rizičnom ponašanju

Mnoga su se istraživanja usmjerila i na otkrivanje odnosa između igranja igara *utrke* i rizičnog ponašanja vozača u svakodnevnom životu. Vjerojatno su u pozadini tog odnosa isti procesi koji se javljaju kad govorimo o odnosu između igranja nasilnih igara i agresivnosti igrača.

Fischer i sur. (2009) proveli su četiri zasebna istraživanja u kojima su pokazali da su sudionici koji su igrali igre utrke pokazali povećanu sklonost rizičnoj vožnji u svakodnevnom životu. Ta je sklonost bila djelomično posredovana promjenom u percepciji sebe kao rizičnog vozača. Drugim riječima, igrači koji su igrali igre utrke bili su skloniji tome da vide sebe kao rizičnog vozača i da se sukladno tome i ponašaju (imali su veću sklonost preuzimanju rizika u svakodnevnom životu) od igrača koji su igrali neku drugu vrstu računalnih igara.

Buellens, Roe i Van den Bulck (2011) su proučavali takve učinke tijekom dvije godine i pokazali da su učinci postojali i nakon tog vremena, tj. da su i dalje igrači koji su igrali igre utrke pokazivali veću sklonost „ludoj vožnji", tj. preuzimanju rizika tijekom vožnje kako bi vožnja bila zabavnija.

Vjerojatno se, kao i kod agresivnog ponašanja, zapravo radi o promjeni stava kod igrača koji su u računalnim igrama izloženi određenom tipu ponašanja. Osobe koje često igraju igre *utrke* imaju pozitivnije stavove prema preuzimanju rizika, a ti su stavovi povezani s namjerom za prihvaćanje ponašanja tog tipa u svakodnevnom životu. Ti su učinci vidljivi čak i nakon kontroliranja osobina agresivnosti i traženja uzbuđenja kod igrača (Beullens, Roe i Van den Bulck, 2011) što govori o tome da se ne radi samo o tome da pojedinci koji su podložni rizičnoj vožnji češće igraju takve igre već i da samo igranje igara utrka mijenja stavove i ponašanja igrača.

U četverogodišnjem istraživanju Hull, Brunelle, Prescott i Sargent (2014) tražili su sudionike da odrede čestinu igranja računalnih igara koje sadrže različite oblike rizičnih ponašanja i vlastito rizično ponašanje u svakodnevnom životu (npr. pušenje, rizično seksualno ponašanje, sklonost opijanju i slično). Rezultati su pokazali da je vrijeme provedeno u igranju povezano sa svim oblicima rizičnog ponašanja, a ne

samo s onim koje je prisutno u računalnoj igri koja se igra. Također je ispitano jesu li rizična ponašanja povezana sa specifičnom igrom i osobinama likova koji su uključeni u igru. Rezultati su pokazali da je igranje igara s likovima koji se rizično ponašaju u cilju da pomognu drugima (poput heroja npr. Spider-Mana) slabo povezano s rizičnim ponašanjima igrača u svakodnevnom životu, za razliku od igranja igara s likovima koji imaju drugačije motive. Vjerojatno je objašnjenje takvih nalaza u tome da igrači likove poput Spider-Mana i njihova ponašanja ne smatraju rizičnima, dok se ista ponašanja kod drugih, devijantnijih likova smatraju ponašanjima u cilju osobnog dobitka (zabave, novca, slave).

6.3.3. DRUŠTVENI ŽIVOT

Za razliku od stereotipnog vjerovanja da se igre igraju u socijalnoj izolaciji, novija istraživanja pokazuju da većina igrača igra igre s prijateljima, bilo u natjecanju ili suradnji (Entertainment Software Association, 2018). Možda je upravo to najveća razlika između suvremenih računalnih igara i onih razvijenih prije nekoliko desetljeća. Tijekom igranja igara na internetu igrači neprestano donose odluke o tome kome od drugih igrača mogu vjerovati, koga trebaju izbjegavati i kako mogu učinkovito voditi grupu. Time uče socijalne vještine i prosocijalno ponašanje koje se može generalizirati na odnose u svakodnevnom životu, izvan konteksta igre (Gentile i sur., 2009).

Osim svog relaksacijskog i zabavnog karaktera igrači računalnih igara, ponajprije MMOPG-a, često izjavljuju da im igranje igara stvara jak osjećaj zajedništva s drugim igračima (Williams, Yee i Caplan, 2008), osjećaj povezanosti s drugima i doživljaj uspjeha (Yee, 2006). Međutim, pretjerano igranje računalnih igara može dovesti i do problema u društvenom životu i smanjenja uključenosti u vlastitu zajednicu (Williams i sur., 2008). Vrlo često igrači izjavljuju da im je lakše održavati razgovore na mreži ili u svijetu igara nego u stvarnom svijetu (Smyth, 2007; Hussain i Griffiths, 2008). Iako su takve izjave potvrda socijalnog aspekta računalnih igara, upućuju i na mogući razlog za zabrinutost jer mogu dovesti do smanjenja kvalitete bliskih odnosa u stvarnom životu (Lo, Wang i Fang, 2005; Kim, Namkoong, Ku i Kim, 2008), povlačenja igrača iz društvenog života, prekida odnosa s prijateljima i obitelji te razvoda (Chappel, Eatough, Davies i Griffiths, 2006).

6.3.3.1. Poticanje stereotipa

Tijekom igranja računalnih igara dolazi i do formiranja određenih stavova o stvarima koje se u tim igrama javljaju. Važno je imati na umu da se na taj način mogu

formirati i neki loši obrasci ponašanja i stereotipi. Na primjer, u računalnim su igrama vrlo često ženski likovi prikazani kao seksualno privlačni, atraktivni i slabi, dok su muški likovi prikazani kao agresivni, snažni i dominantni (Beasley i Standley, 2002; Dill i Thill, 2007; Stermer i Burkley, 2012). Takav pristup zapravo potiče razvoj stereotipnih stavova i potiče ponašanja do kojih takvi stereotipi dovode.

Jedno od prvih istraživanja koje se bavilo tom temom provela je Dietz (1998) analizirajući sadržaj tadašnjih najpopularnijih igara. Pronašla je da je u samo 15 % igara bio prisutan ženski lik kao heroj dok je u 21 % njih ženski lik prikazan kao žrtva. Također, u 28 % njih žene su prikazane kao seksualni objekti, bilo fizičkim izgledom bilo ponašanjima koja su im dana.

Beasley i Standley (2002) u svom su se istraživanju usmjerili na ženske likove i njihovu odjeću kao indikatore seksualnosti. Pronašli su da su od 597 analiziranih likova samo njih 82 bile žene, da su ženski likovi bili oskudnije odjeveni od muških te da su imali naglašenu seksualnost. Dodatno je zabrinjavajuće bilo to da nije postojala razlika u izgledu ženskih likova u igrama namijenjenim djeci i igrama namijenjenim odraslima što upućuje na to da su već od najranije dobi djeca izložena takvim stereotipnim prikazima.

Downs i Smith (2010) su napravili pregled, tj. analizu sadržaja 60 tada popularnih igara i pronašli da su i u tom razdoblju ženski likovi, u usporedbi s muškim likovima, u igrama bili prikazani na hiperseksualizirani način – oskudno i neprimjereno odjeveni, nerealnih tjelesnih atributa. U novije vrijeme tvorci računalnih igara pokušavaju promijeniti te statistike pa se pojavio novi trend nazvan „Lara fenomen" koji se odnosi na pojavu „jakih i kompetentnih, dominantnih ženskih likova" (Jansz i Martis, 2007). Iako se povećava proporcija ženskih likova u igrama, oni su i dalje prikazani na pretjerano seksualan način, naglašeno mršavog tijela i u stereotipnim ulogama (kao pomagaći muškim likovima ili kao likovi koje je potrebno spasiti) (Mou i Peng, 2008).

U jednom je istraživanju dio sudionika gledao niz slika i računalnih igara u kojima su prikazani seksualizirani ženski likovi nakon čega su im dani opisi incidenata seksualnog zlostavljanja u kojima je muški profesor zlostavljao žensku studenticu (Dill, Brown i Collins, 2008). Rezultati su pokazali da su muški sudionici imali veću toleranciju na seksualno zlostavljanje nakon što su gledali takve slike i igre. U istraživanju koje su proveli Beck, Boys, Rose i Beck (2012) dio je sudionika gledao događaje u kojima je prisutno seksualno nasilje dok je drugi dio sudionika gledao košarku. Rezultati su pokazali da su muški sudionici iz prve skupine više podržavali stereotipe o silovanju. Dakle, u razmatranju mogućih posljedica razvoja i podržavanja stereotipa treba imati na umu da ponašanja do kojih stereotipi ponekad dovode mogu biti izuzetno opasna i imati dugoročne posljedice.

Što se tiče ostalih vrsta stereotipa, npr. etničkih, vrlo su rijetka istraživanja u kojima se oni ispituju u kontekstu računalnih igara. Vjerojatno je to posljedica namjernog izbjegavanja etničkog tipiziranja kod izrade računalnih igara, tj. pribjegavanje stvaranju likova nejasnih etničkih karakteristika. Općenito govoreći, likovi koji predstavljaju etničke skupine rjeđe se javljaju u računalnim igrama (Mou i Peng, 2008).

Istraživanja koja jesu provedena (npr. Saleem i Anderson, 2013) pokazuju da igranje igara koje uključuju etničke skupine, npr. likove Arapa prikazanih kao terorista, povećava netrpeljivost prema tim skupinama. S obzirom na to da je te oblike stereotipnih prikazivanja relativno lako izbjeći, važno je osvijestiti javnost o njihovu postojanju i mogućem djelovanju kako bi i proizvođači računalnih igara o njima vodili računa.

6.3.4. AKADEMSKI I POSLOVNI USPJEH

Računalne igre sve se češće koriste u školama za podučavanje pojedinih školskih predmeta, za podučavanje sportskih vještina te za uvježbavanje specifičnih vještina potrebnih u školskom okruženju. Također, često se u poslovnim okruženjima koriste za treninge novih i postojećih zaposlenika.

Međutim, treba imati na umu da igranje računalnih igara, posebno online MMORPG igara, zahtijeva mnogo vremena i samim time može i negativno utjecati na te aktivnosti jer se zapravo zbog njih posvećuje manje vremena školi ili poslu. Istraživanja pokazuju da je vrijeme provedeno u igranju igara povezano sa slabljenjem školskog uspjeha, tj. učenici dobivaju sve slabije ocjene jer troše više novaca i vremena na računalne igre (Gentile i sur., 2004; Smyth, 2007; Hart i sur., 2009). Ti rezultati pokazuju da pretjerano igranje računalnih igara smanjuje vrijeme provedeno u aktivnostima poput čitanja, pisanja zadaća i učenja. Međutim, ako učenici igraju samo računalne igre namijenjene edukaciji, takvi rezultati nisu zabilježeni.

Jednaka je situacija sa studentima i s odraslim osobama jer vrijeme provedeno u igranju računalnih igara i kod njih ostavlja manje vremena za druge aktivnosti. Dodatno, nekoliko je istraživanja pokazalo da je čestina igranja računalnih igara povezana s problemima na radnom mjestu i gubitkom posla (Chappell, Eatough, Davies i Griffiths, 2006; Kim i sur., 2008) što upućuje na to da se ovoj temi treba ozbiljno pristupiti. Vjerojatno je najbolji način izbjegavanja negativnih posljedica upravo ograničavanje vremena provedenog u igri kako bi se održala zdrava ravnoteža između vremena provedenog u stvarnom i u virtualnom svijetu.

6.3.5. ZDRAVLJE

Jedna od neospornih činjenica u današnje vrijeme je da i mladi i odrasli sve više vremena provode na računalu, između ostalog igrajući računalne igre. Zato su stručnjaci u području zdravstva sve više zainteresirani za učinke igranja računalnih igara na zdravlje igrača.

S obzirom na svoju edukativnu dimenziju, računalne igre vrlo se jednostavno a kreativno mogu koristiti u medicinskim intervencijama u svrhu motiviranja pacijenata i poboljšanja njihova zdravlja (za pregled vidi Kato, 2010).

Jedan od primjera takve upotrebe računalnih igara je igra Re-Mission namijenjena djeci oboljeloj od raka. U njoj je igračima omogućeno pucanje na stanice raka čime se pobjeđuju infekcije i simptomi poput mučnine i zatvora kroz koje se djecu uči najboljem načinu pristupanja tretmanu protiv raka. Istraživanje na djeci oboljeloj od raka u kontroliranoj međunarodnoj studiji pokazalo je da su oboljela djeca koja su igrala tu igru pokazala veću razinu samoučinkovitosti, veće znanje o bolesti i veću uključenost u tretman (Kato, Cole, Bradlyn i Pollock, 2008). Trenutno postoji relativno malen broj istraživanja učinaka navedene vrste igara pa se korisnicima svakako savjetuje oprez glede njihove uporabe u svrhu intervencije. Vrlo je mali broj igara do sada znanstveno evaluiran pa njihovi učinci u usporedbi s konvencionalnim pristupima nisu dokazani.

Kada govorimo o negativnim učincima igranja na zdravlje igrača, rezultati su istraživanja prilično kontradiktorni. U jednom dijelu istraživanja nisu zabilježene povezanosti između igranja računalnih igara i slabijeg zdravlja ili manje kvalitete života igrača (Smyth, 2007; Hart i sur., 2009), dok dio njih pokazuje da pretjerano igranje računalnih igara može značajno narušiti zdravlje igrača (Williams i sur., 2008). Najčešće se spominju zdravstveni problemi povezani s manjom kvalitetom sna, tj. smanjenom količinom spavanja kao posljedicom učestalog igranja (Chappel i sur., 2006; Smyth, 2007). Uz to, posljedice dugotrajne upotrebe računala mogu biti glavobolje, umor, zamagljen vid, disfunkcija mišića i slične tegobe do kojih dovodi nedostatak kretanja, manjak sna i dugotrajno sjedenje. Također su kod igrača računalnih igara zamijećeni psihosomatski problemi, bolovi u mišićima i problemi sa zglobovima šake uzrokovani neprestanim ponavljajućim pokretima. Stručnjaci potvrđuju da prekomjerno ponavljanje malih pokreta i loš položaj tijela i ruku može dovesti do ozljeda (Anđelić, Čekerevac i Dragović, 2014).

Zbog kompulzivnog igranja može doći do zanemarivanja zdravlja (Američka psihijatrijska udruga, 2014). U usporedbi s igračima drugih vrsta igara (npr. arkadnih) igrači MMORPG-a lošijeg su zdravlja, imaju manju kvalitetu sna, više teškoća sa socijalizacijom u svakodnevnom životu i slabije akademsko postignuće (Smyth, 2007).

6.3.5.1. Može li igranje računalnih igara postati ovisnost?

Općenito gledano, sve zabilježene zdravstvene posljedice igranja igara zapravo su povezane s **prekomjernim** igranjem računalnih igara, tj. ponašanjem koje se vrlo često u literaturi naziva ovisnošću o računalnim igrama. S time su povezani i neki zabilježeni ekstremni slučajevi u kojima je igranje računalnih igara dovelo do smrti igrača ili do ozbiljnog zanemarivanja vlastite djece (Sublette i Mullan, 2012), ali navedeni su slučajevi još uvijek, na sreću, rijetki.

Neka su istraživanja zaista pokazala da igrači mogu pokazivati simptome slične simptomima ovisnosti, poput teškoća u obiteljskom, akademskom i psihološkom funkcioniranju (npr. van Rooij, Schoenmakers, Vermulst, van den Eijnden i van de Mheen, 2011; Gentile i sur., 2009) te da je to u većoj mjeri slučaj s igrama na internetu posebno MMORPG igrama. Dostupne igre na internetu Kücklich (2005) dijeli na dvije skupine: „usputne, opuštene" igre kojima je svrha jedino zabava i prolazak vremena te „ozbiljne" igre koje kod igrača stvaraju stalnu žudnju za provođenjem sve više vremena igrajući ih. Najčešće se istraživači i kritičari igara na internetu uspredotočuju upravo na ovu drugu skupinu kako bi ispitali moguće štetne učinke provođenja velike količine vremena u igranju tih igara i mogućnost stvaranja ovisnosti o igrama tog tipa. Čini se da je osnova razvoja ponašanja ovisnosti o igrama slična neurobiološka podloga kao kod ovisnosti o psihoaktivnim tvarima te MMORPG igre na internetu imaju jaču komponentu ovisnosti od samostalnih računalnih igara za jednu osobu (Griffiths, Kuss i King, 2012) .

U peto izdanje *Dijagnostičkog i statističkog priručnika za duševne poremećaje, DSM-5* (Američka psihijatrijska udruga, 2014) uvrštena je kao nova kategorija ovisnost o internetskim igrama. Navedeno je da ovisnost o internetskim igrama ime veliko javnozdravstveno značenje i da zaslužuje biti neovisan poremećaj.

U DSM-u-5 se navodi da je ovisnost o kockanju trenutačno jedini poremećaj koji nije u vezi sa psihoaktivnim tvarima, ali da postoje drugi poremećaji ponašanja koji pokazuju neke sličnosti s poremećajima uzimanja psihoaktivnih tvari i s ovisnošću o kockanju. Jedan od takvih, za koje se u medicinskom okruženju obično koristi riječ ovisnost, je kompulzivno igranje igara na internetu (Američka psihijatrijska udruga, 2014). Pronađene su određene sličnosti ponašanja u ovisnosti o internetskim igrama s onim u ovisnosti o kockanju i o psihoaktivnim tvarima, ali u literaturi nema neke standardne definicije prema kojoj bi se izveli podaci o njihovoj prevalenciji.

„Ovisnost o internetskim igrama oblik je pretjeranog i prolongiranog igranja na internetu koji rezultira skupinom kognitivnih simptoma i simptoma ponašanja, uključujući progresivni gubitak kontrole nad igranjem, toleranciju i simptome sustezanja, analogno simptomima poremećaja uzimanja psihoaktivnih tvari" (Američka

psihijatrijska udruga, 2014, str. 796). Osobe s tom ovisnosti nastavljaju sjediti za računalom i sudjelovati u igrama unatoč zanemarivanju drugih aktivnosti i to obično 8–10 ili više sati dnevno, najmanje 30 sati tjedno. Ako je sudjelovanje u igrama na neki način spriječeno, pojedinci postaju uznemireni i ljuti, često provode duga razdoblja bez hrane i spavanja te zanemaruju uobičajene obveze poput škole, posla i obitelji (Američka psihijatrijska udruga, 2014).

Vjerojatno se određeni broj igrača koristi računalnim igrama kao bijegom od stvarnosti i kao načinom nošenja s drugim problemima u životu poput manjka prijatelja, teškoćama u ljubavnim vezama i problemima s fizičkim izgledom (Griffiths i Beranuy Fargues, 2009). Smahel, Blinka i Ledabyl (2008) zaključuju da stavovi igrača prema njihovim avatarima mogu imati snažnu ulogu u ovisničkoj prirodi igara na internetu. Oni igrači kod kojih su vidljivi simptomi ovisnosti najčešće smatraju svog avatara boljim od njih samih i žele biti kao on u svakodnevnom životu. Čini se da je upravo to poistovjećivanje s avatarom rizičan faktor za razvijanje tog oblika ovisnosti.

Postoje dva osnovna simptoma ovisnosti (Beranuy, Carbonell i Griffiths, 2013):

a) psihološka ovisnost koja se sastoji od žudnje, gubitka kontrole, promjene raspoloženja i

b) ozbiljni učinci koji su posljedica ovisničkog ponašanja.

Moguće je da postoje i drugi simptomi poput tolerancije, simptoma odvikavanja, kognitivne distorzije i rizika od vraćanja. Također, treba voditi računa o trajanju simptoma jer novost bilo kojeg hobija može dovesti do njegove pretjerane upotrebe koja se smanjuje s navikavanjem pa isto vrijedi i za igranje računalnih igara (Sánchez-Carbonell, Beranuy, Castellana, Chamarro i Oberst, 2008).

Beranuy i sur. (2013) iznose iskustva devet pacijenata koji su zahtijevali zdravstvenu skrb zbog različitih problema povezanih s igranjem MMORPG, pri čemu je glavni cilj istraživanja bio razumijevanje tih problema, ispitivanje njihove funkcije i usporedba simptoma takvog ponašanja sa simptomima nekih ranije priznatih ovisnosti.

Rezultati istraživanja pokazuju da igranje računalnih igara ispunjava barem tri funkcije: disocijacija, zabava i virtualno prijateljstvo. Klimmt, Schmid i Orthmann (2009) smatraju da igrači uživaju u tim igrama ponajprije zbog socijalnih odnosa koji su njihov dio, a i samo društvo igrača može stvarati pritisak na nastavak igranja. To može biti slično pritisku drugih ovisnika (npr. ovisnika o narkoticima). Također su pronađeni ostali simptomi slični ovisnosti poput: gubitka kontrole, promjene raspoloženja (npr. krivnja, depresivnost) zbog igranja i gubitka kontrole i žudnja za igranjem kada ne igraju. Ta su tri svojstva dio simptoma potrebnih za dijagnostiku

ovisnosti/psihološke ovisnosti koje su opisane kod ovisnosti o drogama (Camí i Farré, 2003) i ovisnosti o internetu (Griffiths, 2000; Sánchez-Carbonell i sur., 2008).

Prema navedenome, MMORPG zadovoljava kriterije za ovisnost – promjena raspoloženja, gubitak kontrole, žudnja i ozbiljni negativni učinci. Smatra se da MMORPG izazivaju ovisnost zbog svoje socijalizirajuće, potkrepljujuće prirode i anonimnosti koju pružaju igračima (Sánchez-Carbonell i sur., 2008; Kuss i Griffiths, 2012).

Ovisnost ne bi trebalo miješati s čestinom igranja igara jer, iako su ta dva konstrukta pozitivno povezana, oni predstavljaju zasebne, neovisne fenomene (Blinka, Škařupová i Mitterova, 2016). Bez obzira radi li se zaista o ovisnosti ili ne, trebalo bi voditi računa o znakovima mogućeg pretjeranog igranja:

- stalno produživanje vremena igranja
- tolerancija na uzbuđenje do koje dovodi igranje
- apstinencijski simptomi – nemir, nervoza, razdražljivost, agresivnost kada se pokuša smanjiti količina igranja
- nemogućnost prestajanja igranja
- gubitak zanimanja za aktivnosti koje su ranije bile važne poput zanemarivanje hobija, prijatelja i obitelji
- igranje kao bijeg od problema svakodnevice
- laganje o igranju
- sukobi s prijateljima i bliskim osobama i problemi u školi/na poslu

6.4. UTJECAJ RAČUNALNIH IGARA NA PERCEPCIJU STVARNOSTI

S obzirom na to da je ljudsko ponašanje oblikovano iskustvom, opasnost učestalog igranja računalnih igara leži upravo u tome da se iskustva iz virtualnog svijeta mogu prenijeti u stvarni svijet. U svim računalnim igrama, a posebno u MMORPG igrama koje su bogate socijalnim elementima, dolazi do **stapanja dvaju različitih svijetova** – virtualnog i stvarnog – i njihovog kombiniranja kako bi se stvorili novi i bolji načini razumijevanja i virtualnog (svijeta igre) i stvarnog svijeta (fizičkog). Drugim riječima, nestaju granice između igrača i njegova lika (avatara). Igrači tijekom igranja uče vještine korištenja mašte kako bi razmišljali izvan granica i pronašli ono što je zajedničko u obama svijetovima i ono po čemu se ta dva svijeta razlikuju. Posebno je zanimljivo pitanje što iz jednog svijeta možemo prenijeti i upotrijebiti u drugom svijetu?

Upravo anonimnost koju pruža igranje MMORPG potiče pojedince s niskim samopoštovanjem i nedovoljno razvijenim socijalnim vještinama na stvaranje virtualnog svijeta koji ponekad čak i zamjenjuje stvarni.

Još jedan faktor koji treba spomenuti je mogućnost prodaje dobara stečenih u virtualnom svijetu u stvarnom svijetu zbog čega mnogi igrači provode mnogo vremena igrajući igre i pokušavajući zaraditi novac u svakodnevnom životu (Kowert i Oldmeadow, 2013).

Ako se osvrnemo na MMORPG igre i postojanje avatara, važno je imati na umu da se u više od 50 % slučajeva stvoreni avatar razlikuje od stvarnog igrača u smislu da predstavlja idealiziran, čudan, iskrivljen dio njih samih. Stvarna je opasnost da se kod igrača može javiti miješanje navedenih identiteta, stvarnog i virtualnog. To zamagljivanje granica između stvarnog i virtualnog svijeta posebno je opasno kod djece i mladih jer postaju neosjetljivi na ponašanja koja izvode u igrama kao što su nasilje, agresija i ubijanje. Subrahmanyam, Greenfield, Kraut i Gross (2001) navode primjer djece koja su igrala *SimCity* i vjerovala da se radi o pravim ljudima koji žive od energije dobivene strujom umjesto suncem te da će ih, ako isključe računalo, ubiti. Također, kod djece moguća posljedica provođenja veće količine vremena u virtualnom svijetu je i smanjena poslušnost autoritetima (roditeljima i učiteljima) jer, igrajući igru, uče da mogu raditi po svom i na kraju dobiti što žele. Zato se preporučuje da roditelji nadgledaju i ograničavaju igranje igara kod djece te pokušaju negativne utjecaje zamijeniti pozitivnima i tako djelovati na dječje stavove, razumijevanje, reakcije i ponašanje djece.

6.5. PEGI sustav

Svakodnevno se na tržištu računalnih igara javlja velik broj novih igara i teško je stalno pratiti što koja igra sadrži i za koga je prikladna. Te su informacije osobito važne kad se radi o mlađim korisnicima igara. Zato je svakako preporučljivo pratiti oznake na igrama koje korisnike upućuju na to kako je pojedina igra klasificirana. Jedan od najpoznatijih sustava klasifikacije računalnih igara je PEGI sustav (The Pan-European Game Information System). Oznake koje navedena klasifikacija sadrži nemaju veze s težinom igara već isključivo s dobi igrača – upućuju na to za koju je dob određena igra namijenjena. Pregled PEGI dobnih oznaka, preuzet sa službene stranice https://pegi.info, te njihov opis, nalazi se u Tablici 1.

Tablica 1. Prikaz PEGI sustava dobnih oznaka

Oznaka	Opis
	Ovu oznaku imaju igre za koje se smatra da su prikladne za djecu do tri godine starosti, tj. za igrače svih dobi. Tako označene igre ne bi smjele sadržavati zvukove ili slike koje mogu prestrašiti malu djecu. Mogu sadržavati određenu količinu nasilja koje se prikazuje u komičnom kontekstu, ali ne smiju sadržavati uvredljive izraze. Važno je osigurati da dijete ne povezuje likove iz igre s osobama iz stvarnoga života.
	U ovu skupinu ubrajaju se igre koje bi mogle dobiti oznaku 3, ali sadrže neke prizore i zvukove koji bi mogli zastrašiti djecu. Mogu sadržavati blage oblike nasilja, poput impliciranog nasilja (koje nije eksplicitno) i nerealističnog nasilja.
	Ovu oznaku imaju igre koje ne bi smjela igrati djeca mlađa od 12 godina. Sadržavaju nasilje usmjereno prema izmišljenim likovima ili nerealistično nasilje usmjereno prema likovima koji izgledaju kao ljudi ili kao prepoznatljive životinje. Ove igre mogu sadržavati i seksualne sadržaje. Vulgarni izrazi ne smiju biti jako izraženi i ne smiju se koristiti psovke. Također mogu sadržavati realistične prizore kockanja (npr. kartanje za novce).
	Ove igre smiju igrati samo odrasli. Sadrže prizore nasilja (ili seksualnih aktivnosti) koji su vrlo realistični i gotovo jednaki onima u stvarnome životu. Također mogu sadržavati ekstremno vulgaran rječnik, prizore upotrebe duhana, alkohola i droga te prikaze određenih kriminalnih radnji.
	Ova klasifikacija označava da igru smiju igrati samo punoljetne osobe jer sadrže prikaze teškog nasilja i/ili sadrže ubijanje bez motiva, nasilje prema bespomoćnim likovima ili seksualno nasilje. Mogu sadržavati prikaze seksualnih aktivnosti i konzumacije droge u privlačnom svjetlu.

PEGI sustav dobnih oznaka koristi se od 2003. godine. Prihvaćen je u više od 35 zemalja diljem Europe i podržan je od strane Europske komisije. Taj sustav pruža brzu informaciju o preporučenoj dobi potencijalnih igrača. Spomenuti sustav osmišljen je kako bi pomogao roditeljima prilikom kupnje igara i pružio im pomoć u nastojanju da zaštite djecu i mlade od neprimjerenih sadržaja.

S obzirom na to da velik broj internetskih stranica sadrži i male, jednostavne igre, naknadno je osmišljena oznaka PEGI OK koju mogu dobiti igre koje su primjerene za

sve dobne skupine. Ona označava da igra ne sadržava nikakav potencijalno neprimjeren sadržaj, a izgleda ovako:

Uz PEGI dobne oznake često se mogu pronaći i objašnjenja zašto je igra dobila određenu dobnu oznaku. To mogu biti prikazi nasilja, neprimjeren rječnik, prizori koji kod djece mogu izazvati strah, prikazi diskriminacije ili sadržaji koji bi mogli potaknuti diskriminaciju i slično. U Tablici 2 prikazane su PEGI oznake sadržaja.

Tablica 2. Prikaz PEGI sustava oznaka sadržaja

Oznaka	Opis
	NASILJE Ova oznaka obilježava da igra sadrži prikaze nasilja. U igrama s oznakom PEGI 7 to može biti jedino nerealistično i implicitno nasilje, a u igrama s oznakom PEGI 12 to može biti nasilje usmjereno prema izmišljenim likovima ili nerealistično nasilje.
	NEPRIMJEREN RJEČNIK Ova oznaka obilježava da igra sadrži vulgarne sadržaje i može se naći na igrama označenima kao PEGI 12, PEGI 16 i PEGI 18.
	STRAH Ova oznaka može se naći na igrama označenima kao PEGI 7 (ako sadržava slike ili zvukove koji bi mogli prestrašiti malu djecu) i PEGI 12 (ako sadržava zastrašujuće zvukove ili efekte, ali bez nasilnog sadržaja).
	HAZARDERSKE IGRE/KOCKANJE Ova oznaka obilježava da igra sadrži elemente koji potiču kockanje ili igrača uče kockanju. Simulacije kockanja odnose se na igre na sreću koje se mogu naći u kasinima. Ovakav sadržaj mogu imati igre PEGI 12, PEGI 16 i PEGI 18.
	SEKS Ova oznaka može se naći na igrama PEGI 12 (ako sadrže seksualne sadržaje), PEGI 16 (ako sadrže golotinju ili prikaze blaže prikaze seksa) te PEGI 18 (ako sadrže eksplicitne seksualne aktivnosti). Prikazi golotinje u neseksualnom okruženju ne zahtijevaju posebnu dobnu oznaku, pa ni ova nije potrebna.

	DROGA Ova oznaka može se naći na igrama koje prikazuju upotrebu droga, alkohola ili duhanskih proizvoda. Igre s takvim sadržajem uvijek su PEGI 16 ili PEGI 18.
	DISKRIMINACIJA Igre s ovom oznakom sadrže etničke, vjerske, nacionalne i druge stereotipe i mogu poticati na mržnju. Igre s ovakvim sadržajem uvijek su PEGI 18.
	ONLINE Ova oznaka pokazuje da se igra može igrati online, s drugim igračima.

6.6. SAVJETI ZA RODITELJE I DJECU

S obzirom na moguće opasnosti i zamke koje sa sobom nosi upotreba interneta i virtualne komunikacije s drugima, iznimno je važno djecu i odrasle informirati o načinima zaštite i izbjegavanja nepoželjnih situacija. Upravo zato pružatelji usluga, istraživači i stručnjaci daju savjete čiji pregled ovdje navodimo.

Savjeti za roditelje

- Uvijek provjerite dobnu oznaku na igri.
- Potražite sažetak sadržaja igre ili neku njezinu recenziju, a najbolje je da ju i sami prvo odigrate.
- Igrajte igre sa svojom djecom, budite s njima dok ih igraju i razgovarajte s njima o igrama. Objasnite im zbog čega neke igre za njih nisu primjerene.
- Vodite računa o tome da neke igre na internetu mogu omogućavati preuzimanje dodatnog softvera koji može izmijeniti igru.
- Igre na internetu često se igraju s nepoznatim ljudima i uključuju komunikaciju s njima pa je važno upozoriti dijete da ne otkriva svoje osobne podatke i da vam kaže ako se netko meprimjereno ponaša. Upozorite dijete da ne dogovara sastanke s drugim igračima osim ako ih na njih Vi ne pratite.
- Postavite roditeljsku zaštitu na računalo.
- Prijavite neprimjereno ponašanje pisanjem komentara na stranicama ili ispunjavanjem obrazaca za pritužbu. Potaknite dijete da Vam kaže za zadirkivanje, prijetnje ili uvrede te za svaki neželjeni sadržaj ili pozive na sastanke izvan igre.

- Prekinite komunikaciju ili promijenite djetetove podatke na internetu u slučaju bilo kakvog nepoželjnog ponašanja unutar igre.

Savjeti za djecu

- Ružno ponašanje, vrijeđanje i varanje nisu prihvatljiva ponašanja i ne treba ih tolerirati ni kada ste na internetu. Možete onemogućiti takvim igračima da vas kontaktiraju, prijaviti ih pružatelju usluga i/ili reći roditeljima.
- Recite odmah svojim roditeljima ako ste naišli na neke informacije koje vam se ne sviđaju ili zbog kojih se osjećate nelagodno.
- Nemojte odavati svoje osobne podatke kao što su adresa, telefonski broj, zaporka ili fotografija.
- Nemojte se susretati s igračima s kojima igrate igre na internetu, a da o tome niste obavijestili svoje roditelje.

6.7. ZAKLJUČAK

Računalne igre same po sebi nisu loše i mogu dovesti do mnogobrojnih pozitivnih učinaka. Na primjer, čini se da određene vrste igara poboljšavaju kognitivno funkcioniranje pri čemu se ono može generalizirati i na svakodnevne životne situacije. Također, iako se čini da je igranje igara samo razbibriga, ono može poticati upornost i optimizam, povećati samopoštovanje i dovesti do pozitivnih emocija koje se mogu prenijeti na svakodnevne situacije.

Međutim, postoje i stvarne opasnosti koje se odnose na igranje igara poput mogućnosti razvijanja ovisnosti o njima, različitih zdravstvenih teškoća, društvene izoliranosti i nemogućnosti razdvajanja virtualne od fizičke stvarnosti. Iako su razlozi za zabrinutost stvarni, nije potrebno u potpunosti zabraniti igranje računalnih igara sebi i drugima. Korisnije je biti oprezan i postaviti sebi i/ili djeci i mladima jasna pravila, ograničiti vrijeme koje se provodi u igri i osvijestiti koja se ponašanja smatraju neprikladnima. Roditelji bi svakako trebali razgovarati sa svojom djecom, nadgledati njihovu igru i podučiti ih pravilima kako bi djeca bila sigurna i uživala u iskustvu igranja.

6.8. LITERATURA

Aldao, A., Nolen-Hoeksema, S. i Schweizer, S. (2010). Emotion-regulation strategies across psychopathology: A meta-analytic review. *Clinical Psychology Review, 30,* 217-237.

Američka psihijatrijska udruga (2014). *Dijagnostički i statistički priručnik za duševne poremećaje, peto izdanje, DSM-5.* Jastrebarsko: Naklada Slap.

Anderson, C. A., Shibuya, A., Ihori, N., Swing, E. L., Bushman, B. J., Sakamoto, A. i Saleem, M. (2010). Violent video game effects on aggression, empathy, and prosocial behavior in Eastern and Western countries: A meta-analytic review. *Psychological Bulletin, 136,* 151-173.

Anđelić, S., Čekerevac, Z. i Dragović, N. (2014). The Impact of information technologies on preschool child development. *Croatian Journal of Education: Hrvatski časopis za odgoj i obrazovanje, 16*(1), 259-287.

Bartholow, B. D., Bushman, B. J. i Sestir, M. A. (2006). Chronic violent video game exposure and desensitization: behavioral and event-related brain potential data. *Journal of Experimental Social Psychology 42,* 532-539.

Bavelier, D., Achtman, R. L., Mani, M. i Föcker, J. (2012). Neural bases of selective attention in action video game players. *Vision Research, 61,* 132-143.

Bavelier, D., Green, C. S., Han, D. H., Renshaw, P. F., Merzenich, M. M. i Gentile, D. A. (2011). Brains on video games. *Nature Reviews Neuroscience, 12,* 763-768.

Beasley, B. i Standley, T. C. (2002). Shirts vs. skins: Clothing as an indicator of gender role stereotyping in video games. *Mass Communication & Society, 5,* 279-293.

Beck, V. S., Boys, S., Rose, C. i Beck, E. (2012). Violence against women in video games: A prequel or sequel to rape myth acceptance? *Journal of Interpersonal Violence, 27*(15), 3016-3031.

Beranuy, M., Carbonell, X. i Griffiths, M. D. (2013). A qualitative analysis of online gaming addicts in treatment. *International Journal of Mental Health and Addiction, 11*(2), 149-161.

Beullens, K., Roe, K. i Van den Bulck, J. (2011). Excellent gamer, excellent driver? The impact of adolescents' video game playing on driving behavior: a two-wave panel study. *Accident Analysis & Prevention, 43*(1), 58-65.

Blinka, L., Škařupová, K. i Mitterova, K. (2016). Dysfunctional impulsivity in online gaming addiction and engagement. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(3), article 5.

Bogost, I. i Poremba, C. (2008). Can games get real? A closer look at „documentary" digital games. U: A. Jahn-Sudmann i R. Stockmann (Ur.), *Computer games as a sociocultural phenomenon: Games without frontiers, wars without tears.* (str. 12-21). London: Palgrave Macmillan.

Bryant, J., Carveth, R.A. i Brown, D. (1981). Television viewing and anxiety: An experimental examination. *Journal of Communication, 31*(1), 106-119.

Camí, J. i Farré, M. (2003) Drug addiction. *New England Journal of Medicine, 349*, 975-986.

Carnagey, N. L., Anderson, C. A. i Bushman, B. J. (2007). The effect of video game violence on physiological desensitization to real life violence. *Journal of Experimental Social Psychology, 43,* 489-496.

Chappell, D., Eatough, V., Davies, M. i Griffiths, M. (2006). EverQuest —It's just a computer game right? An interpretative phenomenological analysis of online gaming addiction. *International Journal of Mental Health and Addiction, 4*(3), 205-216.

Dietz, T. L. (1998). An examination of violence and gender role portrayals in video games: implications for gender socialization and aggressive behavior. *Sex Roles, 38*, 425-442.

Dill, K. E. i Thill, K. P. (2007) Video game characters and the socialization of gender roles: Young people's perceptions mirror sexist media depictions. *Sex Roles, 57*, 851-864.

Dill, K. E., Brown, B. P. i Collins, M. A. (2008). Effects of exposure to sex-stereotyped video game characters on tolerance of sexual harassment. *Journal of Experimental Social Psychology, 44*(5), 1402-1408.

Downs, E. i Smith, S. (2010). Keeping abreast of hypersexuality: A video game character content analysis. *Sex Roles, 62*(11-12), 721-733.

Engelhardt, C. R., Bartholow, B. D., Kerr, G. T., i Bushman, B. J. (2011). This is your brain on violent video games: neural desensitization to violence predicts increased aggression following violent video game exposure. *Journal of Experimental Social Psychology, 47,* 1033-1036.

Entertainment Software Association (2018). Essential facts about the computer and video game industry. 2018. Sales, demograpphic and usage data. Preuzeto s https://www.theesa.com/esa-research/2018-essential-facts-about-the-computer-and-video-game-industry/, 1.4.2019.

Eskasasnanda, D.W. (2017). Causes and effects of online video game playing among junior-senior high school students in Malang East Java. *International Journal of Indonesian Society and Culture, 9*(2),191-202.

EU Kids Online Hrvatska (2017). Preuzeto s http://hrkids.online/, 15.3.2019.

Ferguson, C. J. (2007). The good, the bad and the ugly: A meta-analytic review of positive and negative effects of violent video games. *Psychiatric Quarterly, 78,* 309-316.

Ferguson, C. J. (2013). Violent video games and the Supreme Court: Lessons for the scientific community in the wake of Brown v. Entertainment Merchants Association. *American Psychologist, 68*(2), *57-74.*

Fischer, P., Greitemeyer, T., Morton, T., Kastenmüller, A., Postmes, T., Frey, D., … Odenwälder, J. (2009). The racing-game effect: why do video racing games increase risk-taking inclinations? *Personality and Social Psychology Bulletin, 35*(10), 1395-1409.

Funk, J. B., Bechtoldt-Baldacci, H., Pasold, T. i Baumgartner, J. (2004). Violence exposure in real-life, video games, television, movies, and the internet: Is there desensitization? *Journal of Adolescence, 27,* 23-39.

Gentile, D. A., Anderson, C. A., Yukawa, S., Ihori, N., Saleem, M., Ming, L. K., … Sakamoto, A. (2009). The effects of prosocial video games on prosocial behaviors: International

evidence from correlational, longitudinal, and experimental studies. *Personality and Social Psychology Bulletin, 35,* 752-763.

Gentile, D. A., Lynch, P. J., Linder, J. R. i Walsh, D. A. (2004). The effects of violent video game habits on adolescent hostility, aggressive behaviors, and school performance. *Journal of Adolescence, 27*, 5-22.

Granic, I., Lobel, A. i Engels, R. C. M. E. (2014). The Benefits of Playing Video Games. *American Psychologist, 69*(1), 66-78.

Green, C. S. i Bavelier, D. (2012). Learning, attentional control, and action video games. *Current Biology, 22,* 197-206.

Greitemeyer, T. i Mügge, D. O. (2014). Video games do affect social outcomes: A meta-analytic review of the effects of violent and prosocial video game play. *Personality and Social Psychology Bulletin, 40*(5), 578-589.

Griffiths, M. (2000). Does internet and computer "addiction" exist? Some case study evidence. *CyberPsychology & Behavior, 3,* 211-218.

Griffiths, M. D. i Beranuy Fargues, M. (2009). Adicción a los videojuegos: una breve revisión psicológica. *Revista de Psicoterapia, 73*, 33-49.

Griffiths, M. D., Kuss, D. J. i King, D. L. (2012). Video game addiction: Past, present and future. *Current Psychiatry Reviews, 8*, 308-318.

Groves, C. L. i Anderson, C. A. (2015). Negative effects of video game play. U: R. Nakatsu, M, Rauterberg i P. Ciancarini (Ur.), *Handbook of Digital Games and Entertainment Technologies* (str. 1-26). Singapore: Springer.

Hart, G. M., Johnson, B., Stamm, B., Angers, N., Robinson, A., Lally, T. i Fagley, W. H. (2009). Effects of Video Games on Adolescents and Adults. *Cyberpsychology & Behavior, 12*(1), 63-65.

Herz, J. C. (1997). *Joystick Nation*. London: Abacus.

Hull, J. G., Brunelle, T. J., Prescott, A. T. i Sargent, J. D. (2014). A longitudinal study of risk-glorifying video games and behavioral deviance. *Journal of Personality and Social Psychology, 107*(2), 300-325.

Hussain, Z. i Griffiths, M. D. (2008). Gender Swapping and Socializing in Cyberspace: An Exploratory Study. *Cyberpsychology & Behavior, 11*(1), 47-53.

Jackson, L. A., Witt, E. A., Games, A. I., Fitzgerald, H. E., von Eye, A. i Zhao, Y. (2012). Information technology use and creativity: Findings from the Children and Technology Project. *Computers in Human Behavior, 28,* 370-376.

Jansz, J. i Martis, R. G. (2007). The Laura phenomenon: Powerful female characters in video games. *Sex Role, 56*, 141-148.

Kato, P. M. (2010). Video Games in Health Care: Closing the Gap. *Review of General Psychology, 14*(2), 113-121.

Kato, P. M., Cole, S. W., Bradlyn, A. S. i Pollock, B. H. (2008). A video game improves behavioral outcomes in adolescents and young adults with cancer: A randomized trial. *Pediatrics, 122,* e305-e317.

Kim, E. J., Namkoong, K., Ku, T. i Kim, S. J. (2008). The relationship between online game addiction and aggression, self-control and narcissistic personality traits. *European Psychiatry, 23*(3), 212-218.

Klimmt, C., Schmid, H. i Orthmann, J. (2009). Exploring the enjoyment of playing browser games. *Cyberpsychology & Behavior, 12,* 231-234.

Kowert, R. i Oldmeadow, J. (2013). (A)Social reputation: Exploring the relationship between online video game involvement and social competence. *Computers in Human Behavior 29*(4), 1872-1878

Kücklich, J. (2005). Precarious playbour: Modders and the digital games industry. *The Fibreculture Journal, 5*(1). Preuzeto s http://five.fibreculturejournal.org/fcj-025-precarious-playbour-modders-and-the-digital-games-industry/, 10.4.2019.

Kuss, D. J. i Griffiths, M. D. (2012). Online gaming addiction in adolescence: A literature review of empirical research. *Journal of Behavioural Addiction, 1,* 3-22.

Lo, S. K., Wang, C. C. i Fang, W. (2005). Physical Interpersonal Relationships and Social Anxiety among Online Game Players. *Cyberpsychology & Behavior, 8*(1), 15-20.

Möller, I. i Krahé, B. (2009). Exposure to Violent Video Games and Aggression in German Adolescents: A Longitudinal Analysis. *Aggressive Behavior, 35*(1), 75-89.

Mou, Y. i Peng, W. (2008). Gender and racial stereotypes in popular video games. U: R. E. Ferdig (Ur.), *Handbook of Research on Effective Electronic Gaming in Education* (str. 922-937). Information science reference, IGI Global.

PEGI, Pan European Game Information. Preuzeto s https://pegi.info, 10.4.2019.

Prensky, M. (2012). *From digital natives to digital wisdom: Hopeful essays for 21st century learning*. Thousand Oaks, CA: Corwin Press.

Prot, S., Anderson, C. A., Gentile, D. A., Brown, S. C. i Swing, E. L. (2014). The positive and negative effects of video game play. U: A. Jordan i D. Romer (Ur.), *Media and the Well-Being of Children and Adolescents* (str. 109-128). New York: Oxford University Press.

Ryan, R. M., Rigby, C. S. i Przybylski, A. (2006). The motivational pull of video games: A self-determination theory approach. *Motivation and Emotion, 30,* 347-363.

Saleem, M. i Anderson, C. A. (2013). Arabs as terrorists: Effects of stereotypes within a violent context on perceptions, attitudes, and affect. *Psychology of Violence, 3*, 84-99

Sánchez-Carbonell, X., Beranuy, M., Castellana, M., Chamarro, A. i Oberst, U. (2008). La adicción a internet y al móvil, ¿moda o trastorno? *Adicciones, 20*(2), 149-160.

Sherry, J. L. (2004). Flow and media enjoyment. *Communication Theory, 14*(4), 328-347.

Smahel, D., Blinka, L. i Ledabyl, O. (2008). Playing MMORPGs: Connections between addiction and identifying with a character. *Cyberpsychology & Behavior, 11*(6), 715-718.

Smyth, J. M. (2007). Beyond Self-selection in video game play: An experimental examination of the consequences of Massively Multiplayer Online Role-Playing Game Play. *Cyberpsychology & Behavior, 10*(5), 717-721.

Stermer, S. P. i Burkley, M. (2012). Xbox or SeXbox? An examination of sexualized content in video games. *Social and Personality Psychology Compass, 6/7*(7), 525-535.

Stone, A. R. (1991). Will the Real Body Please Stand Up? Boundary stories about virtual cultures. U: M. Benedikt (Ur.), *Cyberspace: First steps* (str. 81-118). Cambridge, MA: MIT PreSS.

Sublette, V. A. i Mullan, B. (2012). Consequences of play: A systematic review of the effects of online gaming. *International Journal of Mental Health and Addiction, 10*(1), 3-23.

Subrahmanyam, K., Greenfield, P., Kraut, R. i Gross, E. (2001). The impact of computer use on children's and adolescents' development. *Journal of Applied Developmental Psychology, 22*(1), 7-30.

Sweetser, P. i Wyeth, P. (2005). GameFlow: A model for evaluating player enjoyment in games. *Computers in Entertainment, 3*(3), 1-24.

Talarn, A. i Carbonell, X. (2009). Algunas reflexiones a propósito de los juegos (y los jugadores) de rol online. Identidad y adicción. *Revista de Psicoterapia, 19*(73), 50-68.

Uttal, D. H., Meadow, N. G., Tipton, E., Hand, L. L., Alden, A. R., Warren, C. i Newcombe, N. S. (2012). The malleability of spatial skills: a meta-analysis of training studies. *Psychological Bulletin, 139*(2), 352-402.

van Rooij, A. J., Schoenmakers, T. M., Vermulst, A. A., van den Eijnden, R. J. J. M. i van de Mheen, D. (2011). Online video game addiction: Identification of addicted adolescent gamers. *Addiction, 106,* 205–212.

Velki, T. (2018). *Priručnik za rad s hiperaktivnom djecom u školi*. Jastrebarsko: Naklada Slap.

Ventura, M., Shute, V. i Zhao, W. (2013). The relationship between video game use and a performance-based measure of persistence. *Computers & Education, 60,* 52–58.

Wai, J., Lubinski, D., Benbow, C. P. i Steiger, J. H. (2010). Accomplishment in science, technology, engineering, and mathematics (STEM) and its relation to STEM educational dose: A 25-year longitudinal study. *Journal of Educational Psychology, 102*(4), 860-871.

Wallenius, M., Punamäki, R. L. i Rimpelä, A. (2006). Digital Game Playing and Direct and Indirect Aggression in Early Adolescence: The Roles of Age, Social Intelligence, and Parent-Child Communication. *Yournal of Youth and Adolescence, 36,* 325-336.

Williams, D., Yee, N. i Caplan, S. E. (2008). Who plays, how much, and why? Debunking the stereotypical gamer profile. *Journal of Computer-Mediated Communication, 13*(4), 993-1018.

Wolf, K. D. (2008). The Instructional Design and Motivational Mechanisms of World of Warcraft. U: J. Fromme i A. Unger (Ur.), *Computer Games And New Media Cultures. a Handbook of Digital Games Studies* (557-570). London: Springer.

Yee, N. (2006). Motivations for Play in Online Games. *Cyberpsychology & Behavior, 9*(6), 772-775.

PRAVNI ASPEKTI DIGITALNOG SVIJETA

doc. dr. sc. Barbara Herceg Pakšić
Pravni fakultet Sveučilišta Josipa Jurja Strossmayera u Osijeku

7. VIRTUALNA KOMUNIKACIJA I IZAZOVI KAZNENOG PRAVA NOVOG DOBA

Sažetak

Kazneno pravo dio je pravnog sustava svake države sa zadaćom određivanja kaznenih djela i sankcija za počinitelje tih djela. Ovo poglavlje sadrži osvrt na kaznenopravne stavove hrvatskog zakonodavca kad je riječ o izazovima virtualne komunikacije. Naime, prihvaćajući da je napredovanjem tehnologije i kriminalitet pridobio nove oblike i obrise koji na specifičan način štete ljudskim pravima i slobodama, Kazneni zakon nastoji suzbijati takva neprihvatljiva ponašanja propisivanjem kaznenih djela i odgovarajućih sankcija za njih. Riječ je o dinamičnom području unutar kojega se situacija brzo mijenja, a i kaznenopravni autori nisu suglasni o tome kako pravilno reagirati na specifične negativne društvene fenomene ove sfere. Utoliko je tema ovoga poglavlja podrobniji prikaz dviju odabranih tema virtualnog kriminaliteta, i to govora mržnje koji se iznosi na internetu te virtualnog mamljenja djeteta radi njegovog spolnog iskorištavanja. U posljednjem se dijelu iznose neke napomene koje se odnose na specifičnost kaznenopravnih sankcija te rasprostranjenost interneta, računala i računalnih podataka u pozitivnom tekstu Kaznenog zakona.

7.1. UVODNE NAPOMENE

Skup modaliteta komunikacija na internetu (engl. *online communication*) okupljenih pod pojmom informacijsko-komunikacijska tehnologija, proizvod je novijeg doba. Uz brojne prednosti uporabe podrazumijeva i mnogobrojne rizike kojih korisnici (a i osobe s njima povezane) moraju biti svjesni kako bi se mogli zaštititi, u što se poglavito ubraja standardni korpus ljudskih prava i sloboda. Relevantni nacionalni i međunarodni dokumenti priznaju moguću opasnost informacijsko-komunikacijskih tehnologija. To je osobito značajno kod različitih štetnih ponašanja spram djece koji uz mladež općenito pripadaju osobito osjetljivoj društvenoj skupini. Njihov je viktimizacijski rizik povećan i uvjetovan nizom razloga što posljedično znači i povećanu društvenu potrebu za njihovom zaštitom. Kazneno je pravo dio javnog prava, posljednje zaštitno sredstvo države, koje svoj utjecaj i zadaću vrši prijetnjom državne prisile kao najjačeg oblika prisile u društvu. Propisivanjem kaznenih djela i pripadajućih sankcija, odnosno kazni, kazneno pravo nastoji suzbiti sva ona ponašanja pojedinaca ili pravnih osoba koja su zbog njihove neprilagođenosti zajedničkom životu, pogibeljnosti za određene vrijednosti i dobra u toj zajednici ili iz drugih razloga neprihvatljiva i zbog toga nedopuštena i zabranjena (Horvatić, Derenčinović i Cvitanović, 2016., str. 7). Kazneno pravo nastoji odgovarajuće sankcionirati počinitelje kaznenih djela, onemogućiti ponovno počinjenje djela, utjecati na potencijalne počinitelje da ne čine kaznena djela, proklamirati pravednost kažnjavanja i jačati povjerenje građana u pravni poredak. Isto tako, svojim mehanizmima nastoji zaštititi žrtve kaznenih djela te omogućiti zajedničku sigurnost života u društvu. S obzirom na opseg poglavlja nije moguće obraditi sve izazove koje uporaba interneta stavlja pred kazneno pravo. Internet je pogodan medij za potencijalna kaznena djela stoga je nastao novi prostor inkriminiranja i za neka područja ponašanja koja nisu bila inkriminirana u prošlim kaznenim zakonima. Računalni kriminalitet vrlo je širok pojam koji se još naziva i visokotehnološki kriminalitet, e-kriminalitet, cyber-kriminalitet. Zbog toga smo pozornost usredotočili na dva specifična negativna fenomena uz razradu nekih dodatnih pitanja koja se javljaju u kaznenopravnom sustavu pri analizi te vrste kriminaliteta. Uporabom informacijsko-komunikacijskih tehnologija uobičajena kaznena djela dobivaju nove modalitete odnosno načine počinjenja. Znamo da se kazneno pravo ne razvija kao izoliran sustav, već na njega itekako utječe činjenica da je Republika Hrvatska članica međunarodnih i europskih asocijacija. Zato je pri obradi nužno prikazati i one akte koji su utjecali na današnji normativni okvir i inkriminacije u Kaznenom zakonu. Potom se, uz relevantne kaznenopravne odredbe, razmatraju suštinske konture pojedinih odabranih štetnih ponašanja u virtualnom svijetu u kojemu se kao žrtve pojavljuju mlade osobe. Utoliko ćemo, u poglavljima koja slijede, podrobnije razmotriti dva negativna društvena

fenomena, štetna ponašanja na internetu: govor mržnje (engl. *online hate speech*) kao kršenje slobode izražavanja. Potom, mamljenje djeteta za zadovoljenje seksualnih potreba (engl. *grooming, sexual grooming*) te ćemo u konačnici spomenuti neka specifična pitanja koja pokazuju prilagodljivost kaznenog prava na kaznena djela koja se čine u virtualnom svijetu.

7.2. GOVOR MRŽNJE I NJEGOV MREŽNI MODALITET

Sloboda izražavanja jedna je od esencijalnih sloboda svakog suvremenog društva. Zajamčena je važnim međunarodnim dokumentima, poput Konvencije za zaštitu ljudskih prava i temeljnih sloboda (čl. 10) ili Povelje o temeljnim pravima Europske unije (čl. 11. st. 1). Europski je sud za ljudska prava istakao kako je Ta sloboda konstitutivni element društva i temeljni preduvjet njegovog razvoja (Handyside v. United Kingdom, 1976). Međutim, u toj je presudi sud istaknuo i kako je zajamčena sloboda izražavanja primjenjiva i na izjave ili informacije koje uznemiruju ili šokiraju društvo, što otvara pitanje granica dopuštenog slobodnog izražavanja. Sloboda izražavanja nije neograničena, podliježe specifičnim granicama izražavanja a jedno od nedopuštenih izražavanja obuhvaća i tzv. govor mržnje. Prema svakodnevnom iskustvu možemo reći da je riječ o relativno čestom društvenom fenomenu, lako prepoznatljivom, koji međutim nije obuhvaćen univerzalno prihvaćenom definicijom (Simpson, 2013). Ipak, u literaturi se najčešće koristi opis da govor mržnje obuhvaća „sve oblike izražavanja kojima se šire, raspiruju, potiču ili opravdavaju rasna mržnja, ksenofobija, antisemitizam ili drugi oblici mržnje temeljeni na netoleranciji, uključujući tu i netoleranciju izraženu u obliku agresivnog nacionalizma i etnocentrizma, te diskriminacija i neprijateljstvo prema manjinama, migrantima i osobama imigrantskog porijekla" (Preporuka Ministarskog odbora Vijeća Europe No. R (97) 20, 1997). „Mržnju" bi trebalo shvaćati kao upućivanje na mržnju utemeljenu na rasi, boji, vjeroispovijesti, porijeklu ili nacionalnom ili etničkom podrijetlu. (Okvirna odluka vijeća 2008/913/PUP od 28. studenoga 2008. o suzbijanju određenih oblika i načina izražavanja rasizma i ksenofobije kaznenopravnim sredstvima). Takav način izražavanja usmjeren je dakle prema specifičnim društvenim skupinama, a sadržaj mu je obilježen izrazima mržnje i zbog toga se oni koji ga koriste ne mogu pozivati na slobodu izražavanja. U spomenutoj je Preporuci također navedeno kako bi države članice trebale „utvrditi i održavati cjeloviti pravni okvir koji se sastoji od građanskih, kaznenih i upravnih zakonskih odredbi o govoru mržnje."

Ciljevi su govora mržnje višestruki, no svakako su najpogubniji spram pripadnika skupine na koju je usmjeren. Među ciljevima Alaburić (2003) navodi sljedeće: emocionalni stres, osjećaj poniženja i gubitka ljudskog dostojanstva, negiranje i ograničavanje osobnih sloboda i ljudskih prava žrtava, interiorizacija diskriminatorne poruke, održavanje i daljnje perpetuiranje stanja/odnosa subordinacije i društvene i političke nejednakosti, ušutkavanje žrtava na način da ih se zastrašivanjem i prijetnjama zapravo onemogućava u odgovaranju, što ima porazne posljedice za kvalitetu ukupnog javnog diskursa te lako poticanje na fizičko nasilje.

Posljedice govora mržnje višestruko su društveno štetne i pogubne. Međutim, prikladna društvena reakcija na verbalizaciju diskriminacije, netolerancije i nasilja veliki je izazov. Nema jednostavnih smjernica kako se suočiti s govorom mržnje u općim komunikacijskim procesima pa je zbog toga riječ i o odnosu pravnog sustava prema slabijima i drukčijima (Herceg Pakšić i Lachner, 2015). Zbog toga ga je potrebno suzbijati, ograničavati i sankcionirati kaznenim pravom. Da to nije lako uspješno izvesti, govore i stajališta kako je riječ o najkompleksnijem problemu u području slobode izražavanja (Alaburić, 2003). Dodatno, važno je istaknuti da govor mržnje (bez obzira na terminološko oblikovanje fenomena), nije ograničen samo na riječi, već se može raditi i o simbolima, slikama, fotografijama, gestama, glazbi – koji su usmjereni na izražavanje predrasudnog, nasilnopoticajnog mišljenja (Herceg Pakšić, 2017). Isto tako, govor mržnje obuhvaća i tzv. *denijalizam* (Lobba, 2015), odnosno negiranje, umanjivanje ili opravdavanje zločina holokausta i drugih nacističkih zločina, potom genocida i zločina protiv čovječnosti.

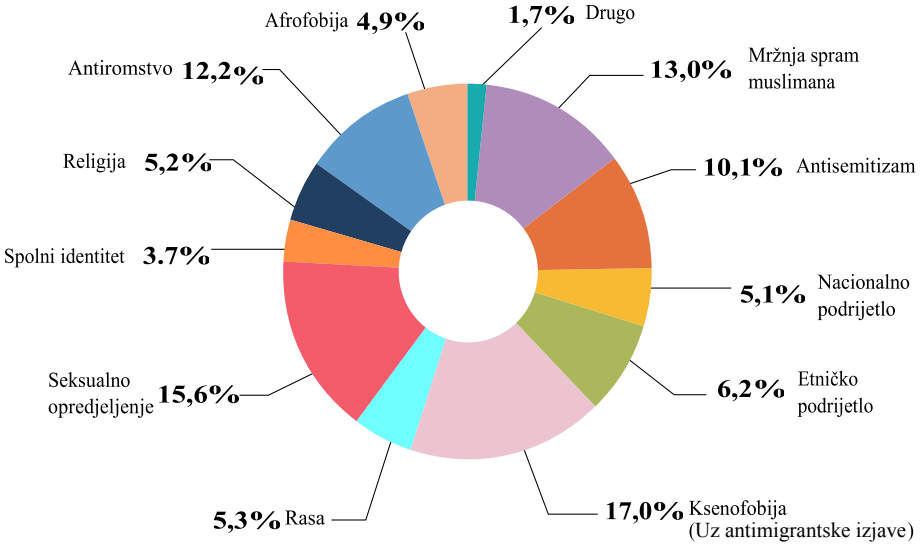
Razvojem društvenih mreža govor je mržnje, uz *offline*, dobio i *online* modalitet. Sukladno istraživanjima pojavnih oblika govora mržnje u sudskoj praksi u Republici Hrvatskoj, neki autori ukazuju kako se prevalentno vrši uporabom društvenih mreža odnosno Facebooka (Munivrana Vajda i Šurina Marton, 2016, str. 446).

U pravnom sustavu Republike Hrvatske govor je mržnje zabranjen cijelim spletom relevantnih odredaba. Riječ je o odredbama ustavnog ranga gdje, primjerice, odredba čl. 39 zabranjuje i proglašava kažnjivim svako pozivanje ili poticanje na rat ili uporabu nasilja, na nacionalnu, rasnu ili vjersku mržnju ili bilo koji oblik nesnošljivosti. Potom zakonski rang podrazumijeva Kazneni zakon koji u čl. 325 pod nazivom Javno poticanje na nasilje i mržnju kaznom zatvora do tri godina zapriječuje ponašanje kojim se tiskom, radijom, televizijom, računalnim sustavom ili mrežom, na javnom skupu ili na drugi način javno potiče ili javnosti učini dostupnim letke, slike ili druge materijale kojima se poziva na nasilje ili mržnju usmjerenu prema skupini ljudi ili pripadniku skupine zbog njihove rasne, vjerske, nacionalne ili etničke pripadnosti, jezika, podrijetla, boje kože, spola, spolnog opredjeljenja, rodnog identiteta, invaliditeta ili kakvih drugih osobina. Također, predmetni kazneni članak

sankcionira i udruživanje u skupinu radi počinjenja tog djela kao i organizaciju i vođenje skupine te već spomenuti denijalizam. Međutim, niz prekršajnih zakona također sankcionira govor mržnje, poglavito kad je riječ o sprečavanju nereda na sportskim natjecanjima, potom prekršajima protiv javnog reda i mira, suzbijanju diskriminacije, prekršaji koji se mogu počiniti pri javnim okupljanjima. Dodatno, splet zakona u području reguliranja djelovanja medija (tzv. medijsko zakonodavstvo) dotiče se i govora mržnje. Primjerice, Zakon o elektroničkim medijima proklamira kako audiovizualni i radijski programi trebaju poštovati ljudsko dostojanstvo i ljudska prava i temeljne slobode te pridonositi poštivanju tuđih mišljenja i uvjerenja te promicati međusobno razumijevanje te da nije dopušteno prenositi priloge koji vrijeđaju dostojanstvo čovjeka ili na bilo koji način potiču, promiču i veličaju nasilje.

Govor mržnje koji se čini na interentu u središtu je pozornosti na europskoj razini. Države članice Europske unije imaju odgovornost štiti svoje građane od takvog govora te koristiti učinkovite nacionalne mehanizme među koje pripada i kazneno pravo. Utoliko postoji cijeli niz inicijativa kojima se njegovo suzbijanje nastoji učiniti što uspješnijim. Najprije, važno je istaknuti da rasizam i ksenofobija predstavljaju neposredno kršenje načela slobode, demokracije, poštovanja ljudskih prava i temeljnih sloboda i vladavine prava, načela na kojima se temelji Europska unija i koja su zajednička državama članicama. Stoga se propisuje obveza da se ustanove kaznena djela koja se odnose na rasizam i ksenofobiju u nacionalnim pravnim sustavima (Okvirna odluka vijeća 2008/913/PUP od 28. studenoga 2008. o suzbijanju određenih oblika i načina izražavanja rasizma i ksenofobije kaznenopravnim sredstvima, 2008). Europska komisija te četiri velike internetske platforme, odnosno IT tvrtke – Facebook, Twitter, Youtube i Microsoft, u svibnju 2016. godine predstavili su Kodeks postupanja za borbu protiv nezakonitog govora mržnje na internetu. Potom su i drugi slijedili njihov primjer pa su Instagram, Google+, Snapchat, Dailymotion and jeuxvideo.com najavili pristupanje tom Kodeksu. U njemu se ističe potreba da je na ilegalni govor na internetu potrebno reagirati ekspeditivno, putem mrežnoga posrednika i platformi društvenih medija, i to, čim je zaprimljena obavijest, ukloniti ju u primjerenom vremenskom roku koji je određen kao 24 sata od obavijesti. Primjena, odnosno implementacija tog kodeksa prati se i evaluira redovito od strane Europske komisije (Countering illegal hate speech online #NoPlace4Hate, 2019). Posljednje, četvrto izvješće pokazalo je kako IT tvrtke nadziru većinu prijava u roku od 24 sata te miču oko 72 % govora mržnje koji im se prijavi. Od svih društvenih mreža Facebook zaprima najveći broj prijava, potom Twitter pa Youtube. Sukladno tom izvješću, kad je riječ o temeljima mržnje, najveći postotak odlazi na ksenofobiju, a slijedi ju mržnja prema seksualnoj orijentaciji. U najvećem je broju dakle govor mržnje motiviran rasističkom mržnjom prema etničkim manjinama, migrantima i

izbjeglicama (Code of Conduct on countering illegal hate speech online, Fourth evaluation confirms self-regulation works, 2019). U grafičkom prikazu daju se temelji iskazanog govora mržnje sukladno najnovijim podacima spomenutog izvješća.



Grafički prikaz preuzet iz: Code of Conduct on countering illegal hate speech online, Fourth evaluation confirms self-regulation works, 2019, str. 5.

U cilju veće učinkovitosti uklanjanja govora mržnje, Europska unija financira različite projekte iz toga područja. Primjerice, „Platforms, Experts, Tools: Specialised Cyber-Activists Network (sCAN)“, „Social and Emotional Learning for Mutual Awareness (SELMA)“, „Hatemeter“, „International Network Against Cyber Hate (INACH)“.

Dodatno, u rujnu 2017. godine Europska je komisija usvojila Komunikaciju o postupcima za prijavu i uklanjanje nezakonitog sadržaja na internetu unutar koje se nalaze smjernice za društvene mreže (Communication on Tackling Illegal Content Online - Towards an enhanced responsibility of online platforms, 2017.)

Da su nezakoniti sadržaji na internetu općenito veliki izazov, potvrđeno je i u ožujku 2018., Preporukom Europske komisije za učinkovito suzbijanje takvih sadržaja. Riječ o širem pojmu jer nezakoniti sadržaju nadilaze govor mržnje i obuhvaćaju i mnoge druge pojave koje su prethodno već dobile neki oblik europskog akta kojim se zahtijeva suzbijanje. Dakle, nezakonit sadržaj obuhvaća sve informacije koje nisu u skladu s pravom EU-a ili pravom država članica, primjerice teroristički sadržaj, materijale koji se odnose na seksualno zlostavljanje djece, nezakoniti govor mržnje,

poslovne prijevare i zlouporabe ili povrede prava intelektualnog vlasništva (Preporuka Komisije za učinkovito suzbijanje nezakonitog sadržaja na internetu, 2018). Ta je preporuka sadržajno povezana uz prethodno spomenutu Komunikaciju iz 2017. te joj je cilj utvrditi operativne mjere koje bi pružatelji usluga i države članice trebali provesti radi otkrivanja nezakonitog sadržaja na internetu i njegova uklanjanja primjenom reaktivnih mjera (tzv. postupcima „obavješćivanja i djelovanja") ili proaktivnim mjerama.

Neke su države članice usvojile recentno zakonodavstvo kojim nastoje na nacionalnoj razini smanjiti pojavu govora mržnje na internetu jasno uspostavljajući odgovornost društvenih platformi za uklanjanje nezakonitih sadržaja. U tom smislu Njemačka je u srpnju 2017. godine usvojila Zakon o jačanju provedbe zakona na društvenim mrežama (Netzwerkdurchsetzungsgesetz-NetzDG) koji je usmjeren na reguliranje odgovornosti društvene mreže. Neki su hrvatski autori već predložili da se prilagođen oblik takvog zakonskog teksta usvoji i u Hrvatskoj (Roksandić Vidlička i Mamić, 2018, str. 345). Sukladno dostupnim podacima u trenutku pisanja ovih redaka Republiku Hrvatsku očekuje poseban zakon. Najavljen je Zakon o nedopuštenom ponašanju na internetu kojim bi se željelo regulirati pravila ponašanja na društvenim mrežama, odnosno definirati odgovornost za objavljeni sadržaj na internetu i društvenim mrežama.

7.3. MAMLJENJE DJETETA ZA ZADOVOLJENJE SPOLNIH POTREBA (ENGL. *ONLINE GROOMING*)

Seksualno izrabljivanje i zlostavljanje djece posebno je osjetljiva tema koja zaokuplja pozornost svojom aktualnošću, pogotovo u novije vrijeme. Prije svega jer je riječ o žrtvama koje su najranjivija društvena kategorija. Potom i zbog toga što suzbijanje tih ponašanja zahtijeva od kaznenog zakonodavca specifičan pristup: posebno oblikovane inkriminacije, dodatna pravila unutar kaznenog postupka kako se žrtve ne bi dodatno viktimizirale te posebno educirane osobe koje s djetetom dolaze u kontakt u različitim stadijima kaznenog postupka. Posljedice koje to zlostavljanje ostavlja osobito su teške za djetetov psihofizički razvoj te najčešće traju cijeli život. Prvi je svjetski kongres, tematski orjentiran prema suzbijanju seksualnog izrabljivanja djece, održan prije više od dva desetljeća (1996. godine) u Stockholmu (Muntarbhorn, 2007). Na njemu su sudjelovali predstavnici 122 vlade, a navodi se da je to bilo prvo javno priznanje vlada spram postojanja te vrste nasilja nad djecom. U međuvremenu je razvoj tehnologije iznjedrio nove izazove takve vrste zaštite. Ponajprije se misli na nove oblike zlostavljanja djece modalitetima na internetu odnosno uporabu informa-

cijsko-komunikacijskih tehnologija kao što su slanje eksplicitnih seksualnih poruka (engl. *sexting*), mamljenja ili vrbovanja djece radi seksualnog kontakta (engl. *grooming*), virtualnog zlostavljanja (engl. *cyberbullying*) uz već postojeći problem dječje pornografije na internetu kao iznimno profitabilnog oblika virtualnog kriminaliteta (engl. *cyber-crime*). Takva ponašanja često prolaze nekažnjeno te statistički podaci ukazuju na nizak udio procesuiranja kaznenih djela iz seksualne sfere, a stvarni broj djece žrtava tog zlostavljanja ostaje nepoznat. Navedeni fenomen zaokuplja pažnju poredbenih autora već više od desetljeće i pol, koliko ga poznaju i neka zakonodavstva. Primjerice, u Engleskoj je mamljenje ili vrbovanje djece radi seksualnog kontakta (engl. *grooming*) postalo kazneno djelo 2003. godine kad je kroz Sexual Offences Act u čl. 15. unesena ta inkriminacija pod nazivom Susret s djetetom praćen seksualnim mamljenjem (engl. *Meeting a child following sexual grooming)*. Od tada se broj prijavljenih slučajeva i osuda stalno povećava (Kool, 2011, str. 47). Iste godine uvela ga je i Njemačka, ali ne kao zasebnu inkriminaciju, nego kao dio inkriminacije u par. 176. Kaznenog zakona (*Strafgesetzbuch*) koji se zove Seksualna zlouporaba djece (njem. *Sexueller Mißbrauch von Kindern*). U Hrvatskoj opsežnije rasprave još nije bilo zbog čega je i razumijevanje tog pojma na rudimentarnoj razini.

Primjerice, u pravilu se vezuje uz uporabu interneta odnosno ima modalitet na internetu, no to je samo jedan od načina na koji se počinitelji približavaju djeci i podložan je tzv. konceptu opasnog stranca (engl. *stranger-danger*). Istraživanja pokazuju da seksualni zlostavljači zlostavljaju djecu koju znaju od prije, kontakt sa žrtvama u velikoj se mjeri događa dakle *off-line* metodama (u školama, klubovima, ili u obitelji), a sama se zlostavljanja odvijaju u domu žrtve ili domu zlostavljača. Utoliko se mamljenje ili vrbovanje djece radi seksualnog kontakta (engl. *grooming*) događao i događa se mimo informacijsko-komunikacijskih tehnologija, i to osobnom interakcijom s djetetom najčešće u javnom prostoru ili osobom od povjerenja, a samo je njegova inačica na internetuzapravo nešto novo. Ipak, može se govoriti o tome da se mamljenje djece može lakše počiniti na internetu s obzirom da su djeca u takvom okruženju manje inhibirana a time i više ranjiva.

Imajući sve to u vidu, a slijedeći suvremena kretanja u tom području, hrvatski se zakonodavac odlučio na novi pristup realiziran prilikom stvaranja Kaznenog zakona: stvorena je nova glava inkriminacija s ciljem učinkovitije zaštite djece od različitih oblika zadiranja u njihov spolni integritet i slobodu, a pritom su uzete u obzir relevantne odredbe međunarodnih akata kao i trendovi u komplementarnim kaznenopravnim sustavima. U daljnjem tekstu usredotočit ćemo se na kriminalizaciju mamljenja ili vrbovanja djece radi seksualnog kontakta (engl. *grooming*) kao novog kaznenog djela koji u hrvatskom Kaznenom zakonu nosi naziv Mamljenje djece za zadovoljenje spolnih potreba, iz čl. 161.

Spolno mamljenje ili vrbovanje djece radi seksualnog kontakta (engl. *sex grooming*) uporabom informacijske i komunikacijske tehnologije samo je jedan relativno novi aspekt spolnog iskorištavanja djece u kibernetičkom prostoru koji može, ali ne mora, uključivati eksplicitnu komunikaciju spolne prirode, a podrazumijeva uspostavljanje kontakta u kibernetičkom prostoru s namjerom spolnog zlostavljanja djeteta u stvarnom svijetu (O'Connell, 2003) (Škrtić, 2013, str. 1143). Drugo određenje kaže da je riječ o odraslim osobama koje aktivno pristupaju djeci i zavode ih na društvenim mrežama, profilima, soba za razgovor na internetu i sličnim virtualnim grupama s ultimativnom namjerom počinjenja seksualnog nasilja spram djece ili proizvodnje pornografskog materijala s djecom (Kool, 2011, str. 48).

Spolno mamljenje ili vrbovanje djece radi seksualnog kontakta u kaznenom pravu jest nova inkriminacija, no nije riječ o novom konceptu. Psihološka ga literatura poznaje kad je riječ o seksualno devijantnom ponašanju. Lingvistički termin se odnosi na pripremu za specifičnu svrhu, ulogu ili funkciju, a u literaturi se upotrebljavaju termini poput *cyber eksploatacije*, *internet zavođenja*, *pripreme djeteta*, *seksualnog groominga* i sl. Smatra se da ga je prvi oblikovao Salter 1995. godine i to kao proces kojim zlostavljač vješto manipulira djetetom stvarajući situaciju u kojoj ono može biti lakše zlostavljano uz manju vjerojatnost da će otkriti o čemu je riječ.

Pripreme počinitelja podrazumijevaju razvijanje digitalnog profila radi prikrivanja stvarnog identiteta (spola, starosti, uključujući i prikrivanje lokacije s koje se ostvaruje komunikacija, vrste informacijsko-komunikacijske opreme, odnosno računala ili mobitela, pretplatničkog broja, IP adrese) i iniciranje digitalnog kontakta s mladom osobom (Škrtić, 2013, str. 1144). Počinitelj zadobiva djetetovo povjerenje bilo izravno (osobnim kontaktom, ako je riječ o *offline groomingu*) bilo uporabom interneta manipulacijom radi kasnijeg seksualnog zlostavljanja u okolnostima koje dopuštaju potpunu kontrolu nad djetetom.

Sukladno recentnim istraživanjima postoje tri tipa počinitelja spolnog mamljenja ili vrbovanja djece radi seksualnog kontakta (engl. *grooming*): oni koji traže intimnost (bez prethodnih osuda za seksualna kaznena djela, u virtualnom svijetu ne mijenjaju svoje indentitet, teže ostvaruju intimni kontakt i dobivaju pristanak mlade osobe, ne komunniciraju na internetu s drugim seksualnim prijestupnicima). Potom, prilagodljive osobe (s ranijim osudama za seksualna kaznena djela, djecu smatraju zrelima, neki od njih imali su neprimjerene fotografije djece, no ne u velikoj mjeri, a ključna je stvar da su prilagođavali svoj virtualni identitet dobi djeteta s kojim su komunicirali) te u konačnici hiperseksualizirane osobe (posjeduju ekstenzivne kolekcije neprimjerenih fotografija djece za što su neki pripadnici te skupine i osuđeni, često komuniciraju s drugim seksualnim prijestupnicima, imaju različite virtualne

identitete, kontakti su s djetetom sadržajno visoko seksualizirani i brzo eskaliraju) (Webster i sur., 2012, str. 14).

Uvažavajući upućenost svake države na supranacionalne akte koji proklamiraju standarde zaštite djece općenito, a potom i u ovom području, kratko izlažemo one najvažnije koje treba smatrati normativom pri kaznenopravnom uređenju.

Konvencija Ujedinjenih Naroda o pravima djeteta iz 1989. godine navodi najvažnije standarde kad je riječ o zaštiti i pravima. Obvezuje države na poduzimanje svih potrebnih mjera (od legislativnih pa do edukativnih) kako bi se djeca zaštitila od svih oblika nasilja, uključujući spolno. Kad je riječ o posljednjem, želi se spriječiti navođenje ili prisila djeteta na bavljenje bilo kojom nezakonitom spolnom djelatnošću, iskorištavanje u prostituciji te pornografskim predstavama i materijalima.

Dva su europska akta kojima je cilj sprečavanje spolnog mamljenja ili vrbovanja djece radi seksualnog kontakta (engl. *grooming*) na način da zahtijevaju njegovo inkriminiranje. Jedan dolazi iz Vijeća Europe a drugi iz Europske unije, a obje platforme zapravo već nekoliko desetljeća vode aktivnu politiku glede suzbijanja seksualnog zlostavljanja i iskorištavanja djece.

Na razini Vijeća Europe to je Konvencija o zaštiti djece od seksualnog iskorištavanja i seksualne zloupotrebe iz 2007. godine (tzv. Lanzarote konvencija). Smatra se prvim ugovorom o ljudskim pravima koji stremi da se zadiranja u seksualnost djece propišu kao kaznena djela. U konačnici pokušava se harmonizirati nacionalna zakonodavstva kako bi se izbjegla činjenica da potencijalni počinitelji odabiru zemlju u kojoj će „blaže proći". Za Republiku Hrvatsku vrijedi od 2011. sukladno Zakonu o njezinom potvrđivanju.

U čl. 23. navodi se *grooming* (*Solicitation of children for sexual purposes*, u spomenutom hrvatskom zakonu pod nazivom Vrbovanje djece u seksualne svrhe), novo djelo dotad neobrađeno u drugim međunarodnim dokumentima toga polja, kao rezultat rastuće zabrinutosti zbog seksualnog zlostavljanja djece od strane odraslih osoba koje su upoznale u virtualnom prosotoru. Članica treba poduzeti potrebne zakonske i druge mjere da kazneno procesuira namjeran prijedlog uporabom informacijsko-komunikacijskih tehnologija odrasle osobe da se sastane sa djetetom koje nije dostiglo starosnu dob (država članica treba odrediti dobnu granicu ispod koje je zabranjeno imati spolni odnošaj s djetetom), u svrhu činjenja spolnog odnošaja s djetetom ili proizvodnje dječje pornografije, kada je takav prijedlog praćen materijalnim postupanjima koja dovode do takvog susreta.

Smatra se da samo virtualno „čavrljanje" uz seksualne konotacije, iako može biti dio spolnog mamljenja ili vrbovanja djece radi seksualnog kontakta (engl. *grooming*) nije dovoljno za kaznenu odgovornost, nego je potreban dodatni element, odnosno prijedlog sastanka s djetetom uz dodatna postupanja u tom smjeru, a djelo je dovršeno

daljnjim konkretnim postupanjem kao što je, primjerice, činjenica dolaska počinitelja na mjesto sastanka. Sukladno konvencijskoj odredbi drugi su oblici spolnog mamljenja ili vrbovanja djece radi seksualnog kontakta (engl. grooming) primjerice stvarni kontakt ili onaj koji nije putem interneta, izvan dosega.

Kad je riječ o Europskoj uniji, treba izdvojiti Direktivu 2011/92/EU Europskog parlamenta i Vijeća o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije te o zamjeni Okvirne odluke vijeća 2004/68/PUP koja je donesena 17. prosinca 2011. Posebno se u čl. 6 (1) spominje mamljenje djece u seksualne svrhe kao *Solicitation of children for sexual purposes*. Odrasla osoba koja uporabom informacijsko-komunikacijske tehnologije predlaže djetetu koje još nije dosegnulo dob za pristanak na spolni odnos susret radi počinjenja kaznenog djela (spolna aktivnost s djetetom koje nije dosegnulo dob pristanka te proizvodnje dječje pornografije), a taj je prijedlog popraćen i drugim materijalnim postupanjem koje vodi prema takvom susretu, kažnjava se kaznom zatvora, ali ne manjom od godinu dana. I tu je spolno mamljenje ili vrbovanje djece radi seksualnog kontakta izvan internetskog postora (engl. *offline grooming*) izvan dosega odredbe, ali se u uvodnom dijelu priznaje važnost i njegova suzbijanja te da bi države članice svakako i ta to trebale propisati kazneno djelo.

Oba spomenuta akta (Konvencija Vijeća Europe te Direktiva Europske unije) imaju mnogo zajedničkoga: djelo nosi isti naziv, zahtijeva se namjera počinitelja, počinjeno je samo uporabom informacijsko-komunikacijske tehnologije dok su ostali oblici, spolnog mamljenja ili vrbovanja djece radi seksualnog kontakta izvan internetskog ili virtualnog prosotora (engl. *off-line grooming*) izvan dosega odredbi. Iste su zlouporabe zbog kojih se spolno mamljenje ili vrbovanje djece radi seksualnog kontakta (engl. *grooming*) vrši, a to je spolna zlouporaba i produkcija dječje pornografije. Termin informacijsko-komunikacijske tehnologije nije posebno definiran, no može se smatrati da je riječ o svim oblicima suvremene elektroničke komunikacije. Ne određuje se ni intenzitet nagovaranja ni broj ostvarenih kontakata s djetetom.

Kazneni zakon (iz 2011. godine, stupio na snagu 1. siječnja 2013.) ima novu glavu kaznenih djela (XVII) pod nazivom Kaznena djela spolnog zlostavljanja i iskorištavanja djeteta. Među njima i novo kazneno djelo u čl. 161. koje se zove Mamljenje djece za zadovoljenje spolnih potreba. Svrha je te odredbe proaktivno djelovanje mehanizma kaznenog prava u stadiju u kojem još nije došlo do izravnog i povređujućeg kontakta djeteta s počiniteljem. Time se ukazuje na novi pristup pružanja kaznenopravne zaštite posebno ranjivoj kategoriji društva i tu promjenu treba ocijeniti prikladnom. Riječ o inkriminiranju dotadašnje specifične pripremne radnje koja vodi seksualnom zlostavljanju i time omogućava kaznenopravnu reakciju prije negoli dođe do fizičkog seksualnog zlostavljanja. To djelo propisuje kaznu od šest mjeseci do

pet godina zatvora za punoljetnu osobu koja bi osobi mlađoj od petnaest godina, u namjeri da ona ili druga osoba nad njom počini spolnu zlouporabu, uporabom informacijsko-komunikacijskih tehnologija ili na drugi način predložila susret s njom ili drugom osobom i koja poduzme mjere da do tog susreta dođe.

Radi potpunije kaznenopravne zaštite predviđena je i kažnjivost pripremnih radnji (kazna zatvora do tri godine za osobu koja bi prikupljala, davala ili prenosila podatke o osobi mlađoj od petnaest godina radi počinjenja spolnog mamljenja ili vrbovanja djece u svrhu seksualnog kontakta (engl. *grooming*)). Pokušaj je djela kažnjiv sukladno odredbama općeg dijela Kaznenog zakona. Nadalje, sukladno tumačenjima, za uspostavu kažnjive zone tog djela nije dovoljan tek kontakt s djetetom, nego je potrebno da punoljetna osoba poduzme preciznije, odnosno konkretne mjere radi susreta s djetetom (Turković, i dr., 2013, str. 219), ali nije potrebno da do stvarnog kontakta i dođe. Djelo se može počiniti samo s izravnom namjerom, počinitelj je svjestan da je riječ o osobi mlađoj od petnaest godina, a dovršeno je kad počinitelj nakon mamljenja/nagovaranja djeteta kroz informacijsko-komunikacijske tehnologije poduzme bilo koju radnju da se ostvari dogovoreni susret.

Obveze iz prikazane Konvencije i Direktive uključuju inkriminiranje spolnog mamljenja ili vrbovanja djece radi seksualnog kontakta upotrebom interneta (engl. *online grooming*) što je i učinjeno u čl. 161. Kaznenog zakona. Uspoređujući tekstove, vidljivo je da je hrvatski zakonodavac otišao i korak naprijed jer nije riječ tek o ispunjavanju minimuma obveza iz Konvencije i Direktive. Naime, tekst hrvatske odredbe sadrži proširenje u dvama smjerovima jer inkriminacija obuhaća ne samo spolno mamljenje ili vrbovanje djece radi seksualnog kontakta upotrebom interneta (engl. *online grooming*), nego i izvan virtualnog svijeta (engl. *offline grooming*) te kažnjavanje i u slučaju kad počinitelj mami dijete kako bi druga osoba, različita od počinitelja nad djetetom počinila spolnu zlouporabu.

Dodatno, moguće je izricati i tzv. sigurnosne mjere, odnosno sankcije koje su namijenjene specijalnopreventivnom djelovanju i utjecaju na one čimbenike koji su doveli do počinjenja djela kako se djelo ne bi ponovilo u budućnosti. Hrvatski Kazneni zakon predviđa izricanje zabrane obavljanja određene djelatnosti ili dužnosti ako je spolno mamljenje ili vrbovanje djece radi seksualnog kontakta (engl. *grooming*) počinjen u okviru dužnosti/djelatnosti, a postoji opasnost ponavljanja. Isto tako, moguće je izreći i zabranu pristupa internetu, o čemu više govorimo u sljedećem poglavlju.

Kazneno pravo tradicionalno ima ulogu očuvanja društvene sigurnosti ostvarujući time klasičnu kaznenopravnu paradigmu gdje djeluje kao čuvar vrijednosti oko kojih se društvo složilo da su važne. Takvim inkriminacijama čini se da kazneno pravo počinje djelovati i kao dizajner društvenih vrijednosti gdje skenira društvo u pogledu

potencijalnih opasnosti kako bi pronašlo način da ih spriječi. Time se stvara ekstenzija tradicionalnih granica kaznenog prava u najširem smislu i trend predostrožnog kaznenog prava. Inkriminacija spolnog mamljenja ili vrbovanja djece radi seksualnog kontakta (engl. *grooming*) primjer je preventivne, a ne tek reaktivne legislative, s obzirom da do seksualnog zlostavljanja neće doći ukoliko počinitelj bude otkriven u tom stadiju.

7.4. DRUGA PITANJA ŠTETNIH PONAŠANJA NA INTERNETU I KAZNENOPRAVNI ODGOVORI

Nasilje (shvaćeno u najširem smislu) počinjeno upotrebom interneta svakako je u porastu poglavito s obzirom na činjenicu da internet ima značajnu ulogu u svakodnevnom životu. Napredak tehnologije uvjetuje promjene u virtualnoj komunikaciji. Takve promjene mogu biti i pozitivne i negativne. Rizici izlaganja štetnim ponašanjima na internetu predmet su i znanstvenog proučavanja gdje se među tekstovima sve više pronalazi pojmove kao što su *cybercrime*, *cyberbullying*, *cyberstalking*... i sl. Izloženost rizicima na internetu može imati dugotrajne i intenzivne negativne posljedice za svaku osobu, a poglavito za mlade koji ih često nisu ni svjesni (Vejmelka i Strabić, 2017, str. 60). Isti autori ističu kako je veća količina vremena provedena u određenim aktivnostima na internetu povezana s češćim sudjelovanjem u elektroničkom nasilju te su rezultati njihova recentnog istraživanja pokazali visoku prevalenciju ovisnosti o internetu (36,2 %) i elektroničkoga nasilja (50,7 %) na slučajno izabranom uzorku učenika devet srednjih škola u Hrvatskoj (Vejmelka i Strabić, 2017, str. 73).

Kazneno pravo nastoji razvijati prikladne odgovore na virtualne modalitete specifičnim opisima kaznenih djela i predviđanjem odgovarajućeg sustava kaznenopravnih sankcija. Utoliko, među tzv. sigurnosnim mjerama postoji i zabrana pristupa internetu koju sud može izreći počinitelju. Riječ je o apsolutnoj odnosno potpunoj zabrani pristupa internetskim sadržajima kao i onemogućavanju izražavanja vlastitih stajališta u virtualnom svijetu dok je izrečena mjera na snazi. Sigurnosne mjere specifična su vrsta kaznenopravne sankcije. Njima se nastoji specijalno preventivno djelovati na počinitelja kako ne bi ponovno počinio kazneno djelo, odnosno nastoji se sprječavati recidivizam. Sukladno trenutnim postavkama Kaznenog zakona sigurnosnu mjeru zabrane pristupa internetu sud će izreći počinitelju koji je kazneno djelo počinio upotrebom interneta ako postoji opasnost da će zlouporabom interneta ponovno počiniti kazneno djelo. Može se izreći u trajanju od šest mjeseci do dvije godine. Ako počinitelju nije izrečena uvjetna osuda ni rad za opće dobro, nego je

osuđen na kaznu zatvora, zabrana pristupa internetu izriče se u trajanju duljem od kazne zatvora, i to od šest mjeseci do dvije godine dulje.

Ta se mjera može i ranije obustaviti, no tek ukoliko je protekla polovina inicijalno izrečenog trajanja, a sud utvrdi da više ne postoji opasnost na strani osuđenika. Kad je izrečena mjera postala pravomoćna, sud mora obavijestiti regulatorno tijelo nadležno za elektroničke komunikacije koje će osigurati njezino provođenje. Riječ je o HAKOM-u, odnosno Hrvatskoj regulatornoj agenciji za mrežne djelatnosti. Dakle, po zaprimanju obavijesti nadležnog suda o pravomoćno izrečenoj mjeri HAKOM treba obavijestiti operatore koji pružaju usluge pristupa internetu da u određenom razdoblju ne smiju sklopiti ugovor o korištenju usluga pristupa internetu odnosno, ako s počiniteljem već imaju zasnovan pretplatnički odnos, da mu moraju obustaviti pružanje usluga u razdoblju koje je određeno mjerom. Međutim, provođenje te mjere u praksi obiluje brojnim izazovima uz značajnu mogućnost izigravanja. Utoliko i mnogi autori ističu da apsolutna zabrana pristupa internetu nije odgovarajuće rješenje jer nema rehabilitativnog potencijala (Cvitanović i Glavić, 2012, str. 914). Ministarstvo je unutarnjih poslova 2013. godine donijelo Pravilnik o izvršavanju sigurnosne mjere zabrane pristupa internetu sa svrhom propisati način na koji HAKOM provodi spomenutu mjeru te obveze operatora elektroničkih komunikacijskih usluga koje pružaju pristup internetu. Potonji treba raskinuti pretplatnički ugovor ako postoji odnosno obustaviti uslugu pružanja pristupa internetu. Mjera zabrane pristupa internetu može se izreći i neubrojivoj osobi.

U nastavku teksta potrebno je nešto reći o kaznenim djelima koje se odnose na internet, računala i računalne podatke koji su trenutno dio teksta Kaznenog zakona. Kad je riječ o kaznenopravnom poimanju računala i računalnog sustava, sukladno čl. 87. st. 18–20, računalni sustav svaka je naprava ili skupina međusobno spojenih ili povezanih naprava od kojih jedna ili više njih na osnovi programa automatski obrađuju podatke kao i računalni podaci koji su u njega spremljeni, obrađeni, učitani ili preneseni za svrhe njegovog rada, korištenja, zaštite i održavanja. Računalni podatak svako je iskazivanje činjenica, informacija ili zamisli u obliku prikladnom za obradu u računalnom sustavu. Računalni program skup je računalnih podataka koji su u stanju prouzročiti da računalni sustav izvrši određenu funkciju.

Treba reći da Kazneni zakon ima cijelu glavu posvećenu kaznenim djelima protiv računalnih sustava, programa i podataka (čl. 266–273). Ovdje se nalaze sljedeća kaznena djela Neovlašteni pristup, Ometanje rada računalnog sustava, Oštećenje računalnih podataka, Neovlašteno presretanje računalnih podataka, Računalno krivotvorenje, Računalna prijevara, Zlouporaba naprava te Teška kaznena djela protiv računalnih sustava, programa i podataka.

Računalni sustav se, uz već prethodno spomenuta kaznena djela, spominje i kod kaznenog djela terorizma (čl. 97. st. 9), potom kao modalitet kod kaznenih djela protiv časti i ugleda i to u kvalificiranom obliku (uvreda, čl. 147. st. 2., teško sramoćenje čl. 148. st. 2 i kleveta, čl. 149. st. 2.). Potom kod kaznenih djela Iskorištavanja djece za pornografiju, čl. 163. st. 4. kroz oduzimanje tzv. *instrumenta sceleris*, kao i kod Iskorištavanja djece za pornografske predstave, čl. 164. st. 5. te kod Upoznavanja djece s pornografijom, i kao modalitet u čl. 165. st. 1. Povreda privatnosti djeteta može se počiniti računalnim sustavom sukladno čl. 178. st. 2., kao i Izrada, nabavljanje, posjedovanje, prodaja ili davanje na uporabu sredstava za krivotvorenje, prema čl. 283. Time virtualni ili računalni modalitet počinjenja djela nije taksativan. Naime, i neka druga kaznena djela moguće je počiniti na taj način ali, njihov opis ne podrazumijeva eksplicitno internet, računalni sustav ili mrežu. Naime, opis sadrži generalnu klauzulu „ili na drugi način", što implicira da se ovdje predmetni modalitet može pojaviti u praksi pa će ga prilikom procesuiranja trebati, primjenom dopuštene analogije unutar zakona, podvoditi pod zakonski opis kaznenog djela.

Od specifičnih kaznenih djela koja u svom opisu spominju internet možemo izdvojiti Krivotvorenje lijekova ili medicinskih proizvoda (čl. 185.) i to u kvalificiranom (težem) obliku gdje zakon prijeti kaznom zatvora od jedne do osam godina onome tko bi počinio djelo sredstavima pogodnim za masovnu distribuciju kao što su informacijski sustavi uključujući i internet. Potom, kazneno djelo Zlouporaba tržišta kapitala (čl. 260.) moguće je počiniti na način da počinitelj širi informacije uporabom medija, interneta ili bilo kojim drugim načinom ili sredstvom kojim daje ili bi mogao davati neistinite ili obmanjujuće znakove, za što je previđena kazna od šest mjeseci do pet godina.

7.5. ZAKLJUČNE MISLI

Izazovi virtualne komunikacije nedvojbeno su i izazovi postavljeni pred kazneno pravo s obzirom da zadaća koju ono općenito nastoji ostvariti vrijedi kako za stvarni, tako i za virtualni svijet. To znači da se neprihvatljiva, društveno štetna i ugrožavajuća ponašanja i u tom modalitetu nastoje suzbijati kaznenopravnim mehanizmom – inkriminacijom specifičnih ponašanja, propisivanjem primjerene sankcije, provođenjem kaznenog postupka te osudom i izvršenjem izrečene sankcije. Virtualni modaliteti kaznenih djela izraženo naglašavaju obilježja i potrebu prilagodljivog pravnog sustava te brze i primjerene reakcije. Osobito je istaknut značajan utjecaj različitih europskih akata u kaznenom pravu na području elektroničkog kriminaliteta. U tom smislu, s osvrtom na predstavljene dvije kaznene inkriminacije (govor mržnje te

mamljenje djece za zadovoljenje seksualnih potreba), možemo reći da hrvatske odredbe idu u korak s vremenom te u značajnoj mjeri implementiraju spomenute europske proklamacije i preuzete obveze. Međutim, legislativna razina tek je početak prema ostvarenju cilja pune zaštite mogućih žrtava. Pravi je izazov oživotvorenje odredbi u praksi svih nadležnih tijela kaznenog postupka (sudova, policije, državnog odvjetništva) jer se njihove radnje slažu u cjelinu poput kaznenopravnog mozaika. Preduvjet za cjelovitu i uspješnu primjenu svakako je razvijanje primjerene sudske prakse koja podrazumijeva učinkovito postupanje svih spomenutih tijela. U tom je smislu od velikog značenja jačanje njihovih kapaciteta u prvom redu edukacijom i primjerima dobre prakse.

7.6. LITERATURA

Alaburić, V. (2003). Ograničavanje ″govora mržnje″ u demokratskom društvu-teorijski, zakonodavni i praktični aspekti, I. i II. dio. *Hrvatska pravna revija*: *časopis za promicanje pravne teorije i prakse, 3*(1), 62-72.

Alaburić, V. (2003). Ograničavanje ″govora mržnje″ u demokratskom društvu-teorijski, zakonodavni i praktični aspekti, I. i II. dio. *Hrvatska pravna revija*: *časopis za promicanje pravne teorije i prakse, 3*(2), 80-90.

Code of Conduct on countering illegal hate speech online, Fourth evaluation confirms self-regulation works. (veljača 2019). Preuzeto s https://ec.europa.eu/info/sites/info/files/code_of_conduct_factsheet_7_web.pdf, 10. 4. 2019.

Communication on Tackling Illegal Content Online - Towards an enhanced responsibility of online platforms. (28. rujan 2017.). Preuzeto s https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms, 10.4.2019.

Countering illegal hate speech online #NoPlace4Hate. (18. ožujak 2019). Preuzeto s https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300, 10.4. 2019.

Cvitanović, L. i Glavić, I. (2012). Uz problematiku sigurnosne mjere zabrane pristupa internetu. *Hrvatski ljetopis za kazneno pravo i praksu, 19*(2), 891-916.

Direktiva 2011/92/EU Europskog parlamenta i Vijeća o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije te o zamjeni Okvirne odluke vijeća 2004/68/PUP. (17. 12 2011). *(OJ L 335). Službeni list Europske unije.*

Handyside v. United Kingdom, App. no. 5493/72 (European Court of Human Rights 7. December 1976).

Herceg Pakšić, B. (2017). Tvorba novih standarda u slučajevima teških oblika govora mržnje: negiranje genocida pred Europskim sudom za ljudska prava. *Zbornik Pravnog fakulteta u Zagrebu, 67*(2), 229-253.

Herceg Pakšić, B. i Lachner, V. (2015). Hate Speech as a Violation of Human Rights: the Meaning, Implications and Regulation in Criminal Law. U: M. Vinković (Ur.), *New Developments in EU Labour, Equality and Human Rights Law* (str. 295-320). Osijek: Faculty of Law, Osijek.

Horvatić, Ž., Derenčinović, D. i Cvitanović, L. (2016.). *Kazneno pravo, opći dio I. Kazneno pravo i kazneni zakon.* Zagreb: Pravni fakultet Sveučilišta u Zagrebu.

Kazneni zakon. *Narodne novine* 125/2011, 144/2012, 56/2015, 61/2015, 101/2017, 118/2018.

Konvencija Ujedinjenih naroda o pravima djeteta. (1989). Narodne novine-Međunarodni ugovori 12/93.

Kool, R. (2011). Prevention by All Means?A Legal Comparison of the Criminalization of Online Grooming and its Enforcement. *Utrecht Law Review, 7*(3), 46-69. doi.org/10.18352/ulr.171

Lobba, P. (2015). Holocaust Denial before the European Court of Human Rights: Evolution of an Exeptional Regime. *The European Journal of International Law, 26*(1), 237-253. doi.org/10.1093/ejil/chv003

Munivrana Vajda, M. i Šurina Marton, A. (2016). Gdje prestaju granice slobode izražavanja, a počinje govor mržnje? Analiza hrvatskog zakonodavstva i prakse u svjetlu europskih standarda. *Hrvatski ljetopis za kaznene znanosti i praksu, 23*(2), 435-467.

Muntarbhorn, V. (2007). *A Commentary on the United Nations Convention on the Rights of a Child, Article 34 Sexual Exploitation and Sexual Abuse of Children*. Leiden*Boston: Martinus Nijhoff Publisher.

O'Connell, R. (2003). A Typology of Cybersexploitation and On-line Grooming. Preston, Cyberspace Research Unit, University of Central Lancashire. Preuzeto s http://www.jisc.ac.uk/uploaded_documents/lis_PaperJPrice.pdf, 11.4.2019.

Okvirna odluka vijeća 2008/913/PUP od 28. studenoga 2008. o suzbijanju određenih oblika i načina izražavanja rasizma i ksenofobije kaznenopravnim sredstvima. (06. prosinca 2008). *Službeni list Europske unije L 328/55.*

Pravilnik o izvršavanju sigurnosne mjere zabrane pristupa internetu. *Narodne novine* 34/2013.

Preporuka Komisije za učinkovito suzbijanje nezakonitog sadržaja na internetu. (01. ožujak 2018). Bruxelles. Preuzeto 10. travanj 2019. iz http://europa.eu/rapid/press-release_MEMO-18-1170_hr.htm

Preporuka Ministarskog odbora Vijeća Europe No. R (97) 20. (30. listopad 1997).

Roksandić Vidlička, S. i Mamić, K. (2018). Zlouporaba društvenih mreža u javnom poticanju na nasilje i mržnju i širenju lažnih vijesti: potreba transplantiranja njemačkog Zakona o jačanju provedbe zakona na društvenim mrežama. *Hrvatski ljetopis za kaznene znanosti i praksu , 25*(2), 329-357.

Simpson, R. M. (2013). Dignity, Harm and Hate Speech. *Law and Philosophy, 2*, 701-728. doi.org/10.1007/s10982-012-9164-z

Škrtić, D. (2013). Mamljenje djeteta za zadovoljenje spolnih potreba uporabom informacijsko-komunikacijske tehnologije. *Zbornik Pravnog fakulteta Sveučilišta u Rijeci, 34*(2), 1139-1170.

Turković, K., Novoselec, P., Grozdanić, V., Kurtović Mišić, A., Derenčinović, D., Bojanić, I., … Maršavelski, A. (2013). *Komentar Kaznenog zakona i drugi izvori novog hrvatskog kaznenog zakonodavstva.* Zagreb: Narodne novine.

Ustav Republike Hrvatske. *Narodne novine* 56/1990, 135/1997, 113/2000, 28/2001, 76/2010, 5/2014.

Vejmelka, L. i Strabić, N. (2017). Online aktivnosti i rizična ponašanja adolescenata u virtualnom okruženju. *Društvena istraživanja, 26*(1), 59-78. doi.org/10.5559/di.26.1.04

Webster, S., Davidson, J., Bifulco, A., Gottschalk, P. C., Grove-Hills, J. T., Schimmenti, A., Craparo, G. (2012). *European Grooming Project Online_*. Prepared for and co-funded by the European Commission Safer Internet Plus Programme. Preuzeto s https://

childhub.org/en/child-protection-online-library/european-online-grooming-project-final-report, 11.4.2019.

Zakon o elektroničkim medijima. *Narodne novine* 153/2009, 84/2011, 94/2013, 136/2013.

Zakon o potvrđivanju Konvencije Vijeća Europe o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja. *Narodne novine, Međunarodni ugovori* 11/2011.

izv. prof. dr. sc. Goran Vojković
Fakultet prometnih znanosti Sveučilišta u Zagrebu

8. OPĆA UREDBA O ZAŠTITI OSOBNIH PODATAKA

Sažetak

Opća Uredba o zaštiti osobnih podataka, GDPR stupila je na snagu 25. svibnja 2018. godine i izravno se primjenjuje na sve članice Europske unije. Ona je na jedinstven način uredila pitanja zaštite osobnih podataka koja su do tada bila regulirana okvirno međunarodnim konvencijama te propisima svake države članice.

Razvoj međunarodne, prekogranične trgovine, zajedno s razvojem mobilnih komunikacija tražio je da se pitanja zaštite osobnih podataka reguliraju jedinstveno za cijelu EU, i to je učinjeno Općom uredbom. Dodatno, pitanja zaštite osobnih podataka danas postaju sve važnija. Podaci u elektroničkom obliku lako se prikupljaju, lako prenose i lako obrađuju suvremenim računalima. Prosječan pametni telefon o svom korisniku daje više podataka (kretanje, navike boravka, kupovne navike) nego što je nekada mogla prikupiti prosječna tajna služba.

U kakofoniji raznih javnih medija (stotine radijskih stanica i portala, desetine televizijskih programa), uz društvene mreže – sve je teže doprijeti do pojedinačnog kupca, znatno teže nego u doba kada je postojalo dva ili tri TV programi te lokalni i nacionalni radio i tiskane novine. Stoga ciljano reklamiranje koje se temelji na prikupljanju osobnih podataka i preferencija određenog pojedinca postaje sve važnije. No, gdje je granica ulaska u nečiju intimu? Gdje dozvoljena marketinška akcija postaje praćenje pojedinca? Što je s hrpom podataka koje danas ostavljamo na svakom mjestu?

Razmjena je podataka potrebna. Danas redovito kupujemo iz drugih europskih država, potrebno je znati i osobne podatke za dostavu i osobne podatke u slučaju

reklamacije. Mnoge su usluge i povezane s otkrivanjem nekih osobnih podataka, primjerice kada nam e-knjižare nude nove knjige iz spektra koji redovno čitamo. No, treba li podatke o dostavi čuvati i nakon što je roba dostavljena pa i jamstvo isteklo? Smije li e-knjižara prodavati drugima informacije volimo li Sherlocka Holmesa ili ruske klasike? Osobni podaci u današnjem svijetu postaju roba koja ima svoju cijenu. I upravo zato ih je potrebno nadzirati. Čim postoji kupac, javiti će se netko tko prodaje robu, u ovom slučaju vaše podatke. Danas tehnički lakše nego ikada.

Možete smatrati da su podaci o vama bezazleni, pa što ako jedna knjižara proda drugoj što volite, samo ćete dobiti usmjerenu reklamu. No, što ako netko napravi cijeli vaš profil, ukrade identitet i podigne kredit u vaše ime, jer bilo je i takvih slučajeva? Ili napravi lažnu putovnicu s vašim podacima pa vas kod idućeg prelaska granice uhite dok se situacija ne razjasni, a to može trajati? Što ako netko nesavjesno proda podatke vašeg suvremenog brojila za struju pa kriminalci saznaju kada niste kod kuće jer brojilo uredno mjeri i potrošnju po satu? Što ako netko (bilo je takvih slučajeva u praksi!) otvori blog s vašom fotografijom i podacima te počne objavljivati rasističke i slične poruke pa zbog toga imate neugodnosti na poslu?

Zloporaba osobnih podataka može biti vrlo ozbiljna, posebno u današnjem informatiziranom društvu. Pravni model zašite privatnosti i osobnih podataka razvija se već nekoliko desetaka godina, a krajnji je rezultat Opća uredba koju ovdje analiziramo, nakon što navedemo i druge, starije dokumente o zaštiti privatnosti i osobnih podataka.

Iako se u ovo informatizirano doba osobni podaci razmjenjuju i obrađuju više nego ikada, ne treba zaboraviti da se o vašim podacima treba pitati vas i da imate pravo tražiti informacije što, kako i koliko dugo se obrađuju vaši osobni podaci. Opća uredba sigurno nije u tome idealan pravni instrument, može se i njoj naći manjkavosti, ali je najbolji pravni instrument koji kao građani Europske unije imamo.

Ovo poglavlje služi upoznavanju s dosadašnjim propisima o zaštiti osobnih podataka te Općom uredbom, ali i potrebi povećanja svijesti o osobnim podacima – ako na Facebooku javno stavite baš sve o sebi, ni jedan pravni akt neće moći zaštiti vaše podatke.

8.1. PRIVATNOST KAO DOSTIGNUĆE SUVREMENOG ČOVJEKA

8.1.1. POČECI SHVAĆANJA PRIVATNOSTI

Koliko god nama danas neobično izgledalo, privatnost kako je danas poznajemo želja je i potreba suvremenog čovjeka povezana s nastankom prvih demokratskih režima (sloboda dopisivanja) ali i građanskog načina života. U povijesti ćemo naći neke početke prava na privatnost. Tako se, primjerice, već oko 200. godine u Zborniku židovskih zakona – Mishni – štiti osoba od tuđeg zavirivanja u njegovu kuću (Brezak, 1998), no sustavno bavljenje privatnošću i pravu na privatnost bitno je novijeg datuma.

Kako bismo ilustrirali drugačiji odnos prema privatnosti u prošlosti, nevedimo nekoliko primjera. U mnogim dijelovima Europe i Male Azije sačuvani su rimski javni zahodi – često luksuzno uređene prostorije u kojima bi korisnici zajednički sjedili, bez ikakvih pregrada, a vjerojatno su i boravak u zahodu koristili za razgovore.

Kasnije, u srednjevjekovno doba, većina je stanovništva živjela u vrlo skromnim uvjetima. Tipična kuća imala je svega jednu ili dvije prostorije u kojima je živjela cijela obitelj i često jedan jedini krevet za sve – kreveti su bili skupi – a zajedničko je spavanje i omogućavalo održavanje topline. Odvojeno spavanje članova obitelji pojavilo se tek kasnije kada je rast standarda omogućio veće objekte. Plemstvo je živjelo nešto luksuznije, ali „logistika" jednog dvorca u kojemu je trebalo sve ručno raditi, od tople vode za jutarnje umivanje pa nadalje, uništavala je praktično svaki trag ikakve privatnosti.

Čak ni Ustav Sjedinjenih Američkih Država, napisan 1787. godine, dokument koji je predstavljao doslovno svjetionik slobode i demokracije te služio i služi kao uzor gotovo svim demokratskim ustavima sve do danas, ne govori o, primjerice, pravu na tajnost dopisivanja, jednog od temeljnih prava unutar skupa prava privatnosti. Ono je u Sjedinjenim Američkim Državama proklamirano tek tumačenjem Četvrtog amandmana na Ustav SAD-a od strane Vrhovnog suda 1877. godine. Tek tada je u pravni sustav SAD-a, dakle države koja je imala najnapredniji ustavni model u smislu zaštite pojedinca uvedeno danas svima razumljivo i temeljno pravo – pravo na tajnost dopisivanja.

8.1.2. OPĆA DEKLARACIJA O LJUDSKIM PRAVIMA

Užasni zločini počinjeni u Drugom svjetskom ratu bili su povod donošenju *Opće deklaracije o ljudskim pravima*, kako je navedeno u samoj Preambuli Deklaracije riječima: „budući da je nepoštivanje i zanemarivanje ljudskih prava rezultiralo barbarskim postupcima koji vrijeđaju savjest čovječanstva i da je izgradnja svijeta u kojemu

će ljudska bića uživati slobodu govora i uvjerenja te biti slobodna od straha i neimaštine, proglašena najvećom težnjom svih ljudi (…)"

Članak 12. Opće deklaracije izričito navodi:

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.

U navedenoj odredbi po prvi se puta na globalnoj razini uređuje pitanje prava na privatnost fizičke osobe. Naravno, od općeg dokumenta Ujedinjenih naroda preko normizacije na nacionalnoj razini do konkretne primjene u praksi država dug je put – posebno za vrijeme Hladnog rata svjedočili smo vrlo grubim nasrtajima na privatnost i osobni život pojedinca u nekadašnjim socijalističkim državama gdje se radi govora išlo na robiju, ali čak i države zapadne demokracije nisu bile imune od uplitanja u privatan život i stavove svojih građana.

8.1.3. POVELJA EUROPSKE UNIJE O TEMELJNIM PRAVIMA

Pitanje privatnosti u smislu zaštite osobnih podataka izričito se nalazi u jednom novijem dokumentu – *Povelji Europske unije o temeljnim pravima* iz 2000. godine koja je u punoj primjeni od stupanja na snagu Lisabonskog ugovora 1. prosinca 2009. godine. Navedena Povelja obvezuje institucije, tijela, urede i agencije Unije te države članice samo kada provode pravo Unije. Za našu temu značajna su dva članka, članak 7. koji navodi:

Svatko ima pravo na poštovanje svojeg privatnog i obiteljskog života, doma i komuniciranja.

Te članak 8. koji i nosi naslov *Zaštita osobnih podataka*, a glasi:

1. Svatko ima pravo na zaštitu osobnih podataka koji se na njega ili nju odnose.

2. Takvi podaci moraju se obrađivati pošteno, u utvrđene svrhe i na temelju suglasnosti osobe o kojoj je riječ, ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom. Svatko ima pravo na pristup prikupljenim podacima koji se na njega ili nju odnose i pravo na njihovo ispravljanje.

3. Poštovanje tih pravila podliježe nadzoru neovisnog tijela.

Tom se odredbom na razini Europske unije pitanje zaštite osobnih podataka podiže na razinu temeljnih ljudskih prava. Naime, kao i sve drugo i pravni okvir ljudskih prava razvija se i mijenja, neka prava koja nisu bila ni spomenuta prije 70 godina, kao što je pitanje osobnih podataka, danas se smatraju gotovo samorazumljivim i teško bi bilo zamisliti demokratski uređenu državu koja ih ne štiti. Što se tiče

razloga zaštite, oni su se pojavili razvojem filozofske i pravne misli, ali i radi prekomjernog tehničkog razvoja koji je obradu osobnih podataka učinio lakom, brzom i pristupačnom svakome.

Upravo to što smo naveli, lako, brzo i pristupačno, predstavlja veliku opasnost za privatnost.

8.2. RAZVOJ RAČUNALA I ZAŠTITA OSOBNIH PODATAKA

Vratimo se za trenutak u šezdesete godine prošlog stoljeća. Osobna računala na koja smo naviknuli ne postoje. Digitalnu revoluciju koja će se pokrenuti za svega nekoliko godina ne predviđaju čak ni pisci znanstvene fantastike. Računalo je nešto veliko, za što trebaju ogromne prostorije i školovani stručnjaci. Mogu ih priuštiti samo države, najveće tvrtke i bogate znanstvene ustanove. Računala međusobno nisu umrežena. Ukoliko netko obrađuje osobne podatke, to je sama država koja to radi za sebe, uz relativno teško sakupljanje podataka na terenu.

Kraj sedamdesetih godina donosi nam osobno računalo. Stroj koji može kupiti svatko s prosječnom plaćom u razvijenoj zemlji. Takva računala mogu obrađivati velik broj podataka, a koji se opet mogu raspačavati i prikupljati uporabom malih i praktičnih diskova. Kartično plaćanje postaje sve učestalije. Računala se povezuju modemima čime je omogućen i praktično trenutni prijenos podataka. Time je omogućeno da složene analize, koje su do tada mogle raditi samo državne institucije, njihove tajne službe ili razvijena sveučilišta, može obavljati praktično bilo tko kod kuće. Povezivanje nečijeg identiteta s, primjerice, podacima kartičnog plaćanja omogućava vrlo detaljan uvid u osobni život pojedinca, što se naravno može iskoristiti u različite nedozvoljene svrhe, primjerice ucjenu.

Eksponencijalni razvoj brzine osobnih računala, a odnedavno i razvoj interneta stvari (engl. *Internet of Things, IoT*) bitno su olakšali praćenje i obradu osobnih podataka pojedinca te ulaženje u njegovu privatnu, pa čak i vrlo intimnu sferu. Mobilni uređaj (danas ih samo tradicijski zovemo „mobilni telefon“ jer ponajmanje služe telefoniranju) prati naše kretanje 24 sata dnevno, često s preciznošću od samo nekoliko metara. Suvremeno brojilo struje mjeri i snagu potrošnje – dakle očitanjem tih podataka može se s velikom sigurnošću predvidjeti kada je netko kod kuće, a kada je nije. Također, mogu se uz malo znanja o tipičnoj potrošnji pojedinih uređaja detektirati nečije prehrambene ili higijenske navike, pa i to je li sam u stanu ili je nekog dana bilo prisutno više osoba. Takvi vrlo intimni podaci mogu doći u posjed i nedobronamjernih osoba.

Razni virtualni asistenti, kakav je primjerice Amazon Echo, temelje se na praćenju onoga što govorimo i pitamo – te mogu biti izvor svakakvih zloporaba. Tehnički, aktiviraju se na kodnu riječ, tipa „Alexa" ili „Computer", no da bi radili, moraju biti stalno uključeni. Mogućnost zloporabe kod takvih uređaja jako je velika, ne samo od davatelja usluge već i od treće strane, zlonamjernih osoba koje mogu preuzeti kontrolu nad takvim virtualnim asistentom i početi aktivno pratiti sve što se u prostoriji govori.

Trenutno najbrži Intelov procesor za osobna računala, Intel Core i9, može se nabaviti za cijenu koja je niža od prosječne plaće u Hrvatskoj. Dakle, cjelokupno računalo koje je u razini superračunala od prije 10–15 godina može se nabaviti za nekih 15.000 kuna i dovoljne je snage da u nekoliko sekundi obradi hrpu podataka o svim građanima Hrvatske! Nešto što je donedavno bilo monopol bogatih država, njihovih obavještajnih službi i agencija koje se bave istraživanjem svemira, postalo je dostupno gotovo svakome.

Mogućnost da netko prikuplja i obrađuje osobne podatke građana danas je tehnički vrlo jednostavna. Bez odgovarajućeg sustava zaštite razvilo bi se potpuno neregulirano tržište osobnih podataka u kojemu bi privatnost praktično svake osobe bila iznimno ugrožena. Stoga je razvoj tehnologije nalagao i razvoj pravnog okvira zaštite osobnih podataka.

8.3. RAZVOJ PRAVNOG OKVIRA ZAŠTITE OSOBNIH PODATAKA

Međunarodne konvencije i načela koja smo spomenuli općenito reguliraju pitanja privatnosti i zaštite osobnih podataka. Ta je načela trebalo konkretizirati gdje se prvo angažirala najstarija europska organizacija – Vijeće Europe,[1] da bi kasnije zaštita osobnih podataka postala i važnim dijelom pravne stečevine Europske unije i stoga obveza za sve njezine članice.

8.3.1. KONVENCIJA 108 VIJEĆA EUROPE

Vijeće Europe 1981. godine donijelo je Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka (poznata i kao Konvencija 108, po rednom broju donošenja), a 2001. godine donijet je i Dodatni protokol uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u svezi nadzornih tijela i

[1] Vijeće Europe nema izravne veze s Europskom unijom i posebna je međunarodna organizacija utemeljena 1949. godine.

međunarodne razmjene podataka. Republika Hrvatska ratificirala je i Konvenciju 108 i Dodatni protokol 2005. godine. Time je sukladno čl. 134. Ustava Republike Hrvatske Konvencija 108 i Dodatni protokol postao dio unutarnjeg prava Republike Hrvatske i po pravnoj snazi iznad zakona.

Iako je od donošenja Konvencije 108 prošlo gotovo 40 godina, taj dokument ostaje međunarodni okvir zaštite osobnih podataka, čak i izvan kruga članica Vijeća Europe, primjerice ratificirala ju je Argentina, Meksiko, Tunis, Urugvaj i još nekoliko država izvan Europe (Popis potpisa i ratifikacija Konvencije 108, 2019).

Svrha Konvencije 108 navedena je u čl. 1. Konvencije: „Svrha je ove Konvencije svakoj fizičkoj osobi, bez obzira na njezino državljanstvo i boravište, na području svake stranke, osigurati poštovanje njezinih prava i temeljnih sloboda, a osobito njezino pravo na privatnost glede automatizirane obrade osobnih podataka koji se na nju odnose ('zaštita podataka')."

Konvencijom su definirani temeljni pojmovi zaštite osobnih podataka koji su oz određene promjene aktualni i danas, primjerice prema čl. 2. Konvencije:

a. „osobni podatak" znači svaku obavijest koja se odnosi na određenog ili odredivog pojedinca („subjekt podatka")
b. „automatizirana zbirka podataka" znači svaki skup podataka koji je predmet automatizirane obrade
c. „automatizirana obrada" obuhvaća sljedeće operacije, izvršene u cijelosti ili djelomično automatiziranim postupkom: pohrana podataka, primjena logičkih i/ili aritmetičkih operacija na te podatke, njihovu promjenu, brisanje, ponovni unos ili širenje
d. „voditelj zbirke podataka" znači fizičku ili pravnu osobu, javnu vlast, službu ili svako drugo tijelo koje je prema unutarnjem pravu nadležno za odlučivanje o svrsi automatizirane zbirke podataka, o kategorijama osobnih podataka koje treba pohraniti i o operacijama koje na njih treba primijeniti.

Konvencija 108 navodi i danas aktualna svojstva osobnih podataka, prema čl. 5. osobni podaci koji su predmet automatizirane obrade trebaju biti:

- pribavljeni i obrađeni u dobroj vjeri i zakonito
- pohranjeni u određene i zakonite svrhe i ne smiju biti uporabljeni na način koji je nespojiv s tim svrhama
- odgovarajući, mjerodavni i ne suvišni u odnosu na svrhe u koje su pohranjeni
- točni i, ako je to potrebno, ažurirani

- sačuvani u obliku koji omogućuje identifikaciju subjekata podataka tijekom razdoblja koje nije duže nego što nalaže svrha u koju su pohranjeni.

Nadalje, Konvencija 108 uvodi i takozvane „posebne kategorije podataka", čl. 6., „Osobni podaci koji otkrivaju rasno podrijetlo, politička mišljenja, vjerska ili druga uvjerenja, kao i osobni podaci koji se tiču zdravlja ili spolnog života, ne mogu se automatizirano obrađivati ako unutarnje pravo ne predviđa primjerenu zaštitu. Isto se primjenjuje na osobne podatke koji se odnose na kaznene presude."

Konvencija uvodi i obvezu čuvanja osobnih podataka, što čak i neki kasniji propisi nisu dovoljno precizno uređivali, dakle propisuje se (čl. 7.) kako za zaštitu osobnih podataka pohranjenih u automatiziranim zbirkama podataka treba poduzeti prikladne sigurnosne mjere protiv slučajnog ili neovlaštenog uništenja ili slučajnog gubitka, kao i protiv neovlaštenog pristupa, preinake ili širenja.

Dodatnim protokolom iz 2001. godine navedeno je kako će svaka država potpisnica osigurati nadležno tijelo za osiguranje sukladnosti s mjerama Konvencije 108 i Dodatnog protokola u njezinom unutarnjem pravu.

Također, detaljnije je definiran i prekogranični prijenos podataka. Čl. 2. Dodatnog protokola navodi se kako će svaka stranka (dakle država potpisnica) omogućit će prijenos osobnih podataka do primatelja koji je pod jurisdikcijom države ili organizacije koja nije stranka Konvencije samo ako spomenuta država ili organizacija osigurava odgovarajuću razinu zaštite za prijenos podataka o kojem je riječ.

Sve države Europske unije ratificirale su Konvenciju 108, a većina članica i Dodatni protokol, stoga je Konvencija 108 još uvijek važan međunarodni ugovor koji regulira pitanje zaštite osobnih podataka.

8.3.2. RAZVOJ PRAVNOG OKVIRA EUROPSKE UNIJE

Europska unija područje je zaštite osobnih podataka regulirala 1995. godine *Direktivom 95/46/EZ o zaštiti pojedinaca u pogledu obrade osobnih podataka i slobodnog kolanja takvih podataka* (Opća Direktiva o zaštiti osobnih podataka).

Kako je u pitanju direktiva, dakle akt koji se izravno ne primjenjuje u državama članicama, svaka članica Europske unije njezine je odredbe trebala unijeti u nacionalno zakonodavstvo. Hrvatska je to, kako ćemo vidjeti, napravila tek 2003. godine.

Donesena je 2002. godine i posebna Direktiva koja se bavila zaštitom osobnih podataka u području mobilne telefonije i općenito elektroničkih komunikacija: *Direktiva 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija*, a kako su se odredbe gore navedenih direktiva odnosile na članice, ali

ne i na samu Uniju, donesena je Uredba br. 45/2001 Europskog parlamenta i Vijeća o zaštiti osoba pri obradi osobnih podataka u institucijama i tijelima Zajednice te o slobodnome protoku takvih podataka koja obvezuje tijela i službenike same EU.

Uvedeno je i posebno tijelo za zaštitu osobnih podataka unutar EU. „Europski nadzornik zaštite osobnih podataka (engl. *European Data Protection Supervisor*) uspostavljen je već spomenutom Uredbom br. 45/2001, koja se primjenjuje u vezi s obradom osobnih podataka u tijelima i institucijama EU-a. On je odgovoran za praćenje i osiguravanje primjene Uredbe kao i drugih akata EU-a koji se odnose na zaštitu temeljnih prava i sloboda fizičkih osoba u vezi s obradom osobnih podataka od strane institucija ili tijela EU-a (Dragičević, 2015)".

Jačanje Europske unije, ali i briga za zaštitu osobnih podataka građana tražilo je daljnje usavršavanje pravnog okvira. Početkom 2012. godine Europska je komisija u skladu s novom pravnom osnovom za uređenje zaštite osobnih podataka (čl. 16. st. 2. podstavak 1. Ugovora o funkcioniranju Europske unije, UFEU) podnijela prijedlog Uredbe o općoj zaštiti osobnih podataka koja bi zamijenila Direktivu iz 1995. godine (Dragičević, 2015). Uredba (engl. *regulation*) u pravu EU-a znači akt koji obvezno i u cjelini vrijedi za sve članice – čime se izbjegavaju i manja odstupanja među državama članicama koja mogu nastati primjenom direktive koje obvezuju države članice po ciljevima, ali ne i po formi.

Zbog osjetljivosti materije donošenje nove uredbe odužilo se tako da je *Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)*, poznata po svojoj engleskoj kratici GDPR (u ovom tekstu ćemo koristiti skraćeni hrvatski naziv: Opća uredba), donijeta 4. travnja 2016. godine, a njezina je primjena započela 25. svibnja 2018. godine.

8.3.3. RAZVOJ PRAVNOG OKVIRA REPUBLIKE HRVATSKE

Republika Hrvatska dosta je kasno počela s razvojem svog pravnog okvira zaštite osobnih podataka. Totalitarni režimi 20. stoljeća u kojima smo živjeli do 1990. godine nisu bili pogodni za zaštitu osobnih prava pojedinca, štoviše u njima se smatralo „normalnim" da državna i partijska tijela imaju pravo nadzora i nad osobnim životom pojedinca. Ratne okolnosti koje su slijedile također nisu pogodovale razvoju zaštite osobnih podataka.

Republika Hrvatska prvi puta cjelovito uređuje pitanje zaštite osobnih podataka *Zakonom o zašiti osobnih podataka* iz 2003. godine. Tim relativno kratkim zakonom (izvorno je imao 40 članaka) uređuje se zaštita osobnih podataka o fizičkim osobama

te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj (čl 1.). Definiran je osobni podatak, zaštita osobnih podataka, privola sudionika i ostali bitni pojmovi. Uređeno je i postupanje s posebnim kategorijama osobnih podataka te iznošenje osobnih podataka iz Republike Hrvatske. Uređeno je pitanje zbirki osobni podataka te Središnji registar u kojemu se nalaze javno dostupne informacije o zbirkama osobnih podataka. Za obavljanje nadzora nad obradom osobnih podataka zakonom je osnovana neovisna ustanova, Agencija za zaštitu osobnih podataka.

Zakon o zaštiti osobnih podataka nekoliko je puta mijenjan i unaprjeđivan, sve do stupanja na snagu Opće uredbe, kojim se izravno uređuje pitanje zaštite osobnih podataka, a kojim je taj Zakon stavljen iznad snage. Novim *Zakonom o provedbi Opće uredbe o zaštiti podataka* uređena su samo ona malobrojna pitanja koja je Opća uredba stavila na dispoziciju državama članicama.

8.4. OPĆA UREDBA O ZAŠTITI OSOBNIH PODATAKA

Većina europskog zakonodavstva sadržana je u direktivama (engl. *directive*) Europske unije. U pitanju su, kako smo već spomenuli, opći akti koji se u pravilu ne primjenjuju izravno, već ciljeve pojedine direktive svaka članica mora u propisanom roku unijeti u vlastito zakonodavstvo, a ako to ne napravi, moguće je i da odgovara za štetu. Ciljeve neke direktive država može unijeti u svoje zakonodavstvo zakonom, neka druga zakonom i dvama provedbenim aktima, treća na treći način. Također, direktive ne sadrže kaznene odredbe, već te odredbe određuje svaka država članica za sebe. U implementaciji direktive, zbog različitih pravnih praksi, jezičnih razlika te ponekad nedorečenosti termina same direktive zna biti manjih razlika između država.

Stoga, kada je potrebno donijeti akt koji će se jedinstveno primjenjivati u cijeloj EU, donose se uredba (engl. *regulation*) koja na jedinstven način rješava određena pitanja. Uredba se primjenjuje jednako i izravno u svim članicama Europske unije. S obzirom na važnost osobnih podataka te današnju stvarnost gdje osobne podatke razmjenjujemo gotovo svakodnevno (od telefoniranja u *roamingu* do kupnje na internetskoj trgovini), Europska unija odlučila je pitanje zaštite osobnih podataka urediti na jedinstven način – uredbom. Samo je nekoliko manje bitnih odredbi ostavljeno na dispoziciju državama članicama.

Ukratko, Opća uredba primjenjuje se u cijeloj Europskoj uniji, a stupila je na snagu 25. svibnja 2018. godine.

8.4.1. RECITAL OPĆE UREDBE

Na početku Opće uredbe nalazi se iznimno duga preambula akta koja se u novije vrijeme naziva i recital. U 173 pasusa recitala, brojčano označenima, nalaze se svrha i ciljevi akta, ovdje Opće uredbe. Oni su pomoć kod pravnog tumačenja akta, a njihov opseg govori o važnosti preciznog tumačenja Opće odredbe. Naime, uvijek se u primjeni u stvarnom životu nalaze slučajevi kada pravna norma nema jedinstveni odgovor te je potrebno tumačenje iste.

„Pravila su žive materije, jer se primjenjuju na životne situacije. Zakonodavac ne može predvidjeti sve životne konstelacije, a ni sudovi ni pravna nauka nisu u položaju da definiraju fiksne metode i granice tumačenja, jer se nalaze u istoj situaciji kao ostale državne vlasti i moraju poštovati načelo pravne države, jednakosti i proporcionalnosti. Umjesto šablonskog postupanja, ono zavisi od pravne dogmatike i kulture. Pravnici su obavezani koristiti transparentna, konzistentna i ubjedljiva obrazloženja svojih odluka“ (Samardžić, 2019).

Navodimo neke najvažnije dijelove početnog dijela recitala.

Zaštita pojedinaca s obzirom na obradu osobnih podataka temeljno je pravo. Člankom 8. stavkom 1. Povelje Europske unije o temeljnim pravima („Povelja”) te člankom 16. stavkom 1. Ugovora o funkcioniranju Europske unije (UFEU) utvrđuje se da svatko ima pravo na zaštitu svojih osobnih podataka (Recital 1).

Dakle, na samom se početku nalazi deklaracija koja navodi kako zaštita osobnih podataka pojedinca ulazi u temeljna prava te se navode osnovni akti EU-a koji navode to pravo.

Ovom Uredbom želi se doprinijeti uspostavi područja slobode, sigurnosti i pravde te gospodarske unije, gospodarskom i socijalnom napretku, jačanju i približavanju gospodarstava na unutarnjem tržištu te dobrobiti pojedinaca (Recital 2).

Ovdje se navodi cilj Uredbe.

Obrada osobnih podataka trebala bi biti osmišljena tako da bude u službi čovječanstva. Pravo na zaštitu osobnih podataka nije apsolutno pravo; mora ga se razmatrati u vezi s njegovom funkcijom u društvu te ga treba ujednačiti s drugim temeljnim pravima u skladu s načelom proporcionalnosti. Ovom se Uredbom poštuju sva temeljna prava i uvažavaju slobode i načela priznata Poveljom koja su sadržana u Ugovorima, osobito poštovanje privatnog i obiteljskog života, doma i komuniciranja, zaštita osobnih podataka, sloboda mišljenja, savjesti i vjeroispovijedi, sloboda izražavanja i informiranja, sloboda poduzetništva, pravo na učinkoviti pravni lijek i pošteno suđenje te pravo na kulturnu, vjersku i jezičnu raznolikost (Recital 4)

Ovaj recital navodi iznimno važno načelo – pravo na zaštitu podataka nije apsolutno pravo već se razmatra u vezi s njegovom funkcijom u društvu te načelom pro-

porcionalnosti. To omogućuje da se, npr. politički dužnosnici obvežu na javnu objavu podataka o primanjima i o imovini.

Gospodarska i društvena integracija proizašla iz funkcioniranja unutarnjeg tržišta dovela je do znatnog povećanja prekograničnih protoka osobnih podataka. Povećala se razmjena osobnih podataka između javnih i privatnih sudionika, uključujući pojedince, udruženja i poduzetnike širom Unije. U skladu s pravom Unije nacionalna tijela država članica pozivaju se na suradnju i razmjenu osobnih podataka kako bi mogla izvršavati svoje dužnosti ili izvršavati zadaće u ime tijela u drugoj državi članici (Recital 5).

Navodi se stvarno stanje koje je razlog donošenja Opće uredbe.

Zbog brzog tehnološkog razvoja i globalizacije pojavili su se novi izazovi u zaštiti osobnih podataka. Opseg prikupljanja i razmjene osobnih podataka značajno se povećava. Tehnologijom se privatnim društvima i tijelima javne vlasti omogućuje uporaba osobnih podataka u dosada nedosegnutom opsegu radi ostvarenja njihovih djelatnosti. Pojedinci svoje osobne informacije sve više čine dostupnima javno i globalno. Tehnologija je preobrazila i gospodarstvo i društveni život te bi trebala dalje olakšavati slobodan protok osobnih podataka u Uniji i prijenos trećim zemljama i međunarodnim organizacijama, osiguravajući pri tome visoku razinu zaštite osobnih podataka (Recital 6).

Odnos je prema tehnologiji dvojak; s jedne strane slobodan protok osobnih podataka olakšava poslovanje, druženje i brojne druge aktivnosti, ali ujedno i predstavlja izazov za zaštitu tih istih podataka.

Za takav razvoj potreban je čvrst i usklađeniji okvir za zaštitu podataka u Uniji koji se temelji na odlučnoj provedbi s obzirom na važnost stvaranja povjerenja koje će omogućiti razvoj digitalne ekonomije na čitavom unutarnjem tržištu. Pojedinci bi trebali imati nadzor nad vlastitim osobnim podacima. Pravnu i praktičnu sigurnost pojedinaca, gospodarskih subjekata i tijela javne vlasti trebalo bi poboljšati (Recital 7).

Građani neće koristiti ili će vrlo malo koristiti digitalno tržište ako su zabrinuti za svoje osobne podatke. Njihova zaštita, ali i mogućnost nadzora nad osobnim podacima jačaju digitalno tržište EU-a.

8.4.2. TEMELJNI POJMOVI

U ovom poglavlju navodimo osnovne pojmove Opće uredbe dok ćemo ostale pojmove koje ona navodi razjasnit daljnjim poglavljima.

8.4.2.1. Osobni podatak

Prema pojmovniku Opće uredbe (čl. 4.) „osobni podaci" znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik/sudionik"); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

Iznimno je bitno uzeti u obzir cjelokupnu odredbu: „identitet utvrđen ili se može utvrditi". Prvi dio je jasan – primjerice ako znamo nečije ime, prezime i adresu, s velikom sigurnošću možemo identificirati pojedinu osobu (osim ako na istoj adresi primjerice djed i unuk imaju isto ime i prezime te će nam trebati i datum rođenja za točnu identifikaciju). U nekoj studijskoj grupi obično će svi studenti imati različito ime i prezime pa ih možemo identificirati po istom, ali i po datumu rođenja.

No, što bi bilo „identitet koji se može utvrditi"? Odgovor nije jednoznačan. Zamislimo da se bavimo medicinskim istraživanjem gripe i u znanstvenom radu opišemo nekoliko slučajeva koje smo medicinski pratili protekle zime. Bez imena i prezimena (a koji su potpuno irelevantni za znanstveno istraživanje) osjetljivi podaci o zdravlju neće se moći povezati s nekom određenom osobom jer oboljelih od gripe ima nekoliko desetaka tisuća svake zime. No, uzmimo kao primjer istraživanje neke rijetke autoimune bolesti koja ostavlja specifične tragove na koži, a ima je svega nekoliko ljudi u županiji ili čak cijeloj državi. U tom slučaju, ako ni ne spomenemo ime i prezime osobe, vrlo je jednostavno povezati istraživanje s konkretnom fizičkom osobom, dakle iznošenjem osjetljivih osobnih podataka. U tom slučaju potrebno je samu osobu pitati za pristanak.

Hoće li neki skup podataka ili izjava predstavljati osobni podatak ili ne, ovisi o vrsti podataka i veličini skupa. Npr. „vlasnik Porchea u Malinskoj na Krku" i „vlasnik Porchea u Zagrebu" bitno su različiti skupovi. U maloj Malinskoj to je vjerojatno jedan pojedinac kojega, ako ima tako rijetko vozilo, svi znaju po njemu. Zagreb opet ima više od nekoliko takvih automobila i spominjanjem same marke automobila nije moguće identificirati fizičku osobu. Dakle, kada govorimo o frazi „identitet koji se može utvrditi", govorimo o vrlo velikom skupu mogućnosti koje mogu identificirati fizičku osobu.

8.4.2.2. Obrada osobnih podataka

Prema definiciji iz Opće Uredbe, „obrada" znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje.

Kao što vidimo, definicija se ne odnosi na tehnologiju obrade podataka, već govorimo o bilo kojim automatiziranim, ali i „ručnim" sustavima obrade.

8.4.2.3. Voditelj i izvršitelj obrade

Prema definiciji „voditelj obrade" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice. Ukratko, voditelj obrade određuje kako će se obrađivati određeni osobni podaci. Pri tome voditelj obrade može i ne mora sam obrađivati osobne podatke. Radi toga Opća uredba poznaje i još jedan pojam: „izvršitelj obrade".

U praksi, voditelj obrade ne mora imati odgovarajuće tehničke i kadrovske uvjete za kvalitetnu obradu osobnih podataka, a često će osim jednostavne obrade trebati i druge usluge za obradu osobnih podataka (npr. analiza tržišta, razne statističke analize, tumačenje podataka i slično). Upravo se u takvim slučajevima javlja izvršitelj obrade. Prema pojmovniku „izvršitelj obrade" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade. Kako smo rekli, u praksi može obavljati i druge poslove, npr. izrada marketinške strategije temeljem analiziranih podataka, ali u toj ulozi neće predstavljati vršitelja obrade.

8.4.3. NAČELA OBRADE

Prema Općoj uredbi (čl. 5.) osobni podaci moraju biti obrađivani:

- zakonito, pošteno i transparentno obrađivani s obzirom na sudionika, dakle pojedinca
- prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama pri čemu daljnja obrada u svrhe arhi-

viranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, ne smatra se neusklađenom s prvotnim svrhama ako se poštuju odgovarajuće zaštitne mjere, primjerice pseudoanonimizacija[2]

- primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju
- točni i prema potrebi ažurni; mora se poduzeti svaka razumna mjera radi osiguravanja da se osobni podaci koji nisu točni, uzimajući u obzir svrhe u koje se obrađuju, bez odlaganja izbrišu ili isprave
- čuvani u obliku koji omogućuje identifikaciju sudionikâ samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju; osobni podaci mogu se pohraniti na dulja razdoblja ako će se osobni podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe
- obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera.

Za sve gore navedeno odgovoran je voditelj obrade.

8.4.4. ZAKONITOST OBRADE

Obrada osobnih podataka zakonita je samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega, a sukladno čl. 6. Opće uredbe:

a) sudionik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha
b) obrada je nužna za izvršavanje ugovora u kojem je sudionik stranka ili kako bi se poduzele radnje na zahtjev sudionika prije sklapanja ugovora
c) obrada je nužna radi poštovanja pravnih obveza voditelja obrade
d) obrada je nužna kako bi se zaštitili ključni interesi sudionika ili druge fizičke osobe

[2] Prema Općoj uredbi „pseudonimizacija" znači obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom sudioniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi. Ukratko, to su podaci iz kojih se više ne može doći do pojedine fizičke osobe jer konkretno ime i prezime uopće nije bitno za statistička i srodna istraživanja.

e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade

f) obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode sudionika koji zahtijevaju zaštitu osobnih podataka, osobito ako je sudionik dijete.

Točka (f) prvog podstavka ne odnosi se na obradu koju provode tijela javne vlasti pri izvršavanju svojih zadaća, dakle kada se obrada obavlja temeljem zakonske dužnosti.

Među glavnim temeljima obrade osobnih podataka je privola koja znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja sudionika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose. U poslovnoj praksi za to često služe nagrade igre – pojedinac sudjeluje u nagradnoj igri na način da ispuni određeni obrazac kojim se od njega traže poslovni podaci.

Kada se obrada temelji na privoli, voditelj obrade mora moći dokazati da je sudionik dao privolu za obradu svojih osobnih podataka. Nadalje, ako sudionik da privolu u vidu pisane izjave koja se odnosi i na druga pitanja, zahtjev za privolu mora biti predočen na način da ga se može jasno razlučiti od drugih pitanja, u razumljivom i lako dostupnom obliku uz uporabu jasnog i jednostavnog jezika. Svaki dio takve izjave koji predstavlja kršenje ove Uredbe nije obvezujući (čl. 7.).

Prema izričitoj odredbi Opće uredbe, sudionik ima pravo u svakom trenutku povući svoju privolu. Povlačenje privole ne utječe na zakonitost obrade na temelju privole prije njezina povlačenja. Prije davanja privole, sudionika se o tome obavješćuje. Povlačenje privole mora biti jednako jednostavno kao i njezino davanje (čl. 7.).

8.4.5. POSEBNE KATEGORIJE OSOBNIH PODATAKA

Opća uredba izričito navodi u čl. 9.: „Zabranjuje se obrada osobnih podataka koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca."

Od te generalne odredbe postoji niz izuzetaka koji omogućavaju da se, primjerice, koristi otisak prsta u sustavima kontrole radnog vremena ili pristupa. Navodimo neke od tih izuzetaka iz čl. 9., pri čemu naglašavamo da kod svake obrade tih izuzetaka treba uzeti u obzir i pravnu praksu, ali i jedno od temeljnih pravnih načela – izuzetke

treba suženo tumačiti. U ovom slučaju, posebnih kategorija osobnih podataka, zabrana obrade istih pravilo je, a mogućnost obrade izuzetak.

Obrada posebnih kategorija osobnih podataka dozvoljena je ako je sudionik dao izričitu privolu za obradu tih osobnih podataka za jednu ili više određenih svrha.

Nadalje, obrada je nužna za potrebe izvršavanja obveza i ostvarivanja posebnih prava voditelja obrade ili sudionika u području radnog prava i prava o socijalnoj sigurnosti te socijalnoj zaštiti u mjeri u kojoj je to odobreno u okviru prava Unije ili prava države članice ili kolektivnog ugovora u skladu s pravom države članice koje propisuje odgovarajuće zaštitne mjere za temeljna prava i interese sudionika. Primjerice, to može biti slučaj gdje je sudionik deklarirao svoja vjerska opredjeljenja kako bi dobio pravo na neradni dan (po Zakonu o blagdanima, spomendanima i neradnim danima u Republici Hrvatskoj „Građani Republike Hrvatske koji Božić slave na dan 7. siječnja u taj dan, islamske vjeroispovijedi u dane Ramazanskog bajrama i Kurban bajrama, te židovske vjeroispovijedi u dane Roš Hašane i Jom Kipura imaju pravo ne raditi".)

Izuzetak je i slučaj kada je obrada je nužna za zaštitu životno važnih interesa sudionika ili drugog pojedinca ako sudionik fizički ili pravno nije u mogućnosti dati privolu. Npr. sudioniku je potreban hitni medicinski zahvat, a nije pri punoj svijesti, pa se iz baze podataka traže podaci je li alergičan na neke lijekove.

Postoji i još jedan važan izuzetak: obrada se provodi u sklopu legitimnih aktivnosti s odgovarajućim zaštitnim mjerama zaklade, udruženja ili drugog neprofitnog tijela s političkim, filozofskim, vjerskim ili sindikalnim ciljem te pod uvjetom da se obrada odnosi samo na članove ili bivše članove tijela ili na osobe koje imaju redovan kontakt s njom u vezi s njezinim svrhama i da osobni podaci nisu priopćeni nikome izvan tog tijela bez privole sudionika. Dakle, sindikat će moći voditi bazu svojih članova, vjerska organizacija ili udruga vjernika također podatke o svojim članovima.

Naravno, izuzetak se odnosi i na slučaj kada se obrada odnosi na osobne podatke za koje je očito da ih je objavio sudionik.

8.4.6. PRAVA SUDIONIKA

Voditelj obrade dužan je sudioniku pružiti informacije o osobnim podacima koji se vode o sudioniku, i to bez naknade (čl. 12.).

Ako su osobni podaci koji se odnose na sudionika prikupljeni od sudionika (čl. 13.), voditelj obrade u trenutku prikupljanja osobnih podataka sudioniku pruža sve sljedeće informacije: (a) identitet i kontaktne podatke voditelja obrade i, ako je primjenjivo, predstavnika voditelja obrade, (b) kontaktne podatke službenika za zaštitu podataka, ako je primjenjivo, (c) svrhe obrade radi kojih se upotrebljavaju osobni

podaci kao i pravnu osnovu za obradu, (d) legitimne interese voditelja obrade ili treće strane, (e) primatelje ili kategorije primatelja osobnih podataka ako ih ima, i (f) ako je primjenjivo, činjenicu da voditelja obrade namjerava osobne podatke prenijeti trećoj zemlji ili međunarodnoj organizaciji.

Osim informacija iz stavka 1., voditelj obrade u trenutku kada se osobni podaci prikupljaju pruža sudioniku sljedeće dodatne informacije potrebne kako bi se osigurala poštena i transparentna obrada i to: razdoblje u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterije kojima se utvrdilo to razdoblje; postojanje prava da se od voditelja obrade zatraži pristup osobnim podacima i ispravak ili brisanje osobnih podataka ili ograničavanje obrade koji se odnose na sudionika ili prava na ulaganje prigovora na obradu takvih te prava na prenosivost podataka; postojanje prava da se u bilo kojem trenutku povuče privolu, a da to ne utječe na zakonitost obrade koja se temeljila na privoli prije nego što je ona povučena; pravo na podnošenje prigovora nadzornom tijelu; informaciju o tome je li pružanje osobnih podataka zakonska ili ugovorna obveza ili uvjet nužan za sklapanje ugovora te ima li sudionik obvezu pružanja osobnih podataka i koje su moguće posljedice ako se takvi podaci ne pruže; te postojanje automatiziranog donošenja odluka.

Sudionik ima pravo bez nepotrebnog odgađanja ishoditi od voditelja obrade ispravak netočnih osobnih podataka koji se na njega odnose. Uzimajući u obzir svrhe obrade, sudionik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave (čl. 16.).

Sudionik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose bez nepotrebnog odgađanja. No, to pravo nije bezuvjetno. Voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako su ispunjeni određeni uvjeti, od kojih navodimo najvažnije: osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili na drugi način obrađeni; sudionik povuče privolu na kojoj se obrada temelji i ne postoji druga pravna osnova za obradu; sudionik uloži prigovor na obradu te ne postoje jači legitimni razlozi za obradu te osobni podaci nezakonito su obrađeni (čl. 17.).

Ako se osobni podaci obrađuju za potrebe izravnog marketinga (čl. 21.), sudionik u svakom trenutku ima pravo uložiti prigovor na obradu osobnih podataka koji se odnose na njega za potrebe takvog marketinga, što uključuje izradu profila u mjeri koja je povezana s takvim izravnim marketingom. Ako se sudionik protivi obradi za potrebe izravnog marketinga, osobni podaci više se ne smiju obrađivati u takve svrhe.

Vrlo je zanimljivo pravo sudionika iz čl. 22. Opće uredbe, a koje se ne nalazi u starijim propisima o zaštiti osobnih podataka, pravo je na automatizirano pojedinačno donošenje odluka: „Ispitanik ima pravo da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila, koja proizvodi

pravne učinke koji se na njega odnose ili na sličan način značajno na njega utječu." Što ovo znači u praksi? Banke i drugi davatelji usluga izrađuju automatizirane profile korisnika, primjerice vezano za kreditni bonitet. Neke osobe takvi automatizirani profili vrlo loše prikazuju, npr. gledaju samo plaću, a osoba zarađuje veći dio prihoda od najma apartmana. Sudionik ima pravo zatražiti da se kod njega provede „ručna" izrada profila gdje će o njegovoj kreditnoj sposobnost odlučiti nadležno tijelo banke.

8.4.7. VODITELJ OBRADE I IZVRŠITELJ OBRADE

Uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s ovom Uredbom (čl. 24.).

Opća uredba govori u čl. 25. i o potrebi odgovarajuće zaštite osobnih podataka koji se prikupljaju. Voditelj obrade, i u vrijeme određivanja sredstava obrade i u vrijeme same obrade, provodi odgovarajuće tehničke i organizacijske mjere poput pseudonimizacije, za omogućavanje učinkovite primjene načela zaštite podataka, kao što je smanjenje količine podataka, te uključenje zaštitnih mjera u obradu kako bi se ispunili zahtjevi iz ove Uredbe i zaštitila prava sudionika. Voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kojima se osigurava da integriranim načinom budu obrađeni samo osobni podaci koji su nužni za svaku posebnu svrhu obrade. Ta se obveza primjenjuje na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost.

Navedeno uključuje klasične mjere informacijske sigurnosti – potrebno je napraviti procjenu rizika i potom odgovarajuće zaštititi podatke. Neće svi podaci biti jednako izloženi, primjerice podaci o zdravlju znatno su osjetljiviji od podataka o članstvu nekog ribičkog društva.

Čl. 28. Opće uredbe uređuje obveze izvršitelja obrade. Ako se obrada provodi u ime voditelja obrade, voditelj obrade koristi se jedino izvršiteljima obrade koji u dovoljnoj mjeri jamče provedbu odgovarajućih tehničkih i organizacijskih mjera na način da je obrada u skladu sa zahtjevima iz ove Uredbe i da se njome osigurava zaštita prava sudionika. Obrada koju provodi izvršitelj obrade uređuje se ugovorom ili drugim pravnim aktom u skladu s pravom Unije ili pravom države članice, koji izvršitelja obrade obvezuje prema voditelju obrade, a koji navodi predmet i trajanje obrade, prirodu i svrhu obrade, vrstu osobnih podataka i kategoriju sudionika te obveze i prava voditelja obrade.

Predaja osobnih podataka drugome na obradu smatra se toliko važnom da se izričito propisuje ugovaranje takvog pravnog posla. U samoj Općoj uredbi detaljno se navodi i što takav ugovor mora sadržavati.

Svaki voditelj obrade i predstavnik voditelja obrade, ako je primjenjivo, vodi evidenciju aktivnosti obrade za koje je odgovoran (čl. 30.). Ako je vjerojatno da će neka vrsta obrade, osobito upotrebom novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade prije obrade provodi procjenu učinka predviđenih postupaka obrade na zaštitu osobnih podataka (čl. 35.).

8.4.8. SLUŽBENIK ZA ZAŠTITU PODATAKA

Voditelj obrade i izvršitelj obrade imenuju službenika za zaštitu podataka u svakom slučaju u kojem:

a) obradu provodi tijelo javne vlasti ili javno tijelo, osim za sudove koji djeluju u okviru svoje sudske nadležnosti

b) osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje se od postupaka obrade koji zbog svoje prirode, opsega i/ili svrha iziskuju redovito i sustavno praćenje sudionika u velikoj mjeri ili

c) osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje se od opsežne obrade posebnih kategorija podataka (čl. 37.).

Grupa poduzetnika može imenovati jednog službenika za zaštitu podataka pod uvjetom da je službenik za zaštitu podataka lako dostupan iz svakog poslovnog nastana. Nadalje se propisuje (također čl. 37.) ako je voditelj obrade ili izvršitelj obrade tijelo javne vlasti ili javno tijelo, za nekoliko takvih vlasti ili tijela može se imenovati jedan službenik za zaštitu podataka uzimajući u obzir njihovu organizacijsku strukturu i veličinu.

Službenik za zaštitu podataka imenuje se na temelju stručnih kvalifikacija, a osobito stručnog znanja o pravu i praksama u području zaštite podataka.

Voditelj obrade i izvršitelj obrade osiguravaju da je službenik za zaštitu podataka na primjeren način i pravodobno uključen u sva pitanja u pogledu zaštite osobnih podataka. Voditelj obrade i izvršitelj obrade podupiru službenika za zaštitu podataka u izvršavanju zadaća pružajući mu potrebna sredstva za izvršavanje tih zadaća i ostvarivanje pristupa osobnim podacima i postupcima obrade te za održavanje njegova stručnog znanja. Voditelj obrade i izvršitelj obrade osiguravaju da službenik za zaštitu podataka ne prima nikakve upute u pogledu izvršenja tih zadaća. Voditelj obrade ili

izvršitelj obrade ne smiju ga razriješiti dužnosti ili kazniti zbog izvršavanja njegovih zadaća. Službenik za zaštitu podataka izravno odgovara najvišoj rukovodećoj razini voditelja obrade ili izvršitelja obrade. Sudionici mogu kontaktirati službenika za zaštitu podataka u pogledu svih pitanja povezanih s obradom svojih osobnih podataka i ostvarivanja svojih prava iz ove Uredbe. Službenik za zaštitu podataka obvezan je tajnošću ili povjerljivošću u vezi s obavljanjem svojih zadaća, u skladu s pravom Unije ili pravom države članice. Službenik za zaštitu podataka može ispunjavati i druge zadaće i dužnosti. Voditelj obrade ili izvršitelj obrade osigurava da takve zadaće i dužnosti ne dovedu do sukoba interesa (čl. 38. Opće uredbe).

Prema čl. 39. Opće uredbe službenik za zaštitu podataka obavlja najmanje sljedeće zadaće:

a) informiranje i savjetovanje voditelja obrade ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz ove Uredbe te drugim odredbama Unije ili države članice o zaštiti podataka
b) praćenje poštovanja ove Uredbe te drugih odredaba Unije ili države članice o zaštiti podataka i politika voditelja obrade ili izvršitelja obrade u odnosu na zaštitu osobnih podataka, uključujući raspodjelu odgovornosti, podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade te povezane revizije
c) pružanje savjeta, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja
d) suradnja s nadzornim tijelom
e) djelovanje kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade, što uključuje i prethodno savjetovanje te savjetovanje, prema potrebi, o svim drugim pitanjima.

Službenik za zaštitu osobnih podataka može biti i na odgovarajući način certificiran.

8.4.9. PRIJENOS OSOBNIH PODATAKA TREĆIM ZEMLJAMA

Unutar EU-a sve zemlje dužne su poštivati odredbe Opće uredbe i primjereno čuvati osobne podatke. To se odnosi i na pravne i fizičke osobe u tim zemljama. No što je s trećim zemljama, onima izvan EU-a? Poslovna praksa (od trgovine do putovanja) traži da se i s tim zemljama razmjenjuju osobni podaci. No, u praksi to može biti opasno; prenijeti osobne podatke u zemlju koja ih ne štiti, nema učinkovito sudstvo ili je sama u političkim neredima može značiti da ti podaci mogu biti zloporabljeni.

Prijenos osobnih podataka trećoj zemlji ili međunarodnoj organizaciji može se dogoditi kada Komisija odluči da treća zemlja, područje, ili jedan ili više određenih sektora unutar te treće zemlje ili međunarodna organizacija o kojoj je riječ osigurava primjerenu razinu zaštite. Takav prijenos ne zahtijeva posebno odobrenje (čl. 45.).

Europska komisija dakle, ocjenjujući vladavinu prava, poštovanje ljudskih prava i temeljnih sloboda, relevantno zakonodavstvo i drugo, po čl. 45. Opće uredbe može nakon procjene primjerenosti stupnja zaštite putem provedbenog akta odlučiti da treća zemlja, područje, ili jedan ili više određenih sektora unutar treće zemlje ili međunarodna organizacija osigurava primjerenu razinu zaštite.

Ako nije donesena takva odluka Komisije, voditelj obrade ili izvršitelj obrade trećoj zemlji ili međunarodnoj organizaciji osobne podatke mogu prenijeti samo ako je voditelj obrade ili izvršitelj obrade predvidio odgovarajuće zaštitne mjere i pod uvjetom da su sudionicima na raspolaganju provediva prava i učinkovita sudska zaštita.

Dakle, Komisija posebnim aktom, ili ako voditelj ili izvršitelj obrade moraju odlučiti hoće li će se obzirom na stanje u nekoj trećoj zemlji dopustiti razmjena osobnih podataka, npr. isključivo potrebna za primjerice avionski let, ili se dozvoljava razmjena i šireg opsega osobnih podataka

8.4.10. NEOVISNO NADZORNO TIJELO - AGENCIJA ZA ZAŠTITU OSOBNIH PODATAKA

Prema Općoj Uredbi, čl. 51. svaka država članica osigurava da je jedno ili više neovisnih tijela javne vlasti odgovorno za praćenje primjene ove Uredbe kako bi se zaštitila temeljna prava i slobode pojedinaca u pogledu obrade i olakšao slobodan protok osobnih podataka unutar Unije („nadzorno tijelo"). Prema čl. 52. Opće uredbe svako nadzorno tijelo djeluje potpuno neovisno pri obavljanju svojih dužnosti i izvršavanju svojih ovlasti u skladu s ovom Uredbom. Član ili članovi svakog nadzornog tijela moraju biti slobodni od vanjskog utjecaja, bilo izravnog bilo neizravnog, pri obavljanju svojih dužnosti i izvršavanju svojih ovlasti u skladu s ovom Uredbom te ne smiju tražiti ni primati upute ni od koga.

Važna je odredba i čl. 77. Opće uredbe prema kojoj, ne dovodeći u pitanje druga upravna ili sudska pravna sredstva, svaki sudionik ima pravo podnijeti pritužbu nadzornom tijelu, osobito u državi članici u kojoj ima uobičajeno boravište, u kojoj je njegovo radno mjesto ili mjesto navodnog kršenja, ako sudionik smatra da obrada osobnih podataka koja se odnosi na njega krši ovu Uredbu.

Sukladno hrvatskom *Zakon o provedbi Opće uredbe o zaštiti podataka* nadzorno tijelo u smislu odredbe članka 51. Opće uredbe je Agencija za zaštitu osobnih poda-

taka, poznata i po svojoj kratici AZOP. Agencija je neovisno državno tijelo. Agencija je u svom radu samostalna i neovisna i za svoj rad odgovara Hrvatskome saboru. Sjedište je Agencije u Zagrebu. Opširnije o Agenciji može se naći na njezinim internetskim stranicama (AZOP, 2019).

8.5. ZAKLJUČAK

Pitanje privatnosti i zaštite osobnih podataka prošlo je dug razvojni put – od razdoblja kada privatnost gotovo da nije postojala do danas kada pravo na privatnost, pravo na tajnost dopisivanja i pravo na zaštitu osobnih podataka postaje dijelom ljudskih prava.

Dok je do prije nekoliko desetaka godina glavna ugroza po pitanju privatnosti pojedinca dolazila od država i njihovih represivnih aparata, razvoj tehnologije doveo je do toga da gotovo svatko danas može ugroziti naše pravo na privatnost. Procesorska snaga nekadašnjih superračunala koja su mogle kupiti samo vlade, vojska i bogata sveučilišta danas je dostupna za dvje do tri hrvatske plaće. Širenje mobilnih telefona koji praktično stalno prate naš položaj te društvenih mreža gdje sami objavljujemo gomile osobnih podataka još su uvelike posložili ovu problematiku.

Opća uredba o zaštiti osobnih podataka, GDPR, dokument je nastao temeljem više od 30 godina razvoja pravne teorije i prakse, prvo u okvirima Vijeća Europe a potom i Europske unije. U pitanju je složen i pravno „težak" propis, opsežan i ne uvijek potpuno precizan. U ovom tekstu naveli smo samo osnove – udžbenici koji se bave detaljno Općom uredbom često imaju i više od 1000 stranica. Uza sve te opsežne tekstove stvara se i pravna praksa Europskog suda, a u pravu Europske unije, podsjetimo se, pravna praksa ima bitno veće značenje nego u hrvatskom pravu.

Osim propisa vrlo je važno podizati i svijest o važnosti zaštite privatnosti i osobnih podataka pojedinca. Ponajprije svijest o tome da se naši osobni podaci obrađuju. Dovoljno je uostalom u Google pretraživač unijeti marku nekog automobila kako bi poslije danima gledali reklame za automobile. Katkada to i nije loše – primjerice Amazon prati naše kupnje i pretraživanja kako bi nam ponudio knjige i glazbu upravo stila koji pratimo. No, u nekim slučajevima ne želimo da se naši osobni podaci pohranjuju i obrađuju i na to imamo potpuno pravo. Imamo i naravno pravo pitati i dobiti informacije kako netko obrađuje naše osobne podatke.

Ponekad i sami moramo poraditi na vlastitoj privatnosti – objaviti na Facebooku kako cijela obitelj u subotu ide na odmor, to tako da je obavijest javna, vidljiva svima, doslovno znači pozvati provalnike u kuću u nedjelju. Uz propise treba i zdravo

razmišljati! Ako se ne brinemo sami za svoje osobne podatke, nema tog pravnog okvira koji nam može pomoći.

Na kraju, ne zaboravite da imate pravo znati kako se, koliko dugo i na koji način obrađuju vaši osobni podaci. Kada je ta obrada dobrovoljna, imate pravo uskratiti pristanak. I ako netko krši propise, imate pravo zatražiti zaštitu od nadležnog tijela.

Uz sve to uvijek se treba zapitati: „Komu i zašto dajem svoje osobne podatke?" Nije rijedak slučaj da trgovački lanac nagradnom igrom kojom daruje automobil sasvim legalno prikupi nekoliko stotina tisuća listića građana, s uredno ispunjenim osobnim podacima i s uredno navedenom svrhom upotrebe u marketinške svrhe. Je li teorijska mogućnost dobivanja nagrade vrijedna vaših podataka? U takvim pitanjima ne može vam pomoći zakonodavac, već samo vlastito razmišljanje i vlastiti stav o privatnosti. Slično kao i kod društvenih mreža, zapitajte se treba li baš svaka informacija o vašem kretanju i navikama biti javna? Kada jeste i kada niste kod kuće? Što jedete? Nije to pitanje samo zaštite osobnih podataka, već i cjelokupne vaše osobnosti. Sutra vaš poslodavac, osiguravajuće društvo ili netko treći može na temelju vaših podataka izraditi vrlo precizan profil vaše osobe i vaših navika.

Dodatne informacije o zaštiti osobnih podataka mogu se naći na stranicama AZOP-a (AZOP, 2019) te Europske komisije (Reforma pravila EU-a o zaštiti podataka u 2018., 2019).

8.6. LITERATURA

AZOP - Agencija za zaštitu osobnih podataka. (2018). Preuzeto s https://www.azop.hr, 16.6.2019.

Brezak, M. (1998). *Pravo na osobnost*. Zagreb: Nakladni zavod Matice Hrvatske.

Direktiva 95/46/EZ o zaštiti pojedinaca u pogledu obrade osobnih podataka i slobodnog kolanja takvih podataka, *Službeni list Europskih zajednica*, L 281 od 23.11.1995.

Direktiva 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija, *Službeni list Europske unije*, L 201/37 od 12.07.2002.

Dragičević, D. (2015). *Pravna informatika i pravo informacijskih tehnologija*. Zagreb: Narodne novine.

Opća deklaracija o ljudskim pravima. *Narodne novine, Međunarodni ugovori,* br. 12/2009.

Povelja Europske unije o temeljnim pravima. *Službeni list Europske unije*, C/303/1 od 12.12.2007.

Popis potpisa i ratifikacija Konvencije 108. (2019). Preuzeto s https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=XClmeYmJ, 16.6.2019.

Reforma pravila EU-a o zaštiti podataka u 2018. (2018). Preuzeto s https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_hr, 16.6.2019.

Samardžić, D. (2012). Tumačenje u skladu sa evropskim pravom i direktivama. *ANALI Pravnog fakulteta Univerziteta u Zenici*. Preuzeto s http://prf.unze.ba/Docs/Anali/godina_5_broj_9/D_Samardzic.pdf, 7.6.2019.

Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27.5.2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), *Službeni list Europske unije*, L 119/1 od 4.5.2016.

Uredba br. 45/2001 Europskog parlamenta i Vijeća o zaštiti osoba pri obradi osobnih podataka u institucijama i tijelima Zajednice te o slobodnome protoku takvih podataka, *Službeni list Europske unije*, L 008/1 od 18.12.2000.

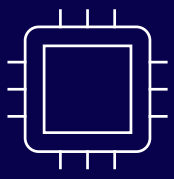
Ustav Republike Hrvatske, *Narodne novine*, br. 56/1990, 135/1997, 08/1998, 113/2000, 124/2000, 28/2001, 41/2001, 55/2001, 76/2010, 85/2010 i 05/2014.

Zakon o blagdanima, spomendanima i neradnim danima u Republici Hrvatskoj (pročišćeni tekst), *Narodne novine*, br. 136/2002.

Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka, *Narodne novine, Međunarodni ugovori*, br. 4/2005.

Zakon o provedbi Opće uredbe o zaštiti podataka, *Narodne novine*, br. 42/2018.

Zakon o zaštiti osobnih podataka, *Narodne novine*, br. 103/2003, 118/2006, 41/2008, 130/2011 i 106/2012.



TEHNIČKI APSEKTI DIGITALNOG SVIJETA

doc. dr. sc. Marin Vuković
Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu

9. OSOBNA SIGURNOST I ZLOĆUDNI PROGRAMI NA INTERNETU

Sažetak

Zlođudni kod općeniti je naziv za računalne programe kojima je cilj na neki način naštetiti računalnom sustavu, računalu i mreži. Prvi takav kod napisan je 1971. godine kao eksperiment. Nazvan je Creeper te se smatra pretečom današnjih modernih zlođudnih programa raznih vrsta. U počecima nastanka zlođudnih programa cilj je bio zastrašiti korisnike porukom na ekranu ili, u najgorem slučaju, onesposobiti napadnuto računalo. Danas je situacija bitno drukčija, a glavni su motivi najčešće financijske prirode.

U ovome poglavlju pojašnjene su vrste zlođudnog koda te načini napada na računalne sustave korisnika te načini napada na proizvodne pogone i državne institucije. Osim metoda poput neželjene pošte (engl. spam), internetske krađe podataka (engl. phishing), društvenog inženjeringa, zlođudni programi usmjereni na osobna računala kornsika (engl. ransomware) i mrežom zaraženih računala (engl. botnet), obrazlažu se načini i razlozi špijunaže te elektroničkog ratovanja.

U današnje vrijeme pojedinac nikako ne smije zanemariti prijetnju zlođudnih programa pametnim telefonima jer je sve više zlođudnih programa usmjereno na pametne telefone. Pametni telefoni vrlo su dostupni, sve se više koriste, a korisnici ih još uvijek ne shvaćaju kao moćne uređaje na kojima se, uz korisne aplikacije, može izvoditi i zlođudni kod.

Korisnike od zlođudnih programa ponajprije štite antivirusni programi. Međutim, korisnici trebaju biti svjesni da rizik uvijek postoji te biti oprezni u upotebi svih vrsta računalnih sustava. Najbitnije je ne biti lakovjeran na ponude besplatnih

sadržaja, programa i medija koji se mogu preuzeti s ilegalnih servisa kao što je torrent ili s ilegalnih mrežnih sjedišta koja nude besplatne inačice programa i alata.

9.1. KRATKA POVIJEST I GLAVNE ZNAČAJKE ZLOĆUDNIH PROGRAMA

Zloćudni kod (engl. *malware*) općeniti je naziv za računalne programe kojima je cilj naštetiti računalnom sustavu na kojemu su pokrenuti. Prvi takvi programi kreirani su eksperimentalno, ne nužno sa zloćudnom namjenom. Kao prvi zloćudni kod navodi se program Creeper iz 1971. godine koji je nakon pokretanja na računalu ispisivao poruku korisnicima (Wikidot). Specifičnost Creepera jest da se samostalno širio i pokretao na računalima u lokalnoj, tada vrlo ograničenoj, mreži. Naziv „*virus*", koji se još uvijek često koristi, uveden je početkom 80-ih godina 20. stoljeća kada su zloćudni programi polako počeli postajati prijetnja računalnim sustavima.

Neki od poznatijih prvih virusa koji su utrli put modernim zloćudnim programima su: Jerusalem (MalwareWiki, 2017), specifičan po tome da se aktivirao na petak 13. i brisao sve podatke te Michelangelo koji se aktivirao 3. ožujka (rođendan poznatog Michelangela) i također brisao podatke korisnika (TrendMicro, 2017). Uz to, zloćudni kod Michelangelo poseban je i po tome da se pokretao na nižoj razini računala od prethodnih virusa – umjesto pokretanja na razini operacijskoga sustava, Michelangelo se izvodio na razini tzv. *Master Boot Record*, odnosno upravljačkog BIOS-a.

S vremenom su se razvijale nove inačice zloćudnih programa sa sve naprednijim funkcionalnostima koje su svakako postajale sve zlonamjernije. Neki od tadašnjih virusa pokušavali su u potpunosti onesposobiti računalo na kojem su pokrenuti pa je u tom smislu izmišljen i termin „*bricking*" što bi u slobodnom prijevodu značilo pretvaranje računala u ciglu, odnosno beskorisnu kutiju. Međutim, danas to više nije slučaj jer svako računalo, poslužitelj, pametni telefon ili bilo koji drugi zaraženi uređaj predstavlja potencijal za daljnje napade zbog svoje procesorske moći. Tako da se današnji zloćudni programi više usmjeravaju na pretvaranje računala u sredstvo kojim napadač može izvoditi daljnje napade ili, pak, zahtijevati otkupninu od korisnika kako bi uklonio zloćudni program.

Možda i najzanimljivija osobina zloćudnih programa je način na koji se šire jer je širenje zapravo jedini način za nanošenje dugoročne i veće štete korisnicima i računalnim sustavima. Već prvi zloćudni programi mogli su se samostalno širiti mrežom, no razlog tome bio je više eksperimentalne prirode i bili su namijenjeni zatvorenim mrežama jer u to doba nije postojao internet kakav danas poznajemo. Prvi doista zlonamjerni programi napravljeni su tako da se šire prijenosnim medijima kao što su diskete koje su u ondašnje vrijeme bile najrašireniji način prijenosa podataka između računala. Zloćudni program kopirao bi se na disketu zajedno s korisnim podatcima te bi se na odredišnom računalu pokrenuo i izvršio svoju namjenu. Iz tog su razloga već u 90-im godinama napravljeni prvi antivirusni programi koji su nadzirali sve datoteke

koje se nalaze na računalu i sve prijenosne medije koji donose podatke u sustav. Od nastanka prvih antivirusnih alata do danas traje svojevrsno natjecanje antivirusnih tvrtki i zlonamjernih pojedinaca i organizacija u tome kako otkriti zloćudni kod odnosno kako napraviti zloćudni kod koji se neće moći otkriti.

Kako bismo bolje shvatili zloćudni kod i ciljeve, potrebno je razraditi motivaciju zloćudnog pojedinca ili organizacije za izradom takvih programa čime se bavi sljedeće poglavlje. Nakon toga bit će predstavljene podvrste zloćudnog koda, ponajprije na temelju načina širenja i funkcionalnosti koje se izvode na zaraženom sustavu ili računalu. Konačno, na kraju će biti opisani načini zaštite te preporuke za korisnike u smislu zaštite vlastitih sustava i podataka.

9.2. ZAŠTO POSTOJE ZLOĆUDNI PROGRAMI?

Kako bi se shvatile funkcionalnosti pojedinih zloćudnih programa, potrebno je razmotriti općenitu motivaciju za izradu zloćudnog koda. Kako je navedeno, cilj prvih zloćudnih programa bio je zastrašiti korisnike porukom na ekranu ili, u najgorem slučaju, onesposobiti napadnuto računalo. Danas je situacija bitno drukčija, a glavni su motivi najčešće financijske prirode.

Internet je najveća svjetska mreža s ogromnim brojem korisnika koji je koriste za zabavu, ali i za informiranje o proizvodima, kupnji i za različite transakcije. Posljedica toga je da se na našim računalima i u okviru internetskih usluga, u tzv. oblaku (engl. *cloud*), nalazi značajna količina naših osobnih i manje osobnih podataka. Podatci o nama, našim navikama i interesima, a posebice brojevi naših kreditnih kartica, telefonski brojevi i slični osobni podatci, potencijalnim napadačima omogućuju stvaranje slike o nama i iskorištavanje tih podataka protiv nas ili naših prijatelja i kolega. U nastavku je dano nekoliko primjera ilegalne zarade na internetu koji predstavljaju dobar motiv za izradu zloćudnog koda.

9.2.1. NEŽELJENE PORUKE (SPAM PORUKE)

Svi smo upoznati s neželjenom poštom, tzv. *spam* porukama u elektroničkom sustavu. Najčešće su to reklame za proizvode koji nas ne zanimaju, a filteri naših e-sandučića više ili manje uspješno ih uklanjaju. No, takve se poruke temelje na količini poslanih poruka. Ako napadač ima pristup velikom broju postojećih e-adresa, nije problem poslati reklamu na tisuće i tisuće osoba i poduzeća. Ukoliko samo mali postotak primatelja uistinu otvori poruku i zainteresira se za proizvod, tzv. kampanja neželjene pošte može ipak biti uspješna. U pozadini je svega neko poduzeće koje na

taj način reklamira svoj proizvod i spremno je napadaču platiti određenu svotu kako bi dosegla određen broj korisnika. S druge strane, napadač se reklamira poduzeću s obećanjem da će njihova reklamna poruka doseći određen broj korisnika i za to traži određeni iznos. Kada sagledamo veličinu interneta, postaje jasno da napadači i od takvih, naizgled bezazlenih napada, mogu imati značajnu novčanu korist.

Ono što je zanimljivo u kontekstu zloćudnog koda jest: kako je napadač došao do svih tih postojećih e-adresa? Česti odgovor je upravo zloćudni kod. Zamislimo da je napadač napravio zloćudni kod koji će nakon zaraze korisničkoga računala ili mrežne usluge za slanje poruka iščitati sve e-adrese s kojima je korisnik komunicirao. Sve su te adrese valjane i napadač može biti siguran da će njegova poruka doista doći do pravog korisnika. Prikupljanje je adresa osobina gotovo svih današnjih zloćudnih programa. Nekada je motiv samo neželjena reklamna elektronička pošta, no češće se radi o tome da se, uz neželjenu reklamnu elektroničku poštu i ostale napade, adrese koriste i za daljnje slanje samog zloćudnog koda kako bi se na isti način prikupilo još više stvarnih e-adresa.

9.2.2. DRUŠTVENI INŽENJERING I INTERNETSKA KRAĐA PODATAKA (ENGL. PHISHING)

Zamislimo da je napadač doista dobio pristup našim kontaktima. Jednostavniji način jest da pokuša na sve te kontakte poslati neželjena pošta u nadi da će netko doista i otvoriti reklamnu poruku. Inteligentniji i znatno uspješniji način jest da napadač kontaktira naše kontakte s lažiranom adresom pošiljatelja i navede naše kontakte na mišljenje da im tu poruku šaljemo mi. Tehnički je to dosta jednostavno izvedivo ukoliko se ne koristi infrastruktura javnog i privatnog ključa popraćena certifikatima. Naši će kontakti tada znatno lakše otvoriti poruku i reagirati na upute iz poruke. Slanje poruka u kojima napadač pokušava navesti primatelja na neku akciju naziva se internetska krađa podataka (engl. *phishing*), a postupak u kojem se te poruke personaliziraju primateljima na temelju ukradenih podataka (u ovom slučaju samo adrese pošiljatelja) društveni inženjering.

Treba svakako naglasiti da je društveni inženjering znatno širi pojam od neželjene pošte i napadačima šruža znatno više mogućnosti ovisno o količini osobnih podataka koje je napadač uspio prikupiti o osobi. Postoje primjeri lažnih poruka u kojima se tražila otkupnina za navodne otmice, a preduvjet za takve poruke bilo je poznavanje obiteljskih prilika i odnosa žrtava kako bi napadači mogli stvoriti priču o navodnoj otmici. U svakom slučaju, društveni inženjering danas je vjerojatno i najopasniji vektor napada jer omogućuje značajnu personalizaciju i otvara put nebrojenim prjevarama na internetu. Ponavljamo, uloga zloćudnog koda jest upravo provala u sustave

i računala te prikupljanje tih osobnih podataka na temelju kojih se izgrađuje prijevara.

Drugi pojam koji je potrebno naglasiti jest internetska krađa podataka (engl. *phishing*). Kako smo naveli, on označava slanje poruke korisniku, odnosno žrtvi, kako bi ga naveo na neku akciju. Internetska krađa podataka (engl. *phishing*) bitna je zato što se upravo pomoću nje izvodi najveći broj prijevara i gotovo uvijek predstavlja prvi vektor odnosno korak napada. Ukoliko korisnik nasjedne na taj prvi korak, napadaču se otvaraju mogućnosti za daljnje napade i akcije kojima je cilj kompromitacija podataka ili sustava korisnika.

Najtipičniji je primjer internetske krađe podataka (engl. *phishing*) poruka u kojoj se primatelja navodi na promjenu zaporke na nekoj usluzi zbog nekog izmišljenog razloga. Ukoliko žrtva povjeruje poruci, poveznica je vodi na lažiranu internetsku stranicu koja izgleda kao stvarna forma za unos podataka za prijavu. Unosom, primjerice, imena i zaporke, žrtva ih zapravo predaje napadaču koji nadalje može pristupati ciljanoj usluzi sa svim ovlastima žrtve. Uz to, žrtva toga često nije ni svjesna. Nakon toga napadač račun žrtve koristi za daljnje napade s lažnim identitetom žrtve. Nedavni primjer takvog napada napravljen je korisnicima usluge Gmail gdje su napadači nakon krađe podataka za pristup svim kontaktima žrtve slali poruke o navodnoj potrebi za financijskom pomoći zbog problema u inozemstvu.

Kao i kod neželjene pošte navedene metode i primjeri u konačnici imaju za cilj napadaču osigurati financijsku dobit, u ovom slučaju na nešto složeniji ali i isplativiji način.

9.2.3. KOMPROMITIRANI UREĐAJI KAO DIO BOTNETA

Do sada razrađena motivacija za izradu zlćudnog koda sadržavala je u pravilu prikupljanje podataka koji napadačima pomažu u provedbi daljnjih napada. Međutim, ako razmatramo slanje neželjene pošte ili internetske krađe podataka porukama (engl. *phishing*), potrebno se zapitati od kuda se šalju te poruke. Kako bi napadač mogao poslatimnogo poruka u kratkom vremenu, potrebna mu je infrastruktura koja se sastoji od mnoštva računala koja mogu obrađivati podatke i slati, u danom primjeru, zlonamjerne e-poruke. Zato je posljednjih godina čest trend u kojemu se zlćudni kod zadržava na računalu ili sustavu žrtve kako bi napadač mogao kontrolirati to računalo i koristiti ga, u ovom primjeru, za slanje poruka. Nakon zaraze korisničkog računala napadač ga može kontrolirati naredbama i pokretati različite scenarije napada. U tom kontekstu važan je pojam tzv. kontrolnog poslužitelja (engl. *command and control server, C&C*) s kojeg napadač šalje naredbe svim zaraženim računalima. Mreža zaraženih računala naziva se *botnet*, a zaraženo računalo koje je dio te mreže *bot*.

Iako problematika mreže zaraženih računala (engl. *botnet*) izlazi iz okvira razmatrane uloge zloćudnih programa, potrebno je napomenuti kako mreže zaraženih računala, tzv. *botneti* služe i za druge maliciozne aktivnosti izuzev slanja neželjene pošte i pošte namijenje internetskoj krađi podataka. Posljednjih godina zabilježen je trend gdje se zaražena računala koriste za napade na infrastrukturu interneta, primjerice poslužitelje usluge DNS (*Domain Name Service*), kako bi se onemogućio pristup uslugama za dio ili cijelu mrežu. U tom slučaju mreže zaraženih računala, tzv. *botnetovi* predstavljaju veliku opasnost koja nadilazi zlonamjerne poruke jer mogu ugroziti čitavo funkcioniranje interneta.

Napadači koji upravljaju velikim mrežama zaraženih računala, tzv. *botnetovima* od njih mogu imati veliku financijsku dobit upravo zbog mogućnosti napada s velikog broja računala u različitim mrežama pa je jedna od čestih primjena mreže zaraženih računala, tzv. *botneta* distribuirani napad uskraćivanjem usluge (*Distributed Denial of Service, DDOS*). Uspješan DDOS ciljanu će uslugu na neko vrijeme učiniti u potpunosti nedostupnom što može biti zanimljivo konkurenciji pa je jasno zašto napadači od toga mogu imati novčanu korist.

Podsjetimo, zloćudni kod pokrenut na računalu žrtve preduvjet je i za napade te vrste pa je motivacija za izradu takvog koda i u tom slučaju jasna.

9.2.4. NAPLATA OTKUPNINE OD ŽRTVE

Ova vrsta ugroze postala je vrlo raširena u posljednjih nekoliko godina i većinom je usmjerena na osobna računala korisnika iako postoje i inačice razvijene za pametne telefone. Zloćudni programi te vrste nazivaju se engl. *ransomware,* a cilj im je šifriranje podataka na korisničkom računalu kako im korisnik više ne bi mogao samostalno pristupiti. Jednom šifrirane podatke nemoguće je dešifrirati bez odgovarajućeg ključa za šifriranje koji je u vlasništvu napadača. Nakon šifriranja napadač kontaktira žrtvu te traži otkupninu za podatke kako bi žrtvi otkrio ključ za dešifriranje. Naravno, plaćanjem otkupnine nema jamstva da će napadač uistinu žrtvi i otkriti ključ i da će žrtva doista moći vratiti svoje podatke.

Kao i kod prethodnih primjera, zloćudni programi usmjereni na osobna računala kornsika, engl. *ransomware*, većinom se prenose porukama, najčešće e-poštom, gdje se metodama internetske krađe podataka (engl. *phishing*) pokušava žrtvu natjerati da pokrene zloćudni kod koji joj je poslan kao privitak poruke. Ukoliko žrtva nije na oprezu, pokrenut će privitak koji će instalirati zloćudni program na računalo. Privitci u kojima se nalazi zloćudni kod ne moraju biti izvršne datoteke (npr. .exe), nego često iskorištavaju postojeće ranjivosti drugih alata na računalu. Primjerice, čest je slučaj gdje se zloćudni kod šalje kao dio datoteke PDF. Prilikom pokretanja alat za

pregled dokumenta u formatu PDF učitava dokument i pritom zbog vlastitih ranjivosti izvrši zloćudni kod koji se nalazi prikriven u dokumentu PDF.

Uz navedene korake napada treba naglasiti i da napadači često koriste metode društvenog inženjeringa, pa tako primjerice računovodstvene odjele tvrtki zasipaju e-poštom koja sadrži privitke koji izgledaju kao računi čime se povećava vjerojatnost da će žrtva doista otvoriti privitak i pokrenuti zloćudni kod.

9.2.5. ŠPIJUNAŽA

Danas je većina poslovanja tvrtki u potpunosti digitalizirana i nalazi se na poslužiteljima u lokalnoj mreži ili, djelomično, u dijeljenom oblaku. Zaposlenici tvrtke, ovisno o ovlastima, imaju određeni pristup povjerljivim dokumentima i podatcima nužnim za poslovanje tvrtke. Ako napadač može ostvariti pristup samo jednom računalu zaposlenika, potencijalno može kompromitirati cijelu mrežu poduzeća.

Primjerice, zamislimo tvrtku koja se bavi proizvodnjom i određeni zaposlenici sudjeluju u dizajnu novih proizvoda i patentiranja. Konkurentsko poduzeće dobilo bi veliku tržišnu prednost ako bi mogla doći u posjed dokumentacije i patentnih prijava novih proizvoda. Ukoliko napadač može doći do takvih podataka, razumljivo je zašto bi mu konkurentska tvrtka htjela platiti informacije pa je opravdan motiv napadača za provalom u takve poslovne sustave. Kao i kod ostalih vrsta zloćudnih programa, i ovdje je najčešći prvi korak slanje poruke u svrhu krađe podataka koja sadrži zloćudni kod i tipično sadrži metode društvenog inženjeringa. Nakon instalacije zloćudnog koda na računalo žrtve, napadač dobiva ovlast žrtve i može pristupati svim informacijama kao i žrtva.

Godinama je zabilježeno podosta slučajeva industrijske špijunaže prema navedenim obrascima, no poduzeća često ne žele potvrditi takve napade kako bi sačuvale ugled. Ipak, postoje primjeri u kojima su na taj način, navodno, napadači iz Kine ili Sjeverne Koreje provaljivali u sustave tehnoloških tvrtki iz Japana kako bi došli do korisnih poslovnih informacija.

9.2.6. ELEKTRONIČKO RATOVANJE (CYBER RATOVANJE)

Najsloženiji zloćudni programi napravljeni su kako bi se špijunirale druge države i sustavi ili nanijela šteta industrijskim i vojnim sustavima od kritične važnosti. Iako je potvrđeno postojanje takvih složenih zloćudnih programa, nikada nisu potvrđeni autori kao ni tko ih je financirao, što je očekivano s obzirom na razinu i ciljeve takvih programa. Pretpostavka je da su ih razvili specijalizirani timovi koji rade za države s

obzirom da se troškovi razvoja takvih programa procjenjuju u milijunima dolara, a indikativne su i mete koje takvi programi ciljaju.

Najpoznatiji primjer takvog zlćudnog programe jest crv Stuxnet (Holloway, 2015) koji je bio najsloženiji zlćudni program u povijesti. Napravljen je da po lokalnoj mreži pronalazi Siemensove kontrolere u proizvodnom pogonu te preuzme kontrolu nad njima kako bi onesposobio ili potpuno uništio fizičku infrastrukturu kojom se njima upravlja. Indikativno je to da su se Siemensovi kontrolori koristili u nuklearnim pogonima Irana i da je na te pogone izveden uspješan napad korištenjem upravo crva Stuxnet pa se može samo pretpostavljati tko stoji je omogućio njegov razvoj. Nakon Stuxneta razvijeno je još nekoliko naprednijih i manje naprednih izvedenica koje je cilj bio špijunaža, no do danas nisu potvrđeni autori. Zanimljivo je da je jedna izvedenica i 2018. godine otkrivena na poslovnoj mreži poznate antivirusne tvrtke Kaspersky Labs (Kaspersky Labs) koja je dulje vremena uopće nije primijetila.

Vektori napada kod takvih vrsta zlćudnoga koda različiti su iako ponovno prednjači **metoda** internetske krađe podataka, engl. *phishing method*, uz društveni inženjering. Kod takvih složenih programa, nakon inicijalne zaraze jednog računala u lokalnoj ili štićenoj mreži, zlćudni programi dalje se sami šire mrežom i na taj način dolaze do novih računala s traženim podacima ili upravljačkim sklopovljem. Primjerice, prema nekim izvorima, pretpostavlja se da Stuxnet nije pokrenut u iranskom nuklearnom pogonu metodom internetske krađe podataka (engl *phishing*), već da se nalazio na USB štapiću koju je netko ostavio blizu nuklearnog pogona. Žrtva je tada uzela USB štapić i uključila je u računalo u zaštićenoj mreži kako bi provjerila podatke na memoriji. No, već nakon uključivanja memorije u računalo, Stuxnet je pokrenut i mogao se dalje samostalno širiti mrežom u potrazi za Siemensovima kontrolorima.

9.2.7. NAPLATA SMS PORUKA ZA USLUGE S DODANOM VRIJEDNOSTI

Dosadašnji primjeri uglavnom su se usmjeravali na računala i sustave, no nikako se ne smije zanemariti prijetnja zlćudnih programa pametnim telefonima. Zapravo, posljednjih nekoliko godina razvija se više zlćudnih programa za pametne telefone nego za tradicionalna računala. Pametni telefoni lako su dostupni, godinama se sve više i više koriste, a korisnici ih još uvijek ne shvaćaju kao moćne uređaje na kojima se, uz korisne aplikacije, može izvoditi i zlćudni kod.

Napadačima su pametni telefoni zanimljivi jer imaju nekoliko specifičnosti u usporedbi s računalima. Prije svega, tu je mogućnost izravne naplate telekomunikacijskog operatera pa napadač može vrlo brzo doći do financijske koristi. Najčešći primjer zarade jest slanje SMS poruka za usluge s dodanom vrijednosti koje su u izravnom ili neizravnom vlasništvu napadača. Na taj način napadač se koristi pametnim

telefonom žrtve kako bi u pozadini slao SMS poruke na vlastitu uslugu i time zarađivao novac, a žrtva uopće nije svjesna slanja poruka. Tipičan scenarij za takvu ranjivost jest da napadač iskoristi postojeću legitimnu aplikaciju u koju ubacuje dio programskog koda za slanje SMS poruka svojoj usluzi. Uobičajeno će napadač preuzeti legitimnu aplikaciju s neke od trgovina aplikacija, provesti proces reverznog inženjerstva kako bi došao do izvornog koda aplikacije i u taj kod ubaciti svoj maliciozni dio koda. Nakon toga aplikacija se ponovno pakira i nudi korisnicima besplatno ilegalnim trgovinama ili sličnim mehanizmima za dijeljenje sadržaja (npr. servisi *torrent*). Korisnicima je primamljiva činjenica da je ta aplikacija sada besplatna, dok bi je u legalnoj trgovini trebali kupiti. Zato pristaju na preuzimanje neprovjerene aplikacije s alternativnih izvora čime se dovode u ugrozu? Po instalaciji takve aplikacije korisnici je mogu uobičajeno upotrebljavati, no nisu svjesni da aplikacija upotrebom iz pozadine šalje skupe SMS poruke na napadačevu uslugu. Danas je takva vrsta ugroze dominantna na uređajima s operacijskim sustavom Android, dok je prvi zabilježeni slučaj takvog zloćudnog koda zabilježen kod operacijskog sustava *Symbian* u obliku igre *Mosquito* (Peikari, Fogie, Read i Hettel, 2004) 2007. godine.

Uz izravnu naplatu pametnim telefonima ne treba zanemariti ni činjenicu da pametni telefoni o nama prikupljaju velike količine podataka kao što su navike u kretanju, upotreba telefona, kontakti, česte lokacije koje posjećujemo i slično pa kao takvi napadačima predstavljaju dobar izvor osobnih podataka o korisnicima. Dodatna je mogućnost i instalacija zloćudnih programa čiji je cilj nadzor uređaja i drugih aplikacija na pametnom telefonu kao što su bankarske aplikacije ili aplikacije za komunikaciju koje otvaraju put za daljnje napade i financijsku korist napadačima. Očekuje se da će se broj prijetnji na pametnim telefonima i dalje povećavati te da će prijetnje postajati sve složenije pa je potrebno obratiti pozornost na izvore iz kojih se aplikacije preuzimaju.

9.3. VRSTE ZLOĆUDNOG KODA

Zloćudni programi vremenom se mijenjaju kako bi mogli ostati neotkriveni antivirusnim alatima. Međutim, postojeće zloćudne programe moguće je klasificirati prema funkcionalnostima i načinu širenja. Pri tome treba reći da se neki primjeri ne mogu jednoznačno klasificirati jer se, evoluirajući, šire na više načina, a ovisno o namjeni mogu imati i različite funkcionalnosti.

Prema tome, zloćudne programe možemo dijeliti na sljedeće kategorije s navedenim glavnim značajkama:

- ✓ računalni virusi – ne šire se samostalno između računala

- ✓ računalni crvi – šire se samostalno između računala
- ✓ trojanski konji – predstavljaju se kao korisni programi
- ✓ *rootkitovi* – napadaču omogućuju kontrolu nad cijelim sustavom žrtve
- ✓ *ransomware* – šifriraju podatke žrtve
- ✓ *spyware* – nadziru aktivnosti žrtve.

9.3.1. RAČUNALNI VIRUSI

Računalni virusi vrsta su zloćudnog koda koji se samostalno izvršava kako bi nanio štetu sustavu na kojemu se pokreće. Virusi se često ugrađuju u legitimne datoteke kako bi se pokrenuli kada korisnik pokrene i datoteku, primjerice sliku, dokument u formatu PDF ili .doc. Često se dodaju na početak ili kraj legitimne datoteke kako bi se neprimjetno pokrenuli pa će se tako virus izvršiti, a ostatak legitimne datoteke korisniku će se uobičajeno prikazati kako on ne bi posumnjao na moguću zarazu.

Glavno je svojstvo virusa da se nakon prvog pokretanja sami pokušavaju replicirati unutar računala ili sustava na kojima su pokrenuti, no u pravilu se ne šire samostalno između računala. Replikacija se može provesti tako da virus prije svega utvrdi na kojem je operacijskom sustavu pokrenut, pa prema tome „zna" koje sve datoteke postoje i gdje se sve može ubaciti. Nadalje, pretražuje sustav s poznatim datotekama i redom se dodaje u njih kako bi se zaraza proširila. Ovisno o metama virusa postoji nekoliko podvrsta koje su opisane u nastavku.

Prva i najstarija vrsta su virusi koji ciljaju datotečni sustav. Takvi će se virusi ubacivati u sve datoteke kako je opisano. Poseban je problem da, ako takvi virusi dospiju u memoriju računala, tada se mogu zapisati u svaku izvršnu datoteku koja se pokreće i na taj se način mogu širiti i na ostale programe koji se izvode na napadnutom računalu. Primjer jednog od prvih ovakvih virusa je Jerusalem (MalwareWiki, 2017).

Sljedeća su vrsta virusi koji se ubacuju u *boot* sektore računala. *Boot* sektori dio su memorije, odnosno diska računala koji se učitavaju u memoriju pokretanjem računala i očitavanjem vanjskog medija, kao što je USB štapić (USB *stick*, USB memorija). Oni prilikom pokretanja daju uputu sustavu koje programe treba učitati u memoriju. Ako se virus ubaci u *boot* sektor, to znači da će se on učitati u memoriju računala kod pokretanja čime će biti u stanju nanijeti znatno veću štetu i bit će ga teže ukloniti. Kao primjer prvog takvog virusa navodi se Michelangelo. Svojevrsna su nadogradnja virusa u *boot* sektorima virusi u glavnom *boot* zapisu (*Master Boot Record, MBR*) kojim se određuje kako će se pokrenuti računalo i iz kojih će se *boot* sektora podizati sustav i programi. Takvi su virusi u stanju nanijeti još veću štetu jer će moći

utjecati na pokretanje ostalih programa ili učitavanje čitavih diskovnih particija računala. Jedan od najstarijih primjera MBR virusa je NYB (Symantec, 2000).

Posljednja općenita vrsta virusa su višepartitni virusi. Nazivaju se tako jer se ne ograničavaju samo na datoteke ili samo *boot* sektore, već se pokušavaju replicirati i u datotečni sustav i u *boot* sektore. Zbog toga ih je posebno teško ukloniti jer će se brisanjem virusa iz datotečnog sustava zaraza ponovno proširiti iz *boot* sektora ili MBR-a i obratno. Primjer takvog virusa je Tequilla (F-Secure, 2018).

Uz navedene općenite vrste virusa, možda i najčešća specifična vrsta su makro virusi (engl. *macro*). Pojam makro označava automatizaciju datoteka paketa Microsoft Office kao što su Word, Excel, Powerpoint i Access dokumenti. U odgovarajućim alatima ugrađene su funkcionalnosti koje korisnicima omogućuju pisanje naredbi i koda kako bi se olakšao rad s tim dokumentima. Međutim, u alatima su otkrivene i otkrivaju se određene ranjivosti pa je umjesto legitimnih naredbi moguće ubaciti zlonamjerni kod koji će se izvršiti pokretanjem odgovarajućeg dokumenta. Pri tome će kod imati ovlast programa koji ga je pokrenuo pa će takav makro virus moći napraviti značajnu štetu i izvan okvira alata paketa Microsoft Office. Jedan od najpoznatijih makro virusa je W97M.Melissa (Panda Security, 2013).

Govoreći o računalnim virusima, treba spomenuti i svojstvo polimorfizma. Naime, antivirusni alati, o kojima će biti više riječi kasnije u tekstu, zloćudne programe otkrivaju na principu „otiska". Svaki zloćudni program imat će jedinstven „otisak" koji će odgovarati zapisu izvršnog zloćudnog koda. Postojanjem baze takvih otisaka antivirusni će program u datotečnom sustavu i memoriji računala pretraživati pojavu poznatih otisaka kako bi utvrdio pojavnost zloćudnog programa. Zato je važno svojstvo polimorfizma kod kojeg će zloćudni program replikacijom mijenjati svoj kod kako bi ga bilo teže detektirati. Danas su gotovo svi virusi polimorfni u tom smislu i to je jedan od razloga zašto treba redovito ažurirati antivirusne programe koji tada preuzimanju nove „otiske" izmijenjenih virusa. Glede prikrivanja virusa čest je slučaj i da virusi odmah nakon pokretanja pokušavaju detektirati postoji li na računalu antivirusni program i koje je vrste. Ukoliko postoji, virus će ga pokušati deaktivirati i to često na način da izgleda kao da je antivirusni program pokrenut i ispravan kako korisnik ne bi posumnjao na zarazu.

9.3.2. RAČUNALNI CRVI

Računalni crvi zloćudni su programi čija je glavna karakteristika da se mogu samostalno širiti mrežom. Izuzev načina širenja u ostali su segmentima vrlo slični računalnim virusima pa se u nekim kategorizacijama navode i kao podvrsta virusa. No, za razliku od virusa crv se ne ubacuje u datoteku kako bi ga korisnik ili sustav

pokrenuo, već ima vlastite mehanizme širenja koji ne ovise o izvanjskim akcijama. Upravo zbog te samostalnosti možda su i najopasnija vrsta zloćudnog koda jer su u stanju brzo preplaviti i zaraziti velik broj računala u mreži. Gledajući unazad, treba reći da prvi crvi nisu razvijeni s malicioznim namjerama, već na temelju ideje da se omogući automatizirano ažuriranje programa na računalima. Tako bi se „legitimni" crv pustio u mrežu u kojoj bi sam tražio računala sa starijom inačicom nekog programa, pokrenuo se na takvim računalima i ažurirao program.

Proces je širenja crva sljedeći. Slično kao i virus, crv prvo detektira sustav na kojem se nalazi i pokušava iskoristiti poznate ranjivosti. Nakon uspješnog iskorištavanja ranjivosti, počinje se replicirati i tražiti nove mete. Nove mete pronalazi u kontaktima elektroničke pošte, popisu računala u lokalnoj mreži, tablicama usmjeravanja ili čak slučajno generiranim IP adresama. Prema načinima širenja moguće je razlikovati crve (Symantec, 2016):

- ✓ *e-mail* crvi – šire se elektroničkom poštom, najčešće kao privitak; uz to, eventualno se koriste i metode društvenoga inženjeringa kako bi meta vjerovala pošiljatelju i lakše otvorila privitak s crvom
- ✓ internetski crvi – pretražuju mrežu kako bi identificirali računala s poznatim ranjivostima (npr. identifikacijom verzije operacijskog sustava) i otvorenim vratima te na taj način ulaze u druga računala
- ✓ mrežni crvi – pronalaze dijeljenu pohranu (npr. mrežne diskove, pohranu mrežnog pisača i slično) na koju se kopiraju.

Bez obzira kako su mete pronađene, odgovarajućim se kanalom metama šalju paketi koji ponovno sadrže crva čime cijeli postupak počinje iznova.

Osim širenja glavna funkcionalnost crva jest nanošenje štete računalu na kojemu je pokrenut. Tu je crv vrlo sličan virusu pa tako može brisati ili mijenjati datoteke, prikupljati različite dostupne informacije o korisniku ili, u najgorem slučaju, preuzeti računalo i omogućiti napadaču potpunu kontrolu otvaranjem sustava kroz tzv. *backdoor*. Ukoliko se otvori takav ulaz u računalo, ono postaje dio napadačevog *botneta* i kasnije može biti iskorišteno za različite vrste napada, primjerice napade uskraćivanjem usluge, slanje neželjenih poruka ili upotrebom procesorskih resursa računala. Posljednje je posebno zanimljivo jer postoje i legitimni programi kojima korisnik može dopustiti upotrebu vlastitih resursa, primjerice projekt SETI@home (https://setiathome.berkeley.edu, preuzeto 15. 10. 2018.). U kontekstu zloćudnih crva s rastom popularnosti virtualne valute Bitcoin napravljeni su crvi koji su se pokretali na računalima i rudarili Bitcoinove kako bi napadaču osigurali financijsku dobit.

Uz sve navedeno i s obzirom na činjenicu da su crvi doista najnapredniji zloćudni programi, treba razmisliti i o problemima na koje crvi nailaze. Prije svega,

njihovo agresivno širenje mrežom može biti i loše za njih jer postavlja se pitanje kako spriječiti da crv „prepiše" sam sebe, odnosno više puta zarazi isto računalo? Očigledno, moraju postojati mehanizmi za kontrolu je li crv već pokrenut na nekom računalu što može biti složeno ukoliko je cilj crva da ga bude teško otkriti, čak i „vlastitoj kopiji". Uz to, složeni crvi moraju sadržavati programsku logiku koja će moći detektirati ranjivosti kao i logiku potrebnu za širenje unutar i izvan računala. Zbog svega toga postoji mogućnost da crv jednostavno postane prevelik čime bi se otežalo širenje i olakšalo njegovo prepoznavanje detekcij, a takav bi crv izgubio smisao.

U nastavku su izloženi važniji primjeri računalnih crva kako bi se pojasnile njihove specifičnosti.

Vjerojatno je prvi crv Morris Worm (Bortnik, 2013) koji je napisao student Sveučilišta Cornell Robert Tappan Morris i pokrenuo ga 2. 11. 1988. godine. Prema autoru cilj izrade crva bio je mjerenje veličine interneta. Međutim, problem je bio u mehanizmu širenja jer crv nije ispravno provjeravao je li već pokrenut na računalu pa se više puta pokretao na istom računalu što je u konačnici rezultiralo uskraćivanjem usluge. S obzirom da je crv zahvatio veći broj računala i poslužitelja, slučaj je dobio i sudski epilog u kojem je autor osuđen. Šteta koju je Morris Worm napravio procijenjena je na 1 do 10 milijuna dolara, a prema izvještajima zarazio je 10 % računala s operacijskim sustavom Unix spojenih na internet i oko 2000 računala u prvih petnaest sati od pokretanja.

Povijesno gledano, jedan od prvih crva koji je počinio štetu na globalnoj razini je Nimda (Ducklin, 2011) otkriven 2001. godine i vjerojatno napravljen u Kini. Budući da je koristio više metoda širenja, vrlo se brzo proširio mrežom. Jedan je od prvih koji se mogao pokrenuti bez da korisnik otvori poruku elektroničke pošte u kojoj se nalazio i prvi koji je modificirao mrežne stranice da nude njegove kopije za preuzimanje. Općenito, to je jedan od najrazornijih računalnih crva ikad otkrivenih i u svakom slučaju prvi takve vrste. Napadao je operacijski sustav Microsoft Windows i širio se na sljedeće načine: e-poštom, preuzimanjem s mrežnih stranica, lokalnom mrežom pomoću dijeljene memorije, iskorištavajući ranjivosti MS IIS servera ili *backdoorom* kreiranog od strane drugih crva – Code Red i Sandworm. Kada se jednom pokrenuo na računalu, zarazio je datoteke slično kao i virus, ali se nije dodavao u izvršne datoteke, nego se kopirao s imenom izvršne datoteke, a originalnu je datoteku kopirao u sebe. Kad bi korisnik pokušao pokrenuti zaraženu datoteku, prvo bi se pokrenuo crv, a zatim originalni program. Originalna verzija Nimde zarazila je gotovo 160 000 sustava. Nakon prve inačice sve do danas razvijene su evoluirane inačice crva Nimda koje još uvijek mogu načiniti štetu računalima i sustavima, a mnogi noviji crvi koriste mehanizme koje je prve koristila Nimda.

Govoreći o računalnim crvima, neizbježno je spomenuti do danas najsloženiji crv – Stuxnet (Holloway, 2015) o kojem je bilo riječi u uvodnom dijelu. Otkriven je u lipnju 2010. godine i prvi je crv koji je dizajniran za napad na Siemensove programabilne logičke kontrolere (PLC). Širio se operacijskim sustavom Microsoft Windows, a zarazom računala tražio je kontrolira li računalo na kojem se nalazi neki PLC. Pisan je u nekoliko različitih programskih jezika i neuobičajeno je velik za zloćudni program – oko pola Mb. Ukoliko računalo na kojem je pokrenut ne zadovoljava zahtjeve u smislu kontrole nekog PLC-a, crv postaje inertan i koristi mjere zaštite kako širenjem ne bi obrisao sam sebe na drugom računalu. Između ostalog, sadrži i kompleksnu funkcionalnost koja služi za slanje lažnih senzorskih signala kako se inficirani sustav ne bi isključio ako otkrije neuobičajeno ponašanje. Specifičnost je Stuxneta da je prilikom širenja na operacijski sustav Windows koristio čak četiri tzv. *zero-day* ranjivosti. *Zero-day* ranjivosti su ranjivosti koje prethodno nisu otkrivene, pa za njih ni ne postoje sigurnosne zakrpe što ih čini vrlo rizičnima. Uporaba čak četiriju takvih ranjivosti kod Stuxneta, uz to prvi put u povijesti kod bilo kojeg zloćudnog programa, svakako indicira da je iza njegove izrade tim stručnjaka sa značajnim budžetom i jasnom namjerom kompromitacije PLC-ova. Zanimljivo je i da Stuxnet nije ciljao bilo koje Siemensove PLC-ove, već je imao ugrađenu kontrolu za identifikacijom samo PLC-ova na koje su povezani uređaji za pretvorbu frekvencije jednog od dvaju određenih proizvođača. Dodatno, napadao je samo one sustave koji rade na frekvencijama između 807 i 1210 Hz. Ukoliko je tako, Stuxnet izvršava napad periodičnim mijenjanjem frekvencije na 1410 Hz, 2 Hz i 1064 Hz što utječe na rotacijsku brzinu kontroliranih motora. Iz toga je također očigledno da je Stuxnet razvijen ciljano kako bi napadao usku skupinu uređaja kontroliranih PLC-ovima. Studija širenja pokazala je da su Iran (58,85 %), Indonezija (18,22 %) i Indija (8,31 %) države na koje je Stuxnet najviše utjecao te je prouzročio značajnu štetu iranskom nuklearnom programu skupljajući informacije o industrijskim sustavima i uništavajući centrifuge zbog prebrzog okretanja. Prema izvještajima uništio je petinu iranskih nuklearnih centrifuga, a u procesu je zarazio 200.000 računala.

9.3.3. TROJANSKI KONJI

Trojanski konji specifični su po tome što se korisnicima predstavljaju kao legitimni i korisni programi. Od tuda i ime trojanski konj, prema drvenom konju iz grčke mitologije pomoću kojeg su Grci ušli u grad Troju. Trojanski konji najčešće se šire nekom vrstom društvenog inženjeringa, tj. ne izvršavaju se ni ne šire samostalno. Čest je slučaj u kojemu se nekom od metoda društvenog inženjeringa korisnicima dostavi videozapis, no da bi ga otvorili, moraju preuzeti „novu inačicu" programa za reprodukciju videozapisa u kojemu se zapravo nalazi zloćudni program. Nakon infiltriranja

u sustav cilj je trojanskih konja instaliranje različitih zloćudnih funkcija, često otvaranje *backdoora* kako bi napadač dobio potpunu kontrolu nad računalom. Treba reći i da se trojanski konji ne repliciraju, kao primjerice virusi, već ih pokreće isključivo prevareni korisnik koji ih smatra legitimnim programima.

Jedan od najpoznatijih primjera trojanskog konja je Zeus, prvi puta identificiran 2007. (Kaspersky Labs, 2018). Zeus je inicijalno napravljen za krađu bankovnih podataka u čemu je bio uspješan u svojoj prvoj inačici. Kao i kod ostalih zloćudnih programa, i Zeus je evoluirao pa tako danas njegove inačice služe za instalaciju *ransomware* programa.

9.3.4. ROOTKITOVI

Rootkit je tradicionalni naziv za zloćudne programe koji napadaču omogućuju potpunu kontrolu zaraženog računala. U literaturi se navode kao posebna vrsta zloćudnih programa, no iz prethodnog teksta razvidno je da postoje i virusi, crvi i trojanski konji koji imaju funkcionalnosti rootkita.

Rootkitove možemo razlikovati prema ovlastima koje imaju prilikom infiltracije u sustav. *Rootkit* korisničke razine djeluje pod ovlastima korisnika uz ostale korisničke aplikacije, dok *rootkit* jezgrene razine djeluje na najnižoj razini s najvišim privilegijama operacijskog sustava. Tako može dodavati ili mijenjati dijelove operacijskoga sustava čime se napadačima otvaraju velike mogućnosti i potpuna kontrola zaraženog računala.

Instalacija *rootkita* može se provesti upotrebom nekog drugog zloćudnog koda, kao primjerice trojanskog konja, virusa ili crva. Nakon instalacije, moguće je prikriti napad i zadržati pristup sustavu. Otkrivanje i otklanjanje *rootkita* složeno je zbog njegove mogućnosti mijenjanja programa i postavki operacijskoga sustava s ciljem prikrivanja.

9.3.5. RANSOMWARE

Ransomware je vrsta zloćudnog koda koja šifrira podatke na žrtvinom računalu i traži novčanu otkupninu kako bi ih se dešifriralo. Popularnost je te vrste zloćudnih programa porasla od kraja 2013. zbog pojave kriptovaluta koje su olakšale plaćanje otkupnine, odnosno otežale ulazak u trag napadačima. *Ransomware* djeluje na način da šifrira žrtvine podatke. Žrtva će moći dešifrirati podatke jedino ako dobije pristup korištenom ključu za šifriranje, koji je u vlasništvu napadača. Nakon plaćanja otkupnine napadač bi žrtvi trebao dostaviti ključ što često nije slučaj pa je upitno ima li smisla uopće plaćati otkupninu.

Ransomware se najčešće širi trojanskim konjima koji nakon instalacije provode šifriranje i korisnicima ispisuju poruku u zaključanim podacima i upute za plaćanje otkupnine.

Jedan od prvih *ransomware* programa bio je AIDS Trojan (KnowBe4, 2018) davne 1989. godine, no zbog greške u izradi bilo je jednostavno dešifrirati podatke bez plaćanja otkupnine. Noviji je primjer CryptoLocker (Kaspersky, 2018) koji se pojavio u rujnu 2013. godine i napadao računala s operacijskim sustavom Windows šifrirajući podatke na tvrdom disku 2048-bitnim RSA ključem. Specifičan je po tome da je prvi koristio valutu Bitcoin za naplatu, a procjenjuje se da je uzrokovao štetu od 27 milijuna dolara. Još jedan noviji i poznati *ransomware* je WannaCry (Palmer, 2018), napad je počeo u svibnju 2017. i trajao četiri dana, meta su mu bila računala s operacijskim sustavom Windows, šifrirao je podatke i tražio isplatu u kriptovaluti Bitcoin, a poseban je po tome što je imao mehanizam kojim se mogao samostalno širiti. U medijima je dosta popraćen pa je tako bilo objavljeno kako je uzrokovao zastoje u zračnom prometu i velike štete u industrijskim pogonima.

9.3.6. SPYWARE

Cilj *spyware* programa je, kako im ime govori, nadzor korisnika. Cilj im je neprimjetno zaraziti računalo i u pozadini pratiti što korisnik radi, koje usluge koristi i s kojim podatcima rukuje. Prikupljeni podatci nadalje se mogu koristiti za dodatne napade na korisnika ili njegov krug kontakata. Uz to, *spyware* posjeduje mehanizme za periodino ili stalno slanje prikupljenih podataka napadaču koji mogu biti više ili manje složeni.

Što se tiče širenja, *spyware* se bitno razlikuje od virusa ili crva zato što mu često nije cilj zaraziti što više računala, već bira određene mete. Tipično se instalira trojanskim konjem koji najčešće uključuje neku vrstu društvenog inženjeringa.

Jednostavan i netipičan primjer *spyware*a takozvani su prateći kolačići za mrežna sjedišta (engl. *tracking cookies*). Cilj im je postaviti kolačić u preglednik korisnika kako bi se pratilo koja sve mrežna sjedišta posjećuje te koliko i kako ih koristi. Nešto tipičniji *spyware* instalirat će se na računalo i imati funkciju praćenja pokreta miša i unosa na tipkovnici pa se takvi programi nazivaju *keyloggeri*. U posljednje vrijeme zabilježen je *spyware* koji na računalu žrtve podiže poslužitelj za udaljeno upravljanje i nadzor računala. Kako ne bi bilo zabune, postoje brojni legitimni alati za nadzor i udaljeno upravljanje računalom kao što su TeamViewer i VNC (engl. *Virtual Network Computing*). No, ukoliko ih napadač pokreće i njime se koristi bez znanja korisnika upotrebom nekog zlćudnog programa, onda im je cilj svakako zlonamjeran. Primjeri takvih zlćudnih programa, ponajprije usmjerenih na financijske institucije, su: Dridex, Neverquest i Gozi (Keshet, 2017).

9.4. ZAŠTITA OD ZLOĆUDNIH PROGRAMA

Kako bi se korisnici zaštitili od zlođudnih programa, prije svega potrebno je sažeti kojim sve kanalima zlođudni programi mogu ući u računalo. Konačni cilj zaštite jest da se svi identificirani kanali odgovarajući zaštite, što najčešće i rade antivirusni programi. Prema gornjem tekstu i analizi postojećih primjera zlođudnih programa, možemo identificirati navedene izvore zaraze:

- ✓ e-pošta – zlođudni programi tipično dolaze kao privitak pošte ili se korisnika usmjerava na mrežno sjedište s kojega se preuzima zlođudni program
- ✓ usluge trenutnog poručivanja i kratkih poruka – kao i kod e-pošte, posebice na pametnim telefonima, poruke mogu biti upućene i nekom od usluga trenutnog poručivanja (Whatsapp, Viber, Skype…)
- ✓ društvene mreže – kompromitacijom društvenih mreža moguće je koristiti metode društvenog inženjeringa i navesti korisnike na preuzimanje trojanskih konja izravno s mrežnog sjedišta
- ✓ prijenosni mediji – virusi se najčešće šire tim načinom jer se mogu pokrenuti prilikom čitanja prijenosnog medija bez intervencije korisnika
- ✓ otvorena mrežna vrata – crvi se često šire identifikacijom otvorenih vrata na računalu,
- ✓ ranjive mrežne usluge na računalu – crvi skeniraju računala kako bi identificirali zastarjele inačicr usluga na računalu koje onda iskorištavaju za zarazu
- ✓ preuzimanjem i instalacijom neprovjerenih programa s interneta – na računalima i pametnim telefonima ukoliko nema verifikacije proizvođača.

Većinu navedenih kanala mogu nadzirati antivirusni programi. Tako će kvalitetni programi nadzirati sve poruke koje korisnik dobiva prije otvaranja privitaka te upozoravati korisnika pri preuzimanju datoteka i programa s interneta. Antivirusni programi, ovisno o izvedbi, rade na dva načina. Prvi je način skeniranje ulaza u računalo i samog računala kako bi se otkrilo postojanje „otisaka" zlođudnih programa, kako je prethodno opisano. Preduvjet je za to da je antivirusna tvrtka identificirala neki „otisak" kao zlođudni program zbog čega je bitno periodično ažurirati bazu zlođudnih programa u okviru antivirusnog alata. Međutim, na taj se način neće moći otkriti nove prijetnje koje nisu identificirane kao zlođudni programi. Zato je drugi način rada naprednijih alata nadzor sustava i programa koji se izvode kako bi se utvrdili rizični obrasci. Tako će, primjerice, biti sumnjiv program koji pristupa resursima koji mu zapravo ne trebaju, podacima drugih programa ili aplikacija koji otvara mrežne konekcije iz nejasnih razloga i slično. Sustavi koji imaju takvu funkcionalnost

nadzora računala na toj razini ubrajaju se u domenu sustava za otkrivanje uljeza (engl. *intrusion detection system*). Mogući nedostatak takvih sustava jest da neće moći uvijek prepoznati je li neki program doista prijetnja, ali i da će nekada legitimne programe označiti prijetnjom. Kod takvih programa često se daje obavijest korisniku koji sam treba odlučiti što napraviti, što često nije dobra praksa jer korisnici u pravilu nemaju dovoljno tehničkih znanja da bi mogli razumjeti što podaci koje im takav sustav nudi zapravo znače.

Gledano s motrišta krajnjeg korisnika koji želi koristiti sve dostupne usluge, potrebno je reći kako rizik uvijek postoji i nije moguće imati potpuno siguran sustav. Ta je tvrdnja posebice značajna zbog spomenutih *zero-day* ranjivosti koje svaki sustav ima, no još nisu otkrivene. Ukoliko ih napadač otkrije prije proizvođača operacijskoga sustava ili pojedinih aplikacija, iskorištavanje ranjivosti vrlo je izgledno, često bez obzira na prisutnu zaštitu u smislu antivirusnih alata.

S obzirom da je najčešći vektor napada još uvijek internetska krađa podataka, engl. *phishing,* s nekom vrstom društvenog inženjeringa, korisnici bi trebali biti izrazito sumnjičavi kada dobivaju poruke sumnjivog sadržaja i uvijek provjeriti istinitost tih poruka prije nego li postupe prema uputama i odaju vlastitu zaporku ili instaliraju potencijalno zloćudni program. Što se tiče mrežnih prijetnji, potrebno je redovito i što prije ažurirati nove zakrpe, odnosno nadogradnje operacijskog sustava i aplikacija koje koriste jer je cilj zakrpa, između ostalog, doraditi eventualno pronađene sigurnosne propuste. Tako će se onemogućiti iskorištavanje pronađenih ranjivosti čime se značajno može spriječiti djelovanje zloćudnih programa kao što su crvi koji se šire mrežom.

Konačno, korisnici ne bi smjeli biti lakovjerni glede ponuda besplatnih sadržaja, programa i medija koje mogu preuzeti s ilegalnih servisa kao što je *torrent* ili s ilegalnih mrežnih sjedišta koja nude besplatne inačice programa i alata.

9.5. LITERATURA

Bortnik, S. (6. studenog 2013). *Five interesting facts about the Morris worm*. Preuzeto s https://www.welivesecurity.com/2013/11/06/five-interesting-facts-about-the-morris-worm-for-its-25th-anniversary/, 15.8.2018.

Ducklin, P. (16. rujna 2011). *Memories of the Nimda virus*. Preuzeto s https://nakedsecurity.sophos.com/2011/09/16/memories-of-the-nimda-virus/, 15.8.2018.

Holloway, M. (16. srpnja 2015). *Stuxnet Worm Attack on Iranian Nuclear Facilities*. Preuzeto s http://large.stanford.edu/courses/2015/ph241/holloway1/, 15.8.2018.

Kaspersky. (2018). *Kaspersky web site online*. Preuzeto s https://www.kaspersky.com, 15.8.2018.

Keshet L. (25. siječnja 2017). *Anatomy of an hVNC Attack*. Preuzeto s https://securityintelligence.com/anatomy-of-an-hvnc-attack/, 15.8.2018.

KnowBe4: AIDS Trojan or PC Cyborg Ransomware. (2018). *KnowBe4's Ransomware Knowledgebase online.* Preuzeto s https://www.knowbe4.com/aids-trojan, 15.8.2018.

Palmer, D. (11. svibnja 2018). *WannaCry ransomware crisis, one year on: Are we ready for the next global cyber attack*? Preuzeto s https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/, 15.8.2018.

Peikari, C., Fogie, S., Read, J., i Hettel, D. (2004). *Summer Brings Mosquito-Borne Malware*. Preuzeto s http://www.informit.com/articles/article.aspx?p=327994, 15.8.2018.

SETI@home. (2018). *SETI@home Project online*. Preuzeto s https://setiathome.berkeley.edu/, 15.8.2018.

Tequila. (2018). *F-Secure Corporation's Threat description online*. Preuzeto s https://www.f-secure.com/v-descs/tequila.shtml, 15.8.2018.

The Most Famous Virus History: Melissa, A. (2013). Panda Security's mediacenter online. Preuzeto s https://www.pandasecurity.com/mediacenter/malware/most-famous-virus-history-melissa/, 15.8.2018.

The Michelangelo Virus, 25 Years Later. (2017). *Trend Micro Inc. news online*. Preuzeto s https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-michelangelo-virus-25-years-later, 15.8.2018.

Virus Creeper. (b.d.). U: The Virus Encyclopedia. Preuzeto s http://virus.wikidot.com/creeper, 11.8.2018.

Virus Jerusalem. (2017). *Malware Wiki*. Preuzeto s http://malware.wikia.com/wiki/Jerusalem, 13.8.2018.

Virus NYB. (2000). *Symantec's Security centre online*. Preuzeto s https://www.symantec.com/security-center/writeup/2000-121513-2227-99, 15.8.2018.

What is CryptoLocker? (b.d.). *Avast Software online*. Preuzeto s https://www.avast.com/c-cryptolocker, 15.8.2018.

What is the difference between viruses, worms, and Trojans? (2016). *Symantec's Technical Support online*. Preuzeto s https://support.symantec.com/en_US/article.TECH98539.html, 15.8.2018.

Zeus Virus. (2018). *Kaspersky Lab's threats online*. Preuzeto s https://usa.kaspersky.com/resource-center/threats/zeus-virus, 15.8.2018.

Kaspersky: Cryptolocker Virus Definition (2018). Preuzeto s https://usa.kaspersky.com/resource-center/definitions/cryptolocker, 15.8.2018.

izv. prof. dr. sc. Krešimir Nenadić

Fakultet elektrotehnike, računarstva i informacijskih tehnologija
Sveučilišta Josipa Jurja Strossmayera u Osijeku

10. MREŽNA SIGURNOST

Sažetak

Poglavlje daje pregled mrežne sigurnosti kao i preporuke korisnicima kako održati sigurnost prvo svog uređaja, a zatim i cijele mreže odnosno informacijskog sustava. Definirana je sigurnosna politika koja propisuje pravila i procedure koje svi korisnici mreže trebaju provoditi. U nastavku su navedeni tipovi mrežne sigurnosti i za većinu su tipova navedene preporuke kako izbjeći neželjene događaje s ciljem održavanja određene razine sigurnosti mreže. Neke preporuke koje su iskazane odnose se na administratora mreže i na njih korisnik ne može znatno utjecati, ali su navedene i preporuke koji se korisnici mogu pridržavati te tako povećati sigurnost informacijskog sustava.

10.1. UVOD

Prema definiciji koju navodi CISCO (2018), vodeća kompanija mrežnih tehnologija, mrežnu sigurnost predstavlja skup aktivnosti čiji je cilj zaštititi iskoristivost i cjelovitost računalne mreže i podataka. Za provođenje zaštite mreže potrebno je uključiti i sklopovske (engl. *hardware*) i programske (engl. *software*) tehnologije. Kako bi mrežna sigurnost bila na poželjnoj razini, potrebno je kvalitetno upravljati pristupu mreži i mrežnim resursima. Pristup mreži podrazumijeva komunikaciju s uređajima u ciljanoj mreži, a mrežni resursi predstavljaju usluge koje se pružaju u ciljanoj mreži. Usluge mogu biti pristup datotečnom poslužitelju, pristup mrežnom poslužitelju, uporaba usluge e-pošte i druge usluge. Cilj je samih aktivnosti mrežne sigurnosti detektirati različite prijetnje unutar i izvan mreže i spriječiti širenje ili ulazak prijetnji u mrežu.

Mrežna sigurnost provodi se kroz više slojeva i na različitim dijelovima mreže. Neke od aktivnosti glede sigurnosti provode se na samom rubu mreže (engl. *gateway*) ali i na gotovo svim uređajima unutar mreže. Na svakom sloju mrežne sigurnosti mogu se primijeniti sigurnosne politike i kontrola prometa odnosno podataka.

Prema kompaniji Palo Alto Networks (2018), jednoj od vodećih u području informacijske sigurnosti, sigurnosnu politiku predstavlja niz pravila i procedura za sve osobe koje pristupaju i koriste imovinu i resurse u vlasništvu organizacije. Sigurnosna politika definira se prema načinu odnosa korisnika mreže prema sigurnosti mreže. Stoga je sigurnosna politika jedinstveni dokument svake organizacije. Cilj je sigurnosne politike očuvanje povjerljivosti, cjelovitosti i dostupnosti sustava, odnosno mreže koju koriste članovi organizacije u čijem je vlasništvu mreža. Budući da se ponašanje zaposlenika tijekom vremena mijenja, neprestano je potrebno prilagođavati i sigurnosnu politiku. To je, dakle, dokument podložan stalnim promjenama u smislu poboljšavanja ukupne sigurnosti mreže.

Pitanje sigurnosti mreže ne čini samo jedan element nego sprega većeg broja elemenata. Postoje dvije krajnosti glede sigurnosti računalne mreže – mreža može biti potpuno sigurna (zatvorena) ili potpuno otvorena s potpunim pristupom. Ni jedna navedena krajnost nije preporučljiva. Ako je mreža potpuno sigurna i zatvorena, korisnici neće imati pristup dijelovima potrebnih resursa (pristup datotečnom poslužitelju, intranetu ili nekoj drugoj usluzi). U slučaju druge krajnosti, kada je mreža potpuno otvorena, zlonamjerni napadač bez problema može pristupiti mrežnim resursima i „narediti" drugom računalu da napravi nešto što nije dopušteno.

Svaka organizacija mora procijeniti kako i koliko će zaštititi svoju mrežu. Dio zaštite mreže je i donošenje određenih pravila ponašanja korisnika mreže, politike sigurnosti u obliku zahtjeva i preporuka čime se definiraju sigurnosne mjere i rizici.

Sigurnosne mjere i politiku postavlja uprava organizacije na prijedlog nadležne službe u organizaciji. O provedbi mrežne zaštite brine se mrežni administrator. Zaštita mreže provodi se tako da se sprječava neovlašteni pristup mrežnim resursima. Resursima koji imaju ograničen pristup trebali bi pristupati samo za to ovlaštene osobe ili uređaji. Uz zaštitu potreban je stalni nadzor rada mreže (mrežnih uređaja) i procjena učinkovitosti.

10.2. KONTROLA PRISTUPA MREŽI

Kada se promatra računalna mreža u vlasništvu neke organizacije, pristup toj mreži ograničen je na ovlaštene osobe, najčešće zaposlenike te organizacije. U toj se skupini ovlaštene osobe mogu kategorizirati u više grupa s različitim pravima pristupa mrežnim resursima i uslugama. Sustav može napraviti identifikaciju samog korisnika ili uređaja kojim se pristupa mreži ili usluzi. Identifikacija je prvi korak vezan za mrežnu sigurnost.

Korisnik se identificira svojim korisničkim imenom (engl. *username*) pri pristupu mrežnim resursima ili uslugama. Samo ovlašteni korisnici mogu pristupiti mreži, dijelovima mreže ili određenim uslugama. Identifikacija korisnika obavlja se provjerom postojanja korisničkog imena s popisom ovlaštenih osoba u bazi podataka na nekom od poslužitelja. Ako se korisničko ime nalazi u popisu u bazi podataka, korisniku će se dopustiti pristup ovisno o njegovim ovlastima koje su definirane sigurnosnom politikom.

Uređaj se isto tako može identificirati prilikom pristupa mreži. Na najnižem sloju modela mreže prema OSI (engl. *Open Systems Interconnection*) mrežnom modelu (ISO standard, 2018), pristup mreži može se ograničiti kontrolom fizičkog pristupa priključcima za mrežnu komunikaciju. Slojevi OSI mrežnog modela prikazani su na slici 1. Zaposlenici organizacije mogu pristupati mreži na različite načine. Obično u svom uredu zaposlenici imaju fizički mrežni priključak (RJ45) na koji uređaj spajaju mrežnim kablom. Nakon što posljednji zaposlenik napusti ured, prostorija bi se trebala zaključati kako neovlaštene osobe ne bi imale fizički pristup mrežnim priključcima. Budući da većina zaposlenika nema pristup mrežnoj opremi (usmjerivači, preklopnici, poslužitelji), aspekt koji se odnosi na zaštitu takvih uređaja neće biti obrađen u ovom poglavlju. O sigurnosti navedenih uređaja brinu se mrežni administratori koji su educirani i stručni obavljati zaštitu mreže i mrežnih uređaja. Drugi je način pristupa mreži preko bežične mreže (engl. *WiFi*) za koji nije potreban fizički priključak pa se identifikacija uređaja obavlja drugačije.

Slika 1. Slojevi OSI mrežnog modela

Bez obzira na način pristupa mreži, fizički pristup mrežnim kablom ili bežičnom konekcijom, identifikacija samih uređaja koji pristupaju mreži i njezinim resursima obavlja se u nekoliko slojeva OSI mrežnog modela. Na drugom sloju OSI modela (sloj podatkovne veze) identifikacija uređaja obavlja se fizičkom adresom uređaja (engl. *Media Access Controll* – MAC address). Fizička adresa uređaja jedinstvena je, zapisana u samom uređaju i u pravilu se ne može mijenjati. Primjer fizičke adrese nekog uređaja je: **E8-9A-8F-C7-C8-BD**. Kontrola pristupa mreži fizičkom adresom uređaja izvršava se na preklopniku koji prati promet podataka i uspoređuje fizičke adrese unutar podataka s onima u svojim postavkama. Na taj način može dopustiti ili zabraniti promet ovisno o postavkama koje je podesio administrator mreže. Filtriranje prometa usporedbom fizičkih adresa uređaja ne ovisi o načinu spajanja na mrežu (kabel ili bežični pristup).

Na mrežnom sloju OSI modela identifikacija uređaja obavlja se na osnovu mrežne ili IP adrese. Mrežna adresa isto je tako jedinstvena oznaka uređaja. Ako je mrežna adresa javna, mora biti jedinstvena za cijeli svijet (internet). U slučaju upotrebe privatnih mrežnih adresa, uređaj treba imati jedinstvenu mrežnu adresu unutar te privat-

ne mreže. Kao što preklopnik može obavljati kontrolu (filtriranje) prometa na osnovu fizičke adrese, tako usmjerivač obavlja istu funkciju na osnovu mrežnih adresa. Ovisno o postavkama usmjerivača određeni promet može se propustiti ili zabraniti prije ulaska u mrežu ili napuštanja mreže. Osim po mrežnim adresama usmjerivač može filtrirati promet i po tipu komunikacije, odnosno protokolu koji se koristi prilikom komunikacije.

Kao primjer može se navesti pokušaj pristupanja uslugama neke ustanove kojima se može pristupiti samo s uređaja koji su unutar mreže te ustanove. Ako, na primjer, korisnik čiji uređaj ima IP adresu 145.50.22.88 pokuša pristupiti uslugama na poslužitelju s IP adresom 131.24.99.1, pristup će mu biti odbijen jer korisnikov uređaj nema IP adresu u istoj mreži kao poslužitelj. Provjerom IP adresa može se ograničiti ili potpuno onemogućiti pristup uređajima koji su u rizičnim skupinama ili zemljama na osnovu IP adrese pristupnog uređaja. Ograničenja, odnosno dozvola ili zabrana prometa na osnovu IP adrese mogu se definirati za oba smjera komunikacije. Tako se, na primjer, zaposlenicima neke ustanove može zabraniti pristup nekoj usluzi koju ne pruža ta ustanova. Najčešće poslodavci brane svojim zaposlenicima posjećivanje društvenih mreža za vrijeme radnog vremena ili sa službenih računala. U takvom je slučaju administrator sustava upisao IP adresu poslužitelja društvene mreže u pristupnu listu i toj IP adresi zabranjen je pristup s uređaja koji se nalaze u mreži ustanove. Na sličan način, ali provjerom tipa komunikacije prema broju komunikacijskog porta, može se dopustiti ili zabraniti pristup određenim uslugama prema vrsti usluge odnosno prema vrsti prometa.

Drugi je dio kontrole pristupa mreži autentikacija korisnika. Nakon identifikacije korisničkog imena potrebno je utvrditi je li to stvarno korisnik koji se mreži ili mrežnoj usluzi predstavlja. Autentikacija se obavlja provjerom zaporke koju korisnik upisuje s onom u bazi podataka koja je postavljena prilikom registracije korisnika. Korisnici mogu imati pravo promjene zaporke na neku novu vrijednost. Kvalitetu zaporke, pa time i sigurnost koja se ostvaruje autentikacijom, određuje sigurnosna politika organizacije. Više o kvaliteti zaporke može se pronaći u radovima autora Šolić, Očevčić i Blažević (2015) te u Šolić, Kralik, Ilakovac i Nenadić (2014).

Nakon uspješne identifikacije i autentikacije uređaja ili korisnika, može se pristupiti određenim mrežnim resursima. Kojim mrežnim resursima i uslugama može pristupiti određeni korisnik određuje se sigurnosnom politikom.

10.3. PROGRAMI ZA ZAŠTITU PROTIV VIRUSA I ZLOĆUDNIH PROGRAMA

Svaki korisnik uređaja kojim se spaja na bilo kakvu mrežu treba se zaštititi od raznih vrsta zloćudnih programa. Vrste zloćudnih programa objašnjene su poglavlju o *Osobnoj sigurnost i zloćudnim programima na internetu* u knjizi. Preporuka je svakom korisniku instalacija programa (aplikacija) koja će uređaj štititi od napada zloćudnih programa. Postoje besplatni alati koji na zadovoljavajući način mogu zaštititi uređaj. Korisnik uređaja treba se pobrinuti za redovito osvježavanje same aplikacije novim nadogradnjama kao i preuzimanjem najnovijeg popisa zloćudnih programa kako bi se učinkovito zaštitio od istih.

Kako svaki korisnik treba zaštititi svoj uređaj odgovarajućom aplikacijom protiv zloćudnih programa, tako administrator treba zaštititi poslužitelje od istih prijetnji. Svaki uređaj za svoj uobičajeni rad treba operacijski sustav koji se brine o normalnom funkcioniranju uređaja. Sam operacijski sustav obično nema funkcionalnost koja štiti uređaj od zloćudnih programa pa je takve aplikacije potrebno naknadno instalirati. Aplikacije za zaštitu od zloćudnih programa razlikuju se prema vrsti operacijskog sustava na koji se instaliraju. Osim vrste operacijskog sustava razlikuju se i aplikacije za zaštitu poslužitelja od onih za zaštitu krajnjeg korisnika mrežnih usluga. Postoje programska rješenja koja objedinjuju više funkcionalnosti u zaštiti uređaja, ali se korisnik može odlučiti i na usko specijalizirane aplikacije koje nude zaštitu od samo jedne vrste zloćudnih programa. Ako je uređaj koji treba zaštititi poslužitelj, administrator u dogovoru s upravom organizacije i sigurnosnom politikom treba odlučiti koju će aplikaciju ili aplikacije za zaštitu postaviti na poslužitelj. Odabir ovisi i o financijskom čimbeniku jer su aplikacije za poslužitelje uglavnom komercijalne i cijena im nije niska. Za klijentske uređaje može se odabrati i neko od besplatnih rješenja koje se može preuzeti s interneta ili više različitih aplikacija. Pri instalaciji aplikacija za zaštitu uređaja ne treba pretjerivati u njihovom broju jer neke od aplikacija mogu usporiti rad uređaja ili, u još gorem slučaju, neke aplikacije ne mogu raditi u isto vrijeme s drugim aplikacijama.

Postoji mogućnost zadavanja obvezne aplikacije za zaštitu ako je tako definirano sigurnosnom politikom i ako se takva aplikacija kupi. Čest je slučaj da vlasnik aplikacije prodaje obje vrste aplikacije – za poslužitelje i za klijentska računala. U tom slučaju korisnik nema mogućnost odabira aplikacije, već bi trebao koristiti onu koja je definirana sigurnosnom politikom.

10.4. ZAŠTITA APLIKACIJA

Bilo koja aplikacija, odnosno programsko rješenje, kojom se organizacija koristi u svom radu treba biti zaštićena. Zaštita aplikacija obuhvaća mjere koje su poduzete kako bi se ostvarila ili povećala sigurnost. Mjere koje se mogu poduzeti su: traženje, popravljanje i sprječavanje ranjivosti same aplikacije. Od dijelova životnog ciklusa aplikacije ovdje nas zanima postavljanje, nadogradnja i održavanje aplikacije.

Prilikom izrade aplikacije mogu se pojaviti različiti propusti koji napadaču omogućuju iniciranje različitih vrta napada na aplikaciju, a preko aplikacije i na cijeli sustav odnosno mrežu. Propusti mogu biti uzrokovani i greškama u prevoditelju programskog kôda.

Bez obzira na vrstu propusta, gdje i kada je nastao, on se može otkloniti programskim nadogradnjama. Aplikacije obično imaju mogućnost automatskog preuzimanja nadogradnji i instalacije istih. U slučaju kada ne postoji automatsko preuzimanje i instalacija nadogradnji, iste je potrebno obaviti ručno. Nadogradnja aplikacije sigurnosnom zakrpom tada se obavlja preuzimanjem samo zakrpe ili preuzimanjem nove inačice cijele aplikacije koja sadrži i samu zakrpu.

10.5. ANALIZA PONAŠANJA

Kako bi se detektiralo abnormalno ponašanje uređaja ili korisnika, potrebno je znati ili definirati kako izgleda normalno ponašanje ili funkcioniranje uređaja ili korisnika. Kao što uređaji svojim radom u mrežnom okruženju mogu biti izvor smetnji ili prijetnji, tako i korisnici koji ih koriste svojim ponašanjem tijekom rada na uređaju mogu biti izvor prijetnji. Postoje programski alati koji mogu detektirati ponašanje ili funkcionalnosti koje odstupaju od normalnog ili definiranog sigurnosnom politikom. Praćenje ponašanja sustava, mreže, uređaja i korisnika kontinuirani je proces čiji je cilj održavanje sigurnosti sustava, odnosno cijele mreže.

Korisnik svojim radom na uređaju može narušiti sigurnost mreže te tako postaje izvor prijetnje mrežnoj sigurnosti. U privitku poruke elektroničke pošte korisnik može dobiti datoteku čijim se pokretanjem izvršava neki maliciozni program koji se može proširiti na druge uređaje unutar mreže. Još je jedan oblik narušavanja sigurnosti priključivanje tuđih neprovjerenih memorijskih štapića na uređaj koji je spojen na mrežu. Čest oblik narušavanja sigurnosti od strane korisnika slanje je osobnih pristupnih podataka osobama koje zatraže te podatke. Važno je naglasiti da administrator sustava nikada neće tražiti pristupne podatke od bilo kojeg korisnika tog sustava.

Više o sigurnosti sustava i načinima procjene može se pronaći u radovima autora Šolić, Očevčić i Golub (2014), Očevčić, Nenadić, Šolić i Keser (2017) i Velki, Šolić i Nenadić (2015). O sigurnosti, prijetnjama i rješenjima koje se odnose na društvene mreže može se pronaći u radovima autora Rathore i drugi (2017) i Tayouri (2015).

10.6. GUBITAK PODATAKA

Prijetnju sigurnosti sustava odnosno mreže može predstavljati gubitak podataka. Podaci s bilo koje vrste poslužitelja napadom se mogu obrisati odnosno trajno uništiti. Postoje slučajevi napada na mreže, konkretno na poslužitelje čiji je cilj bio preuzimanje odnosno kopiranje podataka o računima, odnosno o brojevima kreditnih kartica korisnika usluga nekog mrežnog sustava. Jedan je od možda najpoznatijih napada onaj na Sony gdje su napadači prikupili podatke kreditnih kartica korisnika Sony PlayStation uređaja. Detalji o napadu mogu se pogledati na stranici Eurogamer-a (https://www.eurogamer.net/articles/2016-04-26-sony-admitted-the-great-psn-hack-five-years-ago-today, 2016).

Teži je oblik napada na podatke brisanje podataka s poslužitelja ili klijentskog računala. Zaštita od takve vrste napada gdje se podaci brišu odnosno uništavaju je kreiranje kopije podataka na nekom vanjskom uređaju za pohranu podataka ili upotreba internetskih usluga za spremanje podataka. Podaci se mogu duplicirati na nekoj od besplatnih usluga koje nude pohranu podataka u obliku dokumenata ili datoteka.

O zaštiti podataka na poslužiteljima brine se mrežni administrator. Svaki se korisnik treba pobrinuti o održavanju sigurnosne kopije podataka sa svakog svog uređaja. Sinkronizaciju podataka na uređaju i sigurnosne kopije treba obavljati periodično ovisno o korisnikovim potrebama.

Neke usluge na internetu nude mogućnost sinkronizacije podataka na uređaju i podataka na njihovom poslužitelju. Korisnik može mijenjati podatke unutar datoteka na svom uređaju neovisno ima li konekciju na internet ili nema, a sinkronizacija se obavlja kada uređaj ostvari konekciju na internet.

Od gubitka podataka najsigurnije je rješenje održavanje jedne ili više kopija podataka koji su važni.

U posljednje se vrijeme pojavio način napada gdje zloćudni program (engl. *ransomware*) kriptira korisničke podatke na uređaju i traži od korisnika plaćanje određene svote novca na račun kako bi dobio ključ za otključavanje kriptiranih podataka. I za takav slučaj gubitka podataka najjednostavniji je način povrata „*izgubljenih*“ podataka iz sigurnosne kopije.

10.7. SIGURNOST E-POŠTE

Elektronička pošta jedan je od najvećih izvora prijetnji sigurnosti mreže. U posljednje vrijeme svjedoci smo personaliziranih napada, ili barem pokušaja, gdje napadač šalje personaliziranu poruku potencijalnoj žrtvi. Poruka sadrži informacije koje su rezultat socijalnog inženjeringa i taktike „*pecanja*“ (engl. *phishing*) kojima korisnika nagovaraju na razne štetne akcije. U privitku poruke može biti dio zlođudnog kôda koji se može izvršiti i samim otvaranjem poruke bez da korisnik otvara privitak. Šteta koju može nanijeti zlođudni program ili kôd u privitku ne mora biti ograničena samo na korisnikov uređaj, već se zlođudni kôd može mrežom proširiti i na druge uređaje posredstvom poslužitelja.

Preporuka je korisnicima ne otvarati poruke nepoznatih pošiljatelja, a svakako ne otvarati privitke u takvim porukama. Postoje aplikacije koje mogu spriječiti preuzimanje zlođudnog koda iz poruke elektroničke pošte, ali se taj problem može riješiti i na poslužitelju. Dobra zaštita na poslužitelju elektroničke pošte može onemogućiti primanje poruka sa zlođudnim sadržajima.

Još je jedan oblik napada na e-poštu korisnika primanje neželjene pošte (engl. *spam*). Poruka koja kao odredište ima veći broj korisnika e-pošte može biti okarakterizirana kao neželjena poruka. O filtriranju takvih poruka na poslužitelju brine se administrator, ali i svaki korisnik može u aplikaciji koju koristi za čitanje e-pošte podesiti filter za kontrolu neželjene e-pošte.

10.8. VATROZID

Vatrozid (engl. *firewall*) usluga je u obliku sklopovskog i/ili programskog rješenja koja predstavlja prepreku koja se nalazi između poznate i pouzdane mreže te nepoznate i nepouzdane mreže koju može predstavljati internet. Vatrozid koristi skup definiranih pravila koja dopuštaju ili zabranjuju promet u oba smjera – u mrežu ili iz mreže.

Slijedi primjer konfiguracije pristupne liste (engl. *access list*) na usmjerivaču s objašnjenjima. Korisnik koji konfigurira pristupnu listu treba imati odgovarajuće administratorske ovlasti za uređaj na kojemu se vrši konfiguracija.

Primjer 1. Naredbe za postavljanje pristupnih lista na usmjerivaču

Naredba ili akcija	Svrha
Device(config)# ip access-list standard AccessList1	Definira se standardna IP pristupna lista uporabom imena (AccessList1)
Device(config-std-nacl)# deny 172.16.0.0 0.0.255.255	Svim uređajima koji pripadaju mreži sa IP adresom 172.16.0.0 zabranjuje se (engl. *deny*) dolazni promet prema lokalnoj mreži u vlasništvu ustanove u kojoj se nalazi usmjerivač koji se konfigurira.
Device(config-std-nacl)# permit 172.18.5.22 0.0.0.0	Uređaju sa IP adresom 172.18.5.22 dopušta se (engl. *permit*) prolazak kroz pristupnu listu, odnosno dopušta se dolazni promet.
Device(config-ext-nacl)# deny ip 172.18.0.0 0.0.255.255 host 172.16.40.10	Svim uređajima koji pripadaju mreži sa IP adresom 172.18.0.0 zabranjuje se sav promet prema uređaju sa IP adresom 172.16.40.10

Vatrozid može biti postavljen na pojedini poslužitelj s ciljem filtriranja mrežnog prometa. Na taj način se može smanjiti količina podataka koja putuje pojedinim dijelom mreže. Osim na poslužiteljima vatrozid može biti postavljen, odnosno konfiguriran, na usmjerivaču koji predstavlja ulaz/izlaz mreže (engl. *gateway*). Isto tako vatrozid je moguće konfigurirati na klijentskim uređajima kao dio operacijskog sustava ili kao zasebnu aplikaciju. Korisnik treba voditi računa da bi, ako poslužitelji i/ili *gateway* imaju podešen vatrozid, uređaj trebao imati vatrozid istog proizvođača kako ne bi došlo do nemogućnosti mrežne komunikacije.

10.9. SUSTAVI ZA SPRJEČAVANJE UPADA

Sustav za sprječavanje upada u mrežu (engl. *Intrusion Prevention Systems* – IPS) nadzire mrežni promet s ciljem aktivnog blokiranja napada na mrežnu sigurnost. IPS sustavi veliki su sustavi koji imaju mogućnost pamćenja, odnosno bilježenja prijetnji, a neki imaju i mogućnost strojnog učenja s ciljem što veće učinkovitosti sprječavanja neželjenih napada. Osim što mogu blokirati zloćudne aktivnosti, IPS sustavi mogu pratiti progresiju sumnjivih datoteka i zloćudnih programa i kôdova kroz mrežu kako bi spriječili izbijanje i širenje zaraženog odnosno zloćudnog kôda.

10.10. MOBILNI UREĐAJI

Svjedoci smo naglog razvoja i širenja popularnosti mobilnih uređaja, ponajprije pametnih telefona i tableta pa su i takvi uređaji postali cilj napada. U sljedeće tri godine 90 % organizacija u IT sektoru podržavat će korporacijske aplikacije na mobilnim uređajima (CISCO, 2018). Samim time mobilni uređaji postaju zanimljivi napadačima pa je i njih potrebno nekako zaštititi. Na tržištu već postoje aplikacije za zaštitu, kako samih uređaja tako i podataka na njima.

I ovdje vrijedi preporuka o izradi sigurnosne kopije osjetljivih podataka. Na mobilnim uređajima osjetljivi podaci mogu biti i kontakti u imeniku uređaja, poruke pa i datoteke. Mobilni uređaji uglavnom uz operacijski sustav imaju i potrebne funkcionalnosti za sinkronizaciju podataka na uređaju s onima sigurnosne kopije.

Sustavi plaćanja mobilnim uređajem s poslužiteljem komuniciraju sigurnim protokolima pri čemu se razmjenjuju kriptirani podaci. Svi korisnikovi podaci koji se šalju poslužitelju kriptiraju se na mobilnom uređaju te se šalju poslužitelju u kriptiranom obliku. Na strani poslužitelja kriptirani se podaci dekriptiraju kako bi se utvrdio identitet korisnika.

Više o sigurnosti korištenja mobilnih uređaja za različite oblike komunikacije može se pogledati u radu autora La Polla, Martinelli i Sgandurra (2012).

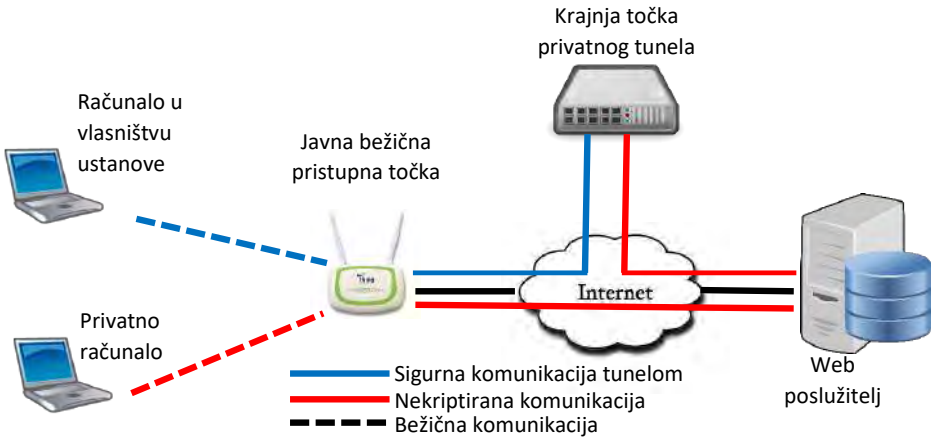
10.11. SEGMENTACIJA MREŽE

Programski definirana segmentacija mreže, odnosno podjela na manje logičke cjeline, pruža mogućnost klasificiranja mrežnog prometa te se tako lakše provodi sigurnosna politika. U idealnom slučaju klasifikacija se temelji na identifikaciji uređaja koji se spaja na mrežu ili je već spojen neovisno o mrežnoj adresi. Uređaju, odnosno korisniku koji koristi uređaj, mogu se dodijeliti prava pristupa pojedinim mrežnim resursima na temeljeu uloge koju obavlja u organizaciji, lokacije gdje se korisnik nalazi ili ovisno o nekom drugom kriteriju. Na taj se način odgovarajućim korisnicima dodjeljuju odgovarajuća prava pristupa, a sumnjivim korisnicima, odnosno njihovim uređajima, može se zabraniti pristup i restriktivno reagirati na određeni način ovisno o sigurnosnoj politici.

10.12. VIRTUALNA PRIVATNA MREŽA

Svrha je virtualne privatne mreže omogućiti ovlaštenim korisnicima koji su fizički izdvojeni od svoje mreže na nekoj drugoj geografskoj lokaciji sigurnu komunikaciju s mrežom. Takva se komunikacija obično kriptira, a za povezivanje dviju geografski udaljenih točki koristi se internet. Tako se udaljenom korisniku čini kao da se nalazi unutar svoje mreže i može koristiti sve resurse kao da se fizički nalazi unutar mreže. Primjer virtualne privatne mreže može se vidjeti na Slici 2.

Postupak kriptiranja pretvorba je informacije (na primjeru običnog teksta) u oblik koji mogu protumačiti samo autorizirane osobe koje znaju kako se kriptirani tekst ponovno pretvara u izvorni oblik postupkom dekriptiranja. Na taj se način osjetljive informacije mogu zaštititi tako da ih ne može protumačiti bilo tko.



Slika 2. Prikaz komunikacije preko VPN mreže

10.13. ZAKLJUČAK

U poglavlju su navedeni neki aspekti mrežne sigurnosti i sigurnog ponašanja korisnika informacijskog sustava. Neposredno prije uporabe mrežnih resursa ili usluga korisnik i uređaj kojim se korisnik koristi trebaju se identificirati kako bi se usluga ili resurs mogli sigurno isporučiti korisniku. Danas su mobilni uređaji (pametni telefoni i tableti) vrlo rašireni pa se i njihova sigurnost treba uzeti u obzir. Navedeni su neki mehanizmi zaštite pristupa mrežnim resursima i uslugama. Korisnik uređaja može sam ili uz pomoć stručnog osoblja voditi brigu o održavanju zadovoljavajuće funkcionalnosti cijelog uređaja, pojedinih sklopovskih komponenti ili programskih

rješenja poput antivirusnih programa. Korisnik svojim radom na uređaju može narušiti sigurnost mreže te tako postaje izvor prijetnje mrežnoj sigurnosti na što trebaju paziti i sami korisnici i mrežni administratori. Navedene su preporuke i mehanizmi osiguranja korisnika i informacijskog sustava od gubitka podataka koji mogu predstavljati važan resurs u informacijskom sustavu. Ponašanje korisnika prilikom čitanja osobne elektroničke pošte također može znatno utjecati na sigurnost, a u tekstu su navedene neke preporuke kako se sigurnost može održati odnosno povećati razina sigurnosti. Osim vatrozida na korisničkim uređajima moguće je postaviti vatrozid i na neke mrežne uređaje što povećava razinu sigurnosti. Sustavi za sprječavanje upada u mrežu još su jedan aspekt mrežne sigurnosti o kojem brinu osobe zadužene za sigurnost informacijskog sustava. Računalnu mrežu moguće je podijeliti na segmente prema nekom kriteriju te tako povećati razinu sigurnosti. Zbog današnjeg načina života, u kojem djelatnici mogu obavljati svoj posao od kuće, u nekim slučajevima nužno je omogućiti pristup mrežnim resursima i uslugama korisnicima koji su fizički izvan mreže. Virtualnom privatnom mrežom takvi korisnici mogu pristupiti mrežnim resursima i uslugama na siguran način kao da se nalaze fizički na svom radnom mjestu u tvrtki.

Zbog značajnog broja aspekata na koje treba obratiti pozornost za sigurnu uporabu uređaja u računalnoj mreži i sigurnog ponašanja korisnika uređaja, potrebno je neprestano educirati sve korisnike informacijskog sustava omogućim prijetnjama.

10.14. LITERATURA

Odom, W. (2016). CCNA Routing and Switching 200-125 Official Cert Guide Library. USA: Cisco Press.

Gregory B. W., Eric A. F. i Udo W. P. (2017). Computer System and Network Security. Boca Raton, USA: CRC Press.

35.100 OSI model. (1994). International Organization for Standardization's store online. Preuzeto s https://www.iso.org/ics/35.100/x/, 22.8.2019.

Očevčić, H., Nenadić, K., Šolić, K. i Keser, T. (2017). The Impact of Information System Risk Management on the Frequency and Intensity of Security Incidents. International journal of electrical and computer engineering systems, 8, 41-46.

Rathore, S., Sharma, K. P., Loia, V., Jeong, Y. S. i Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. Information Sciences, 421, 43-69.

Tayouri D. (2015). The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. Procedia Manufacturing, 3, 1069-1100.

La Polla M., Martinelli F. i Sgandurra D. A. Survey on Security for Mobile Devices. IEEE: IEEE Communications Surveys & Tutorials, 15, 446-471.

Eurogamer (2016). Five years ago today, Sony admitted the great PSN hack. Preuzeto s https://www.eurogamer.net/articles/2016-04-26-sony-admitted-the-great-psn-hack-five-years-ago-today, 22.8.2019.

Šolić, K., Kralik, K., Ilakovac, V. i Nenadić, K. (2014). Lakovjernost ili preposlušno praćenje predavaćevih instrukcija (otkrivanje zaporke). Medix: specijalizirani medicinski dvomjesečnik, 109/110, 239-242.

Šolić, K., Očevčić, H. i Blažević, D. (2015). Survey on Password Quality and Confidentiality. Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije, 56, 69-75.

Šolić, K., Očevčić, H. i Golub, M. (2014). The information systems' security level assessment model based on an ontology and evidential reasoning approach. Computers & security, 55, 100-112.

Velki, T., Šolić, K. i Nenadić, K. (2015). Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK). Psihologijske teme, 24, 401-424.

What is an It security policy? (n.d.). PaloAlto Networks's CyberPedia online. Preuzeto s https://www.paloaltonetworks.com/cyberpedia/what-is-an-it-security-policy, 22.8.2019.

What is network security? (n.d.). CISCO's Security products online. Preuzeto s https://www.cisco.com/c/en/us/products/security/what-is-network-security.html, 22.8.2019.

Ivan Horvat

OTIS d.o.o., Osijek

doc. dr. sc. Krešimir Šolić

Medicinski fakultet Sveučilišta Josipa Jurja Strossmayera u Osijeku

11. OSNOVE KRIPTOGRAFIJE

Sažetak

Prosječan korisnik informacijsko-komunikacijskih sustava danas se učestalo koristi kriptografiju, a da možda toga nije ni svjestan, od kriptiranih zaporki za razne sustave do digitalnih ceritifikata za pristupanje internetskog bankarstvu ili sustavu e-građani. Čak je i običan telefonski razgovor uporabom analogne linije vrsta kriptosustava budući da se koristi frekvencijskom modulacijom ljudskoga glasa, ali s javno poznatim simetričnim ključem.

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje tajnih poruka u obliku koji će moći pročitati samo primatelj kojemu je i namijenjena, a počela se upotrebljavati još u staroj Grčkoj gdje su Spartanci u 5. stoljeću prije Krista koristili napravu za šifriranje nazvanu skital.

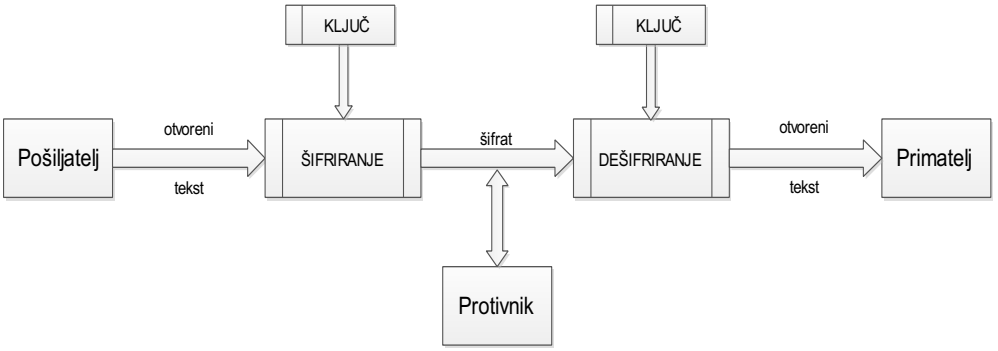
U ovome poglavlju opisan je povijesni razvoj kriptografije, opisani su osnovni načini i mehanizmi kriptiranja i dekriptiranja podataka s jednostavnim primjerima te je kratko opisana kriptografija u današnjoj praktičnoj upotrebi.

Prosječan korisnik radi osobne zaštite te zaštite raznih informacijsko-komunikacijskih sustava kojima se koristi treba biti svjestan kako je izrazito važno čuvati tajnost svojih pristupnih podataka za navedene sustave te kako je on odgovoran za sve što se pod njegovim imenom na tim sustavima pojavljuje i mijenja. Kriptiranje podataka modernim sustavima za enkripciju bez poznavanja lozinke za dekripti-

ranje, npr. zbog računalnog napada zlonamjernim programom internetske krađe podataka, engl. runsomware, ili u slučaju gubitka iste, najčešće rezultira potpunim gubitkom podataka koji nam postaju zauvijek nečitljivi.

11.1. UVODNO O KRIPTOGRAFIJI

Prema Dujella i Maretić (2007) kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Samo komuniciranje odvija se na način da pošiljatelj (onaj koji generira poruku) šalje poruku primatelju (onaj za koga je poruka namijenjena) uporabom nekog komunikacijskog kanala. Taj je kanal najčešće nesiguran, osim ako oba subjekta nisu u npr. zatvorenoj zvučno izoliranoj prostoriji. Od samih početaka ljudske komunikacije postoji želja i potreba za sigurnim komuniciranjem, ali i svjesnost da poruke često putuju nesigurnim kanalima komuniciranja. Osnovni je problem, koji se pokušava riješiti pomoću kriptografije, onemogućiti onoga tko nadzire taj komunikacijski kanal da sazna sadržaj poruke koja se prenosi.



Slika 1. Shema klasične kriptografije

Osnovni pojmovi koji se koriste u kriptografiji su:

- ✓ pošiljatelj – osoba koja šalje poruku
- ✓ primatelj – osoba koja prima poruku, za koju je poruka namijenjena
- ✓ protivnik – treća osoba koja pokušava neovlašteno prisluškivati poruku
- ✓ komuniciranje – razmjena poruka, informacija
- ✓ komunikacijski kanal – put, sredstvo kojim poruka putuje
- ✓ otvoreni tekst – izvorna, nepromijenjena poruka (engl. *plaintext*)
- ✓ ključ – način šifriranja i dešifriranja podataka (engl. *key*)
- ✓ šifriranje – postupak transformacije otvorenog teksta pomoću ključa
- ✓ šifrat/kriptogram – dobiveni rezultat šifriranja (engl. *chipertext*)
- ✓ dešifriranje – postupak transformacije šifrata u otvoreni tekst pomoću ključa

- ✓ kriptografski algoritam – matematička funkcija koja se koristi za šifriranje i dešifriranje
- ✓ prostor ključeva – skup svih mogućih vrijednosti ključeva
- ✓ kriptosustav – sastoji se od kriptografskog algoritma i svih mogućih otvorenih tekstova, šifrata i ključeva.

Kriptoanaliza/dekriptiranje znanstvena je disciplina koja proučava postupke za čitanje šifrata bez poznavanja ključa, a sam se postupak snaziva kriptoanalitički napad. Kriptografija i kriptoanaliza zajedno čine kriptologiju.

Dujella i Maretić (2007) klasificiraju kriptosustave prema:

1. tipu operacija koje se koriste pri šifriranju na:

   supstitucijske šifre – svaki element otvorenog koda zamjenjuje se drugim elementom

   transpozicijske šifre – elementi otvorenog teksta se permutiraju (premještaju)

2. načinu na koji se obrađuje otvoreni tekst na:

   blokovne šifre – obrađuje se blok po blok elemenata otvorenog teksta koristeći jedan te isti ključ

   protočne šifre – obrađuje se element po element otvorenog teksta koristeći se pri tome nizom ključeva (engl. *keystream*) koji se paralelno generira

3. tajnost i javnost ključeva na:

   simetrični (konvencionalni) kriptosustavi – ključ za dešifriranje može se izračunati poznavajući ključ za šifriranje i obratno; ti su ključevi najčešće identični, a sigurnost je u tajnosti ključa.

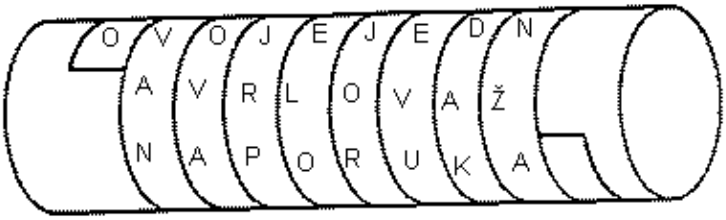
Kriptosustavi s javnim ključem – ključ za dešifriranje ne može se izračunati iz ključa za šifriranje, barem ne u nekom razumnom vremenu. Ključ za šifriranje javni je. Bilo tko može šifrirati poruku pomoću njega, ali poruku može dešifrirati samo osoba koja ima odgovarajući ključ za dešifriranje – privatni (tajni) ključ. Godine 1976. Whitfield Diffie i Martin Hellman prvi su iznijeli ideju javnoga ključa (Dujella i Maretić, 2007).

Osnovna je pretpostavka kriptoanalize da kriptoanalitičar koji pokušava dekriptirati poruku zna koji se kriptosustav upotrebljava. Prema Nizozemcu Augustu Kerckhoffsu, autoru knjige „Vojna kriptografija" iz 1883. godine, to se naziva Kerckhof-

fsovo načelo (Dujella i Maretić, 2007). Iako ta pretpostavka ne mora biti točna, sigurnost kriptosustava ne može počivati na pretpostavci da protivnik ne zna koji kriptosustav upotrebljavamo.

11.2. POVIJESNI RAZVOJ KRIPTOGRAFIJE

Dujella i Maretić (2007) navode kao jednu od prvih poznatih upotreba kriptografije u staroj Grčkoj gdje su Spartanci već u 5. stoljeću prije Krista upotrebljavali napravu za šifriranje. Naprava se nazivala „skital", a sastojala se od štapa ili nekog drugog predmeta oko kojega se namotavala vrpca od pergamenta te se na nju okomito ispisivala poruka. Nakon razmatanja vrpce, poruka bi bila izmiješana te bi ju mogao pročitati samo onaj tko je imao štap iste debljine. To je osnovni primjer transpozicijske šifre.



Slika 2. Skital (Dujella, 2018)

11.2.1. SUPSTITUCIJSKE ŠIFRE

Kao jednu od prvih poznatih uporaba supstitucijske šifre Dujella i Maretić (2007) navode zapisivanje Knjige o Jeremiji, kao dijela Biblije, u 6. stoljeću prije Krista kada je upotrebljena jednostavna šifra zasnovana na načelu zamjene slova abecede, tzv. Hebrejska šifra. U tom je slučaju upotrebljena inačica koja izvrće abecedu naopako, poznata pod imenom ATBASH. Osim „atbash" šifre postoje još „albam" i „atbah" šifra.

Tablica „atbash" šifre za engleski jezik glasi:

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Tablica 1. Atbash (Dujella, 2018)

Tablica „albam“ šifre za engleski jezik glasi:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tablica 2. Albam (Dujella, 2018)

Takav je način kriptiranja recipročan, tj. ako se prvo slovo zamjeni drugim, onda se drugo slovo zamjeni prvim.

11.2.1.1. Cesarova šifra

Riječ je o najpoznatijom supstitucijskoj šifri kojom se koristio poznati rimski vojskovođa, državnik i car Gaj Julije Cezar (Dujella i Maretić, 2007). U Cezarovoj šifri slova otvorenog teksta zamjenjuju se slovima koja se nalaze tri mjesta dalje od njih u alfabetu (A -> D, B -> E, C -> F…) s pretpostavkom da se alfabet ciklički nastavlja, odnosno poslije Z ponovo dolazi A, B, C.

Cezarovu šifru možemo zapisati u tablici:

Otvoreni tekst	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
šifrat	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tablica 3. Cesarova šifra (Dujella, 2018)

A njegova poznata izreka

VENI VIDI VICI

bila bi šifrirana ovako:

YHQL YLGL YLFL

Radi matematičke obrade i modifikacije originalne Cezarove šifre, te analize pomaka različitih od tri, zamijenit ćemo slova alfabeta njihovom brojčanom oznakom pozicije $Z26 = \{0, 1, 2, \ldots, 25\}$ (skup brojeva 0–25), prema tablici:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Tablica 4. Zamjena alfabeta brojčanom oznakom (Dujella, 2018)

Cezarovu šifru definiramo na sljedeći način:

$eK(x) = (x + K) \bmod 26,$

$dK(y) = (y – K) \bmod 26.$ mod 26 – ostatak cjelobrojnog dijeljenja sa 26

Originalna Cesarova šifra ima ključ K=3, odnosno pomicanje alfabeta za točno tri mjesta udesno. Poznavajući kriptosustav (Kerckhoffsovo načelo) i ključ, vrlo je jednostavno otvoreni tekst pretvoriti u šifrat i obrnuto. Problem nastaje kada nam je K nepoznat.

Primjer 1: Potrebno je dekriptirati šifrat TXNOJP dobiven Cezarovom šifrom.

Budući da nam je nepoznat ključ šifriranja, morat ćemo pristupiti kriptoanalizi. Prostor ključeva (skup svih mogućih vrijednosti ključeva) mali je (ima ih samo 26, odnosno 25 budući da bi upotreba ključa 0/26 dalo identičan otvoreni tekst i šifrat) te taj problem možemo riješiti takozvanom „grubom silom" (engl. *brute force*). Napad grubom silom na šifrat napad je pri kojemu isprobavamo sva moguća rješenja dok ne nađemo odgovarajuće. U našem slučaju imamo šifrat pa isprobavamo redom ključeve K=1,2,3… dok ne nađemo neki koji nam daje smisleni tekst.

T	X	N	O	J	P
S	W	M	N	I	O
R	V	L	M	H	N
Q	U	K	L	G	M
P	T	J	K	F	L
O	S	I	J	E	K

Tablica 5. Dekriptiranje uporabom grube sile

Znači, ključ je K=5, a otvoreni tekst je OSIJEK.

Kao što se primjećuje, Cesarova šifra uz jednostavni ključ vrlo je jednostavna za dekriptiranje. Da bismo dobili nešto sigurniju šifru, u funkciju za šifriranje trebamo uvrstiti više od jednog parametra te upotrebljavamo sljedeću afinu funkciju:

f(x)=*a*x+b uz uvjet da je parametar *a* prost broj unutar skupa mod(26), kao i njegov multiplikativni inverz a^{-1}.

Tablica vrijednosti parametra *a* i multiplikativnog inverza a^{-1} u skupu Z_{26}:

a	1	3	5	7	9	11	15	17	19	21	23	25
$\mathbf{a^{-1}}$	1	9	21	15	3	19	7	23	11	5	17	25

Tablica 6. Vrijednosti parametra *a* i multiplikativnog inverza a^{-1} (Dujella, 2018)

Primjer 2: Potrebno je šifrirati otvoreni tekst OSIJEK uz K=(5,3)

Zamjenjujući slova OSIJEK njihovim vrijednostima prema ranije navedenoj Tablici 4. (14,18,8,9,4,10) te upotrebom K=(5,3) -> a = 5; b = 3 dobijemo:

14x5 + 3 = 73, 73 mod 26 = 21
18x5 + 3 = 93, 93 mod 26 = 15
8x5 + 3 = 43, 43 mod 26 = 17
9x5 + 3 = 48, 48 mod 26 = 22
4x5 + 3 = 23, 23 mod 26 = 23
10x5 + 3 = 53, 53 mod 26 = 1

Odnosno šifrat VPRWXB.

Primjer 3: Potrebno je dekriptirati šifrat OZWHRYEZCVWFCTPCUWRCFPYHWI dobiven afinom šifrom

U svojoj knjizi, Dujella i Maretić (2007) opisuju da afina funkcija f(x)=ax+b ima ukupno 12 permutacija za vrijednost a te 26 za vrijednost b, ukupno je moguće 12x26=326 ključeva. Iako je i ovdje moguće primijeniti nasilni (engl. *brute force*) napad, postoji i znatno elegantniji način za dekriptiranje. Ukoliko znamo kojim je jezikom pisan otvoreni tekst, moguće je prema frekvenciji slova „pogoditi" ključ. Najfrekventnija slova u hrvatskom jeziku su A, I, O, E, N, dok je u šifratu najzastupljenije C i W (4 puta).

$e_K(A) = ax0+b=b$, $e_K(I) = 8a+b$

Ako pretpostavimo da je $e_K(A) = C$, a $e_K(I) = W$, dobijemo b=2 i a=9 te otvoreni tekst glasi:

KRIPTOGRAFIJA ZNACI TAJNOPIS

Cezarova i afina funkcija specijalni su slučajevi supstitucijske šifre. Prostor ključeva K može se sastojati od svih permutacija skupa skupa {0, 1, 2, ... , 25} gdje je

$$e_\pi(x) = \pi(x),\ d_\pi(y) = \pi^{-1}(y),$$

gdje je π^{-1} inverzna permutacija od π.

U ovom slučaju imamo 26! mogućih ključeva (1x2x3x4…x26), što je ≈ $4x10^{26}$ kombinacija te je napad upotrebom grube sile praktički nemoguć. Ovdje se kod dekriptiranja upotrebljava kao osnovna metoda analiza frekvencije slova. Broji se pojavljivanje svakog slova u šifratu te se distribucija slova u šifratu uspoređuje s poznatim podacima o distribuciji slova u jeziku otvorenog teksta. Vrlo je vjerojatno da najfrekventnija slova šifrata odgovaraju najfrekventnijim slovima jezika. Ta vjerojatnost raste s duljinom šifrata. Također mogu biti korisni i podatci o najčešćim bigramima (parovima slova) i trigramima (nizovima od tri slova) u jeziku.

FREKVENCIJA SLOVA (u promilima)				
A	115		K	36
I	98		V	35
O	90		L	33
E	84		M	31
N	66		P	29
S	56		C	28
R	54		Z	23
J	51		G	16
T	48		B	15
U	43		H	8
D	37		F	3

Tablica 7. Frekvencije pojedinih slova (Dujella, 2018)

Najfrekventnija slova u engleskom jeziku su: E, T, A, O, I, N, S, R, H, L; u njemačkom jeziku E, N, I, R, S, A, T, D, H, U, a u francuskom E, A, I, S, T, N, R, U, L, O.

Najfrekventniji bigrami u hrvatskom jeziku su: JE (2,7 %), NA (1,5 %), RA (1,5 %), ST, AN, NI, KO, OS, TI, IJ, NO, EN, PR (1,0 %).

Iako postoji veliki broj ključeva, supstitucijska šifra pokazala se vrlo jednostavnom za kriptoanalizu.

11.2.1.2. Vigenèreova šifra

Osnovni problem supstitucijske šifre je što svakom slovu otvorenog teksta odgovara jedno slovo šifrata. To je tzv. monoalfabetska šifra. Kako bi se pojačala sigurnost, u 16. stoljeću počinju se upotrebljavati polialfabetske šifre. Kod njih se svako slovo otvorenog teksta može preslikati u jedno od *m* mogućih slova, gdje je *m* duljina ključa. Prema Dujella i Maretić (2007) tu vrstu šifriranja prvi je opisao francuski diplomat Vigenère 1586. godine te se ta vrsta šifriranja prema njemu naziva *Vigenèreova šifra* (Dujella, 2018).

Pojednostavljeno, ključ nije broj kojim se množi ili zbraja, već je to riječ koja pretvorena u numerički ekvivalent tvori niz brojeva. Ako je ključna riječ OSIJEK (m=6) numerički ekvivalent je ključ K=(14,18,8,9,4,10). Ukoliko je ključna riječ kraća od otvorenog teksta, a gotovo uvijek u pravilu jeste, ona se jednostavno ponavlja koliko puta treba. Ako želimo šifrirati otvoreni tekst HRVATSKA, čiji je numerički ekvivalent (7,17,21,0,19,18,10,0), šifriranjem dobijemo:

	14	18	8	9	4	10	14	18
+	7	17	21	0	19	18	10	0
Mod26	21	9	3	9	23	2	24	18

Tablica 8. Šifriranje riječi HRVATSKA - numerički ekvivalent

Odnosno:

Ključ	O	S	I	J	E	K	O	S
Otvoreni tekst	H	R	V	A	T	S	K	A
šifrat	V	J	D	J	X	C	Y	S

Tablica 9. Šifriranje riječi HRVATSKA - numerički ekvivalent

Primjećujemo da se prvo slovo A iz otvorenog teksta preslikalo u J, a posljednje A u S. Time se izbjegava mogućnost kriptoanalize na temelju frekvencije pojave slova, bigrama i trigrama. Takva vrsta šifri naziva se blokovna šifra budući da se ključ šifriranja pojavljuje (ponavlja) u blokovima. Postoje i druge inačice Vigenèreove šifre, kao npr. s autoključem (engl. *autokey*) u kojoj se originalni ključ upotrebljava samo za šifriranje prvog bloka (od *m* znakova), a dalje se upotrebljava prethodni blok otvorenog teksta. U našem primjeru, za prvih šest znakova koristio bi se originalni ključ OSIJEK, dok bi se za posljednja dva koristio početak otvorenog teksta HR.

Dujella i Maretić (2007) navode Vigenèreova šifru kao jedan je od najdugovječnijih i najpopularnijih kriptosustava u povijesti. Koristila se intenzivno tijekom Američke revolucije te Američkog građanskog rata.

Iako na prvi pogled ovu šifru izgleda gotovo nemoguće probiti, što je čak objavljeno i u časopisu „Scientific American" 1917. godine, već krajem 19. stoljeća započeli su procesi koji će dovesti do njezinog uspješnog dekriptiranja. Prvi je korak određivanje duljine ključne riječi (Dujella i Maretić 2007).

Pretpostavka je da će dva identična odsječka otvorenog teksta biti šifrirana na isti način ukoliko se njihove početne pozicije razlikuju za neki višekratnik od m (koristit će kao ključ isti dio ključne riječi). Posljedično, ako uočimo dva identična odsječka u šifratu, duljine barem tri (odsječci duljine 2 često budu slučajni), tada je vrlo vjerojatno da oni odgovaraju identičnim odsječcima otvorenog teksta. U šifratu tražimo parove identičnih odsječaka (duljine barem 3) te zabilježimo udaljenosti između njihovih početnih položaja. Većina udaljenosti između tih parova trebala bi biti djeljiva s m, odnosno nekim njegovim višekratnikom. Ta se metoda zove Kasiskijev test, a uveo ju je Friedrich Kasiski 1863. godine (Dujella i Maretić 2007).

Nakon saznanja duljine ključa *m*, pristupa se metodi indeksa koincidencije. Sama metoda opisana je u knjizi Dujella i Maretić (2007), a sastoji se u tome da se šifrat stavi u matricu s *m* stupaca te se iščitava učestalost pojavljivanja određenog slova u pojedinom stupcu šifrata budući da smo cijelu Vigenèreovu šifru zapravo rastavili na *m* Cesarovih šifri. Treba napomenuti da za uspjeh u rješavanju šifri nije bitna sposobnost da se poznaje jezik originalnog teksta mada je barem poželjna sposobnost pisanja.

11.2.1.3. Polialfabetska šifra - Playfairova šifra

Dujella i Maretić (2007) iznose da osnovna ideja tog načina šifriranja jeste da umjesto šifriranja slova šifriramo blokove slova od dva elementa (bigrami). Problem realizacije ove ideje je da umjesto 26 elemenata imamo 26 x 26 blokova, odnosno 676

elemenata otvorenog teksta. Algoritam za šifriranje temelji se na matrici 5 x 5 slova koja se konstruira koristeći ključnu riječ, a dalje se upisuju redom preostala slova alfabeta. Ako je ključna riječ OSIJEK, matrica izgleda ovako:

O	S	I	J	E
K	A	B	C	D
F	G	H	L	M
N	P	R	Q	T
U	VW	X	Y	Z

Tablica 10. Izrada Playfairove matrice - ključna riječ OSIJEK

Budući da matrica ima 25 znakova, a alfabet 26, u engleskom jeziku slova I i J se poistovjećuju odnosno jednako šifriraju. U hrvatskom jeziku, da bismo izbjegli moguće nesporazume, poistovjećujemo slova V i W.

Šifriranje se provodi na sljedeći način. Prvo se blokovi otvorenog teksta podijele na blokove po dva slova pazeći da se ni jedan blok ne sastoji od dvaju istih znakova i da je ukupna duljina teksta parna! Oboje postižemo umetanjem slova X gdje je potrebno. Šifriranje se dalje obavlja slijedeći tri pravila ovisno o položaju slova u dobivenoj matrici. Kao primjer koristimo otvoreni tekst SLAVONIJA, odnosno šifriramo parove SL AV ON IJ AX

1. Ako se slova nalaze u istom retku, mijenjamo ih sa slovima koja se nalaze jedno mjesto udesno. Ukoliko dođemo posve do kraja desno, nastavljamo od početka reda, s lijeve strane. IJ -> JE
2. Ako se slova nalaze u istom stupcu, mijenjamo ih sa slovima koja se nalaze jedno mjesto ispod. Ukoliko dođemo posve do kraja dolje, nastavljamo od početka stupca, s gornje strane. ON -> KU, AV -> GS
3. Ako nije zadovoljen ni jedan gore navedeni, uvijek gledamo pravokutnik koji tvore slova te ih zamjenjujemo sa slovima s preostala dva kuta tog pravokutnika. Redoslijed određujemo tako da uzmemo prvo ono slovo koje je u istom retku kao i prvo slovo u našem bloku. SL – JG, AX -> BV

Kriptiranjem otvorenog teksta SLAVONIJA pomoću Playfairove šifre s ključem OSIJEK dobijemo šifrat JGGSKUJEBV.

Dujella i Maretić (2007) navode kako je Playfairovu šifru smislio britanski znanstvenik Charles Wheatstone 1854. godine, a ime je dobila prema barunu Playfairu koji ju je popularizirao. Ta vrsta šifre ima nekoliko značajnih prednosti pred monoalfabetskom supstitucijskom šifrom. Budući da je bigramska (blokovi od 2), u šifratu se gube jednoslovne riječi („a", „i", „u") koje znatno utječu na frekvenciju. Broj bigrama je 676 što je znatno više od standardnih 26 individualnih slova, a i njihova je frekvencija pojavljivanja znatno ujednačenija. Zbog svega toga dugo se vremena smatrala sigurnom i korištena je kao standardna šifra u britanskoj vojsci za vrijeme prvog svjetskog rada, a čak u nekim slučajevima i kasnije.

Ipak, i ta šifra nije u potpunosti sigurna. Kod dugih tekstova šifra postaje nesigurna jer se može koristiti analiza frekvencije bigrama. U otvorenom tekstu najfrekventnije slovo u engleskom jeziku ima učestalost oko 13 %, u šifratu dobivenom Playfairovom šifrom ona iznosi oko 7 %. Također, postoji i metoda vjerojatne riječi koja nam omogućava da pokušamo pogoditi visokofrekventne bigrame (Dujella i Maretić, 2007).

11.2.1.4. Hillova šifra

Godine 1929. Lester Hill predložio je poligramsku šifru kod koje se *m* uzastopnih slova otvorenog teksta zamjenjuje sa *m* slova u šifratu. Za upotrebu ključa preporučio je upotrebu invertibilne matrice (Dujella i Maretić, 2007). Taj sustav već s matricama 3 x 3 skriva ne samo frekvencije slova nego i frekvencije bigrama. Korištenje matrica sa $m \geq 5$ čini ovaj sustav gotovo potpuno sigurnim.

Ipak, ovu je šifru vrlo lako razbiti pomoću napada „poznati otvoreni tekst". Kod tog napada uspoređuje se poznati tekst koji nije kriptiran sa svojim šifratom te se iz toga u ovom slučaju može jednostavno saznati ključ. Za taj napad potrebno je imati jednu šifriranu poruku i njezin otvoreni tekst. Poznavanjem ključa moguće je čitati sve daljnje poruke nastale njegovom uporabom.

11.2.1.5. Jednokratna bilježnica

U želji za definiranjem savršeno sigurnog kriptosustava zaključeno je da je isti moguć samo uz uvjet da šifrat ne daje nikakvu informaciju o otvorenom tekstu. Dujella i Maretić (2007) iznose da je to moguće ako i samo ako je svaki ključ korišten s istom vjerojatnošću i da za svaki šifrat postoji jedinstveni ključ. Realizacija je toga tzv. jednokratna bilježnica. Ovaj sustav ne radi sa slovima već bitovima (nule i jedinice), a otvoreni tekst, šifrat i ključ nizovi su bitova duljine n. Budući da je postupak šifriranja jednostavno zbrajanje bitova otvorenog teksta i ključa, sustav je vrlo lako razbiti

napadom „poznati otvoreni tekst“. Sigurnost tog sustava postiže se samo ako se svaki ključ koristi samo jedanput. Također, problem predstavlja i to što ključ mora biti jednako dug kao i sama poruka.

11.2.2. TRANSPOZICIJSKE ŠIFRE

Kao što smo već naveli, transpozicijske šifre one su kod kojih ne mijenjamo elemente otvorenog teksta, već im mijenjamo međusobni položaj. Najupotrebljavanija transpozicijska šifra u praksi bila je stupčana transpozicija. Otvoreni tekst upisuje se u pravokutnik po recima, a poruka se čita po stupcima, ali s promijenjenim poretkom prema ključu. Kao i kod ostalih šifri, ukoliko se posljednji redak ne ispuni do kraja, prazna mjesta se pune proizvoljnim slovima.

Šifriranje otvorenog teksta:

INFORMACIJSKA SIGURNOST I PRIVATNOST

Stupčanom transpozicijom s ključem: 5 2 7 4 1 3 6

KLJUČ	**5**	**2**	**7**	**4**	**1**	**3**	**6**
	I	N	F	O	R	M	A
OTVORENI	C	I	J	S	K	A	S
TEKST	I	G	U	R	N	O	S
	T	I	P	R	I	V	A
	T	N	O	S	T	X	W

Tablica 11. Šifriranje izraza: INFORMACIJSKA SIGURNOST I PRIVATNOST

Šifrat je:

RKNITNIGINMAOVXOSRRSICIITASSAWFJUPO

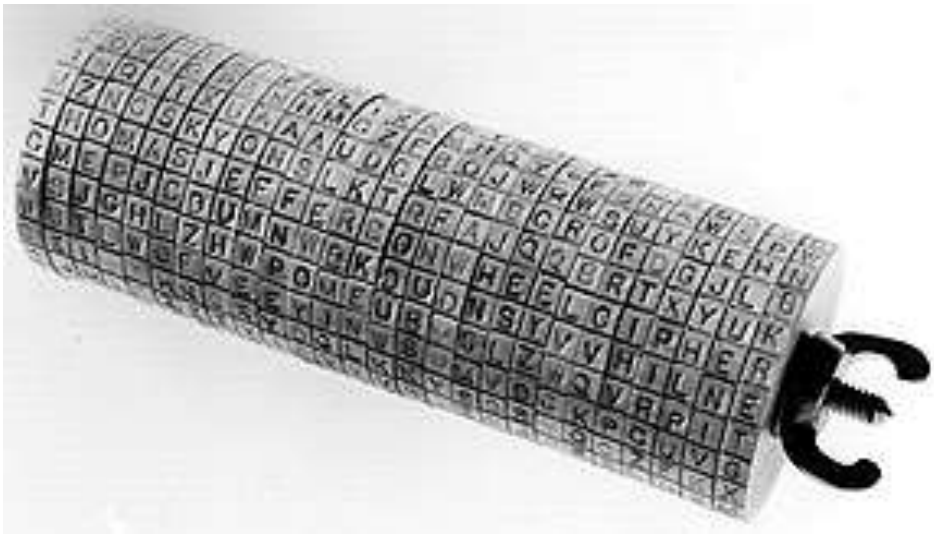
Dekriptiranje transpozicijske šifre provodi se tako da se prvo odredi dimenzija pravokutnika. Broj slova u šifratu faktorizira se i dobijemo nekoliko odgovarajućih dimenzija. U našem slučaju to je 35, odnosno 5x7 i 7x5. Da bi se odredio ispravni format, promatra se odnos samoglasnika i suglasnika u svakom retku. Prema Dujella i Maretić (2007) taj bi odnos trebao biti blizak odnosu u jeziku otvorenog teksta (u hrvatskom 43 % : 57%) Nakon utvrđivanja ispravnog oblika, stupce možemo pokušati anagramirati ili možemo pokušati koristiti frekvencije najčešćih bigrama između parova stupaca. Oni parovi stupaca koji imaju najveće vrijednosti vjerojatno se nalaze jedan pored drugoga.

11.2.3. NAPRAVE ZA ŠIFRIRANJE

Upotrebom naprava za šifriranje kriptosustavi se mogu učiniti kompliciranijima i sigurnijima. Te naprave čine proces šifriranja i dešifriranja bržim a prostor ključeva većim.

11.2.3.1. Jeffersonov kotač

Jedna od prvih upotrebljenih naprava bio je Jeffersonov kotač za šifriranje. Sastojao se od cilindra na kojemu se nalazilo 26 diskova, svaki sa 26 kvadratića na kojima se proizvoljno nalaze slova engleskog alfabeta. Ti diskovi mogu se neovisno rotirati. Šifriranje se obavlja tako da se na jednom retku dobije otvoreni tekst, a kao šifrat koristi se bilo koji od preostalih 25 redaka (Dujella i Maretić, 2007).



Slika 3. Jeffersonov kotač za šifriranje (University of Virginia, 2005)

Dešifriranje se obavlja tako da se rotiranjem diskova u jednom retku dobije šifrat. Sada se između preostalih 25 redaka potraži onaj koji sadrži neki smisleni tekst i taj redak predstavlja otvoreni tekst.

11.2.3.2. Hebernov električni stroj za kodiranje

Dujella i Maretić (2007) opisuju električni uređaj kojim su se dva električna pisača stroja spajala pomoću 26 žica, ali razbacanim rasporedom. Pritiskom na tipku na

pisaćem stroju za otvoreni tekst drugi bi stroj otipkao šifrat tog slova. Dvije godine kasnije u uređaj je ugradio pet tzv. „rotora". Rotori su na svakoj strani imali po 26 električnih kontakata, a okretanje rotora mijenjalo je nasumične spojeve s kontaktima na drugoj strani. Upotreba pt rotora omogućavala je polialfabetsku supstituciju sa 265 kombinacija, odnosno nešto više od 11 milijuna.

11.2.3.3. ENIGMA

Slika 4. ENIGMA (Wikipedija)

Dujella i Maretić (2007) navode kako je Arthur Scherbius, njemački inženjer, izradio i patentirao 1918. godine ENIGMA uređaj, rotorsku mašinu s mogućnošću kodiranja i prijenosa poruka. Za razliku od ostalih rotorskih naprava, ENIGMA je imala tri odnosno pet zupčanika koji su rotore mogli pomicati u nepravilnom slijedu. Neposredno pred Drugi svjetski rat započelo je njezina masovna upotreba u njemačkoj vojsci i mornarici te je tako nastao najpoznatiji stoj za šifriranje. Enigma je bila elektromehanička naprava koja je imala tipkovnicu sa 26 tipki za unos teksta, zaslon sa 26 žaruljica koje su prikazivale šifrirani izlaz, tri (kasnije pet) mehaničkih rotora i električne prespojne ploče. Rotori su bili smješteni tako da se kontakti među njima dodiruju pa je izlaz iz jednoga bio ulaz u drugi. Nakon svakog šifriranog slova prvi bi se rotor okrenuo za jedan kontakt, a kad bi načinio potpuni krug, uzrokovao bi okretanje sljedećeg rotora. Na taj način kodiranje istog slova otvorenog teksta nikada

nije završavalo istim šifratom te je stoga frekvencijska analiza bila neprikladna. Tri rotora sa 26 kontakata daju 263 kombinacija, odnosno 17576.

Kako bi se povećala sigurnost, korišteni su izmjenjivi rotori i prespojni kablovi. Mehanički identični rotori imali su različite električne spojeve te su međusobnom zamjenom mjesta omogućavali 3! = 6 permutacija. Prespojna ploča omogućavala je zamjenu nekih slova prije ulaska u prvi rotor. U početku se koristilo šest prespojnih kablova, a kasnije 10. Kod upotrebe šest kablova ukupan broj kombinacija veći je od 100 milijardi, a kod 10 kabela veći od 150.000 milijardi, što čini „brute force" napad nemogućim. Proboj u kriptoanalizi ENIGME omogućilo je poznavanje procedure šifriranja te jedna nehotična pogreška u proceduri koja je korištena kako bi se osigurala ispravnost primljene poruke.

Šifriranje se odvijalo na sljedeći način. Svaki mjesec operaterima ENIGME bila je dostavljana nova knjiga s ključevima za svaki dan u tom mjesecu. Ključevi su se sastojali od tri dijela: postavke na prespojnoj ploči, raspored rotora i početne orijentacije rotora. Budući da su se dnevno šifrirale velike količine poruka, kako bi se osigurala jedinstvenost ključa, na početku poruke slan je ključ za samu poruku šifriran pomoću dnevnog ključa. Tako su sve poruke slane taj dan imale iste postavke prespojne ploče, isti raspored rotora, ali različitu orijentaciju. Sukladno dnevnom ključu pošiljatelj bi odabrao novu orijentaciju za ključ i uvrstio je u šifrat na početku poruke, ali dvaput kako bi bio siguran da je primatelj dobio ispravan ključ. Ostatak poruke šifrirao bi se upotrebom nove orijentacije. Primatelj bi šifrat koji bi dobio dešifrirao koristeći dnevni ključ za prvih 6 slova šifrata, a za ostalo bi koristio novodobiveni ključ za poruku. Upravo to ponavljanje (1=4, 2=5, 3=6) korišteno je za kriptoanalitički napad na ENIGMU (World Science Festival, 2013).

11.2.3.4. BOMBA

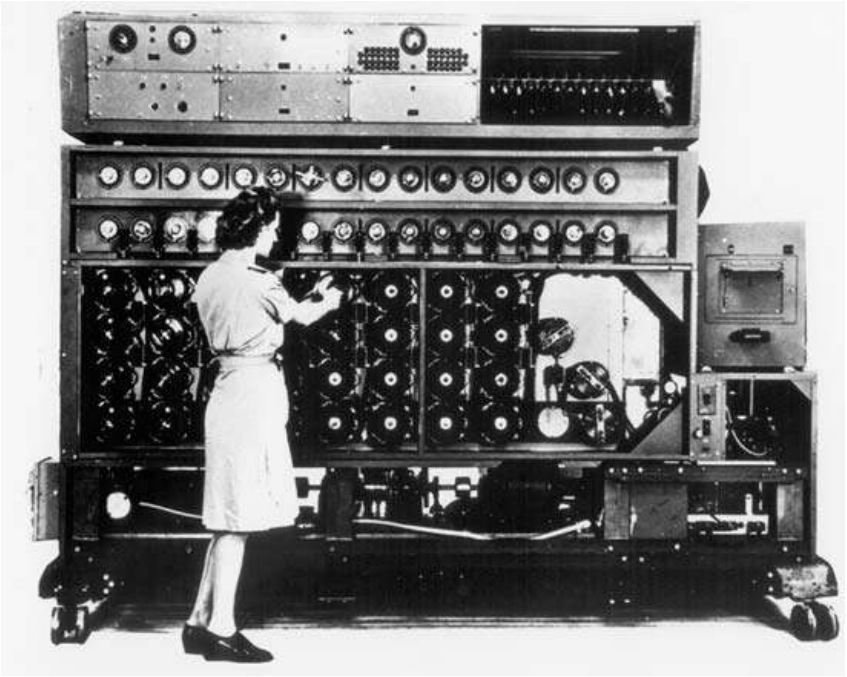
Britanska vojna obavještajna (MI-6) služba dugo je vremena, još od početka Prvog svjetskog rata, uspješno presretala i dešifrirala njemačke vojne, diplomatske i komercijalne poruke (Kahn, 1979). Dolaskom nacista na vlast važnost tajnovitosti ističe se u prvi plan te 1934. godine njemačke vlasti počinju mijenjati šifriranje novim sustavom. Više od četiri godine britanske službe tapkale su u mraku dok 1938. godine nisu saznali da se njemačka vojska koristi uređajem za šifriranje zvanim ENIGMA.

Prvi proboj u dešifriranje ENIGME napravili su poljski matematičari M. Rajewski i H. Zygalski (Copeland, 2010) na temelju ranije opisanih njemačkih uputa za uporabu ENIGME koje je nabavila francuska obavještajna služba. Koristeći dupliranje ključa na početku njemačkih poruka, počeo je osmišljavati metodu za probijanje ENIGME. Ako je ključ ABC, zapisan je dvaput kao ABCABC i šifriran u npr.

FOESCG, Rejewski zaključuje da su F i S šifrat istog slova A, kao i parovi (O,C) i (E,G) kao što opisuje Hrvoje Čavrak u *Hrvatskom matematičkom elektronskom časopisu*: http://e.math.hr/enigma/index.html. To ponavljanje omogućilo je Poljacima da detektiraju uzorke i lance sljedivosti slova te da dužina lanaca ne ovisi o prespojnim pločama, već isključivo o postavkama rotora. Stoga, umjesto 150.000 milijardi kombinacija nakon godinu dana kategorizacije popisano je svih 105.456 mogućih kombinacija rotora. Svakog dana, nakon dovoljnog broja prikupljenih poruka i uočenih lanaca, Rejewski je pomoću svoje baze podataka o postavkama, postavke rotora i rezultirajućih lanaca u njima, pronašao odgovarajući. Time je otkrio postavke dnevnih postavki rotora, a rješavanje prespojne ploče, koja može imati milijarde prespojnih kombinacija, svelo se na problem obične supstitucijske šifre. Nakon što su Nijemci 1939. godine dodali još dva rotora u uređaj ENIGME, povećali broj prespojnih kablova na 10 te prestali ključeve u poruci slati dvaput, dešifriranje ENIGME opet je bilo onemogućeno. Neposredno pred napad Njemačke na Poljsku, Poljaci su poslali Britancima svu dokumentaciju koja se odnosi na ENIGMU.

Brown (1975) opisuje kako su Britanci već imali odjel za kriptoanalizu smješten u Bletchley Parku koji je postao sjedište savezničkih nastojanja za dešifriranje ENIGME. Mladi engleski matematičar Alan Turing osmislio je „Univerzalni stroj", uređaj koji je mogao simulirati rad bilo kojeg drugog uređaja. Iako su govorili da je izgradnja takvog uređaja nemoguća, da bi bio velik kao katedrala sv. Pavla, da bi zahtijevao da cijelo sveučilište samo obučava radnike za njegovo održavanje te da bi trebala jedna hidroelektrana za njegovo napajanje, Alan Turing nije odustajao te je 1938. godine napravljena BOMBA veličine 2,5 x 2,5 metra.

Traženje lanaca slijedivosti slova, koje su Poljaci ručno uspoređivali s bazom, za Britance je obavljao stroj BOMBA, a sve takve poruke dobivene kriptoanalizom bile su označene kao poruke ULTRE.



Slika 4. BOMBA, uređaj za dekriptiranje ENIGME - Encyclopedia Britannica

11.2.3.5. Važnost kriptoanalize

Brown (1975) pojašnjava kako je omogućavanje Britanaca da čitaju gotovo sve poruke njemačke vojske, mornarice i zrakoplovstva bilo ključno za zaustavljanje nacističke Njemačke. Rommel je u Africi pobijeđen kada je ostao bez goriva i streljiva. U očajničkom pokušaju dostave streljiva i goriva tijekom prijelomnih trenutaka uoči bitke za El Alamein, pet brodova isplovilo je iz pet talijanskih luka tijekom noći, no zahvaljujući porukama ULTRE, svih pet brodova presreli su britanski razarači i potopili ih. Zaustavljanje njemačkih podmornica i osiguravanje pomorskih linija također je jedna od zasluga ULTRE. Dan D, savezničko iskrcavanje u Francuskoj omogućile su obmane i čitanje poruke njemačke vrhovne komande. Poruke ULTRE bile su najvažniji događaj na putu poraza nacističke Njemačke.

11.2.4. MODERNI SIMETRIČNI BLOKOVNI KRIPTOSUSTAVI

Kao što smo već rekli, simetrični sustavi oni su kod kojih se ključ za dešifriranje može izračunati poznavajući ključ za šifriranje i obratno. Ti su ključevi najčešće identični, a sigurnost je u tajnosti ključa.

Krajem 60-ih i početkom 70-ih godina 20. stoljeća, razvojem financijskih transakcija, pojaviljuje se potreba za šifrom kojom će se moći koristiti korisnici širom svijeta i u koju će svi imati povjerenje.

Dujella i Maretić (2007) opisuju kako je 1972. godine američki National Bureau of Standards (NBS) inicirao program za zaštitu računalnih i komunikacijskih podataka čiji je jedan od ciljeva bilo i razvijanje standardnog kriptosustava koji je trebao zadovoljiti sljedeće uvjete:

- ✓ visoki stupanj sigurnosti
- ✓ potpuna specifikacija i lako razumijevanje algoritma
- ✓ sigurnost je u ključu, a ne u tajnosti algoritma
- ✓ dostupnost svim korisnicima
- ✓ prilagodljivost uporabi u različitim primjenama
- ✓ ekonomičnost implementacije u elektoničkim uređajima
- ✓ učinkovitost
- ✓ mogućnost provjere
- ✓ mogućnost izvoza (zbog američkih zakona).

11.2.4.1. Data Encryption Standard (DES)

DES je nastao na osnovi zahtjeva NBS-a, a temeljio se na specijalnoj vrsti blokovske šifre – Feistelovoj šifri. Osnovnu ideju iznio je tim kriptografa IBM-a, a doradila ju je NSA. Kao standard prihvaćen je 1976. godine kada je dobio i ime. Dujella i Maretić (2007) opisuju da je glavna ideja upotreba supstitucija i transpozicija kroz više iteracija. DES šifrira otvoreni tekst duljine 64 bita koristeći ključ K duljine 56 bitate dobija šifrat duljine 64 bita. Procedura se sastoji od triju etapa:

1. permutiranje otvorenog teksta fiksnom inicijalnom permutacijom
2. primjena F funkcije (16 rundi iteracija)
3. inverzna permutacija dobivenog međuteksta.

Koraci 1 i 3, permutacija i inverzna permutacija, osiguravaju da se isti čip i isti algoritam koriste i za kriptiranje i dekriptiranje. F funkcija, koja se sastoji od osam supstitucijskih S kutija, provodi se 16 puta kako bi se izrazio tzv. lavinski učinak. Lavinski učinak označava zahtjev da svaka, pa i najmanja promjena ulaznih vrijednosti, rezultira velikom promjenom izlaznih vrijednosti. Ukoliko isti otvoreni tekst šifriramo pomoću dvaju ključeva koji se razlikuju samo u jednom bitu, dobivamo razlike prema tablici:

Runda	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Broj bitova koji se razlikuju	0	2	14	28	32	30	32	35	34	40	38	31	33	28	26	34	35

Tablica 12. Razlike u šifriranju otvorenog teksta

Budući da je učinak lavine izražen već kod tri iteracije, 16 rundi se koristi iz razloga da kriptoanalitički napad ne bude učinkovitiji od napada grubom silom. Budući da je ključ 56-bitni, postoji 2^{56} ključeva, odnosno $7{,}2 \times 10^{16}$. Pretpostavljalo se da će do 1990. godine DES postati nesiguran budući da bi se razvojem računala moglo u razumnom vremenu isprobati sve kombinacije ključa. Prvi puta DES je razbijen 1998. godine računalom koje je koštalo 250.000 $, a trebalo mu je 56 sati za dekriptiranje poruke.

Kao prijelazno rješenje zaštite podataka 1990-ih godina pojavila se ideja povećanja duljine ključa te se počeo koristiti trostruki DES. Iako je njegova duljina ključa 3x56=168 bita, zbog mogućnosti tzv. napada u sredini, broj potrebnih operacija napada je 2^{112} odnosno 5×10^{33}.

11.2.4.2. Advanced Encryption Standard (AES)

Dujella i Maretić (2007) navode „Napredni standard za enkripciju" (AES) kao glavni standard koji se danas koristi za zaštitu podataka od nedopuštenog pristupa i enkripciju podataka. Ključ koji se koristi za kriptiranje podataka može biti različitih duljina. Ovisno o duljini ključa postoje AES-128, AES-192 ili AES-256. Umjesto Feistelove F funkcije AES koristi substitucijsko-permutacijsku mrežu. Razvili su ga Belgijanci Daemen i Rijmen kao RIJNDAEL sustav, a nakon prihvaćanja kao standarda, promijenio je ime u AES. S kutije su dizajnirane tako da kriptosustav bude što otporniji na tzv. diferencijalnu i linearnu kriptoanalizu.

11.2.5. ASIMETRIČNI KRIPTOSUSTAVI

11.2.5.1. Kriptografija javnim ključem

- ✓ Dujella i Maretić (2007) opisuju ideju javnog ključa koja se sastoji u tome da se konstruira kriptosustav kod kojega bi iz poznavanja funkcije šifriranja bilo nemoguće izračunati funkciju dešifriranja. Tada bi funkcija šifriranja mogla biti javna.

- ✓ Kriptiranje se obavlja na način da, ako pošiljatelj A želi poslati poruku x primaocu B, onda B najprije pošalje A svoj javni ključ e_B, potom A šifrira svoju poruku pomoću e_B i pošalje primaocu šifrat $y = e_B(x)$. Konačno, B dešifrira šifrat koristeći svoj tajni ključ za dekriptiranje d_B.
- ✓ Glavne prednosti kriptosustava s javnim ključem u usporedbi sa simetričnima su: nema potrebe za sigurnim komunikacijskim kanalom za razmjenu ključeva, za komunikaciju grupe od N ljudi treba 2N ključeva, za razliku od N(N-1)/2 ključeva kod simetričnog kriptosustava, mogućnost potpisa poruke.
- ✓ Osnovni razlog zašto se javni ključ ne koristi za šifriranje poruka jest da su algoritmi s javnim ključem znatno sporiji (oko 1000 puta) od modernih simetričnih algoritama. Drugi nedostatak kriptosustava s javnim ključem jest da su slabi na napad „odabrani otvoreni tekst".
- ✓ U stvarnom svijetu kriptografija javnog ključa ne predstavlja zamjenu za simetrične kriptosustave. Ona se ne koristi za šifriranje poruka, već za šifriranje ključeva. Naime, osobe A i B komuniciraju pomoću simetričnog kriptosustava s ključem koji su razmijenili pomoću kriptosustava s javnim ključem. To se zove hibridni kriptosustav.
- ✓ U modernoj kriptografiji, koja se koristi u komercijalnom svijetu (tipična situacija je da osoba A želi kupiti nešto od osobe B upotrebom interneta), pojavljuju se, uz klasične, i neki sasvim novi problemi:
  - o POVJERLJIVOST (engl. *confidentiality*): Poruku koju osoba A šalje osobi B ne može pročitati nitko drugi.
  - o VJERODOSTOJNOST (engl. *autenticity*): Osoba B zna da je samo osoba A mogla poslati poruku koju je ona upravo primila.
  - o NETAKNUTOST (engl. *integrity*): Osoba B zna da poruka koju je poslala osoba A nije promijenjena prilikom slanja.
  - o NEPOBITNOST (engl. *non-repudiation*): Osoba A ne može kasnije zanijekati da je poslala poruku.

11.3. KRIPTOGRAFIJA U PRAKSI

Neki su od primjera današnje primjene kriptografije svakako internetsko bankarstvo kojim se koristi sve veći broj korisnika interneta, zatim tu su različite kriptovalute od kojih je najpoznatija i najrasprostranjenija Bitcoin te izrazito opasan zloćudni računalni program *Cryptoloker* koji predstavlja trenutno najpoznatiju vrstu inter-

netske krađe podataka, engl. *ransomware*, programa koji zaključavaju korisničke podatke i traže za njih otkupninu.

11.3.1. INTERNETSKO BANKARSTVO

Internetsko bankarstvo odvija se upotrebom nesigurnog medija (interneta) koji je moguće neovlašteno prisluškivati. Zbog toga se sva komunikacija obavlja https protokolom koji kriptira komunikaciju na oba kraja. Sustav je kriptiranja ranije opisani AES, a razmjena ključeva obavlja se upotrebom kriptografije javnog ključa (Certifikat na kartici korisnika). Taj se način smatra sigurnijim nego razmjena autorizacijske lozinke putem tokena banke.

Budući da se autorizacija u sustav banke provodi korisničkim certifikatom koji se aktivira PIN-om, zbog sigurnosti preporučuje se vađenje kartice sa certifikatom kada se ne koristi. Budući da postoje neželjeni programi koji vam se mogu instalirati na računalo te pratiti i sve unose na tipkovnici te u pozadini sami pokrenuti neku bankovnu transakciju, u posljednje se vrijeme preferira i 2FA (engl. *Two Factor Authentication* - autentifikacija u dva koraka). To obično traži dodatni uređaj (mobitel, dodatni token ili sl.) na koji se šalje jednokratna lozinka za autentifikaciju. Tek u slučaju posjedovanja obiju lozinki i certifikata na kartici, korisnik je autentificiran u sustav.

11.3.2. KRIPTOVALUTE - BITCOIN

Upotreba kriptovaluta, odnosno u ovom primjeru bitcoina, primjer je upotrebe kriptografije s javnim ključem. Javni ključ bitcoinu služi kao funkcija iz koje računa adresu na koju šaljemo neki iznos, odnosno koristimo javni ključ osobe kojoj šaljemo sredstva, jednako kao što se kod kripografije služimo njime da nekome pošaljemo poruku. Privatnim, tajnim ključem, odobravamo transakciju sa svoga računa. Privatni je ključ 256-bitni broj, odnosno postoji oko 10^{77} brojeva mogućih ključeva.

Kao i svaki bitan podatak privatni ključ treba držati minimalno na dvama mjestima (preporuka na trima) te paziti da se ne izgubi. Svatko tko ima naš privatni ključ, može obaviti transakciju u naše ime.

11.3.3. CRYPTOLOCKER

Jedna je od vrsti internetske krađe podataka, engl. *ransmware*, zlonamjerni računalni program, trojanac, napravljen s ciljem „zaključavanja" odnosno kriptiranja korisničkih dokumenata te traženja otkupnine za njih. Budući da on nije virus, većina

antivirusnih programa neće ga detektirati. Program se koristi asimetričnom kriptografijom odnosno šifriranjem javnim i dešifriranjem tajnim ključem. Ovisno o inačici koristi različite algoritme, pa čak i 2048 bitni RSA ključ. Javni ključ pohranjuje se na napadnutom računalu i pomoću njega provodi se šifriranje, dok se tajni ključ (za dešifriranje) pohranjuje na nekom udaljenom serveru pod kontrolom napadača.

Nakon završenog kriptiranja podataka, od korisnika se traži otkupnina kako bi mu se dostavio tajni ključ kojim može dekriptirati svoje podatke.

Jedini učinkovit način zaštite podataka redovita je izrada sigurnosne kopije (engl. *backup*), kao i kod svih drugih mogućih uzroka gubitka podataka, tako i kod *cryptolockera*. Sigurnosna kopija bi se trebala izvoditi u redovitim vremenskim intervalima (tjedan, mjesec) te spremati izvan računala budući da neke inačice *cryptolocker-a* mogu zaključati i vanjske i mrežne diskove.

11.4. LITERATURA

Brown, A. C. (1975). *Bodyguard of lies*. New York, NY: Harper & Row.

Copeland, B. J. (21. siječnja 2010). *Ultra Allied Intelligence Project*. Preuzeto s https://www.britannica.com/topic/Ultra-Allied-intelligence-project, 12.7.2018.

Čavrak, H. (b.d.). ENIGMA. Preuzeto s http://e.math.hr/enigma/index.html, 12.7.2018.

Dujella, A. (b.d.). Viginereova šifra. Preuzeto s http://e.math.hr/vigenere/index.html, 12.7.2018.

Dujella, A. i Maretić, M. (2007). *Kriptografija*. Sveučilište u Zagrebu: ELEMENT.

Enigma. (b.d.). U: Wikipedia. Preuzeto s https://commons.wikimedia.org/wiki/File:Bundesarchiv_Bild_101I-241-2173-09,_Russland,_Verschl%C3%BCsselungsger%C3%A4t_Enigma.jpg, 12.7.2018.

Galinović, A. (2005). *Povijest kriptografije*. Preuzeto s http://web.zpr.fer.hr/ergonomija/2005/galinovic/index.html, 12.7.2018.

Kahn, D. (1979). *Šifranti protiv špijuna I-IV*. (CIP Zagreb, Trans.). New York, NY: The Codebreakers (originalni članak je objavljen 1967. godine).

Ledinek, S. (26. rujna 2016). Što je Ransomware i zašto nitko nije imun? Preuzeto s http://www.pcekspert.com/clanak/sto-je-ransomware-i-zasto-nitko-nije-imun/, 12.7.2018.

Lončar, Z. (16. studenog 2017). Kriptografija za smrtnike. Preuzeto s https://bitfalls.com/hr/2017/11/16/cryptography-mortals-lets-explain-public-private-keys/, 12.7.2018.

University of Virginia, Department of Computer Science: Cryptology - Principles and Applications (16. rujna 2016). Preuzeto s http://www.cs.virginia.edu/cs588/challenges/jeffersonwheel/, 12.7.2018.

World Science Festival. (14. svibnja 2013). The Enigma Machine Explained. Preuzeto s https://www.youtube.com/watch?v=ASfAPOiq_eQ, 12.7.2018.

izv. prof. dr. sc. Vesna Ilakovac

Medicinski fakultet Sveučilišta Josipa Jurja Strossmayera u Osijeku

Kristina Kralik, prof., predavač

Medicinski fakultet Sveučilišta Josipa Jurja Strossmayera u Osijeku

12. OSOBITOSTI ZAŠTITE PODATAKA U BIOMEDICINI I ZDRAVSTVU

Sažetak

U skupini osobnih podataka posebno se ističu podaci o zdravlju. Zbog svoje osjetljive prirode ti su podaci oduvijek imali poseban status. Od Hipokratove zakletve do najnovije Preporuke Vijeća Europe, podaci o zdravlju pokušavaju se zaštititi. Uz problem zaštite zdravstvenih podataka, razvoj interneta i lakoća objavljivanja različitih sadržaja otvorio je i problem zaštite korisnika interneta od neprimjerenih i neprovjerenih podataka o zdravlju kojima internet obiluje.

Ovo poglavlje govori o osobitostima podataka o zdravlju daje pregled dokumenata koji se bave njihovom zaštitom i dimenzija zaštite podataka skreće pozornost na opasnosti koje donose neprovjerene i neprimjerene informacije o zdravlju na internetu i daje upute gdje i kako se mogu pronaći pouzdane zdravstvene informacije na internetu.

12.1. OSOBITOSTI MEDICINSKIH I ZDRAVSTVENIH PODATAKA

Podaci o zdravlju i bolesti pojedinca oduvijek su imali poseban status. Još u antičko doba, ti su se podatci smatrali povjerljivim. Prvi tekst koji govori o čuvanju profesionalne liječničke tajne je Hipokratova prisega najstarija i najpoznatija medicinska prisega. Pretpostavlja se da datira iz 4. stoljeća prije Krista i unatoč tomu što se prema predaji vjeruje da je autor prisege sam Hipokrat, povjesničari ne znaju pouzdano tko ju je napisao (Hulkower, 2016). U antičkom tekstu Hipokratove prisege (Borovečki, Mustajbegović i Jakšić, 2013) stoji: „Što pri svojem poslu budem saznao ili vidio, pa i inače, u saobraćaju s ljudima, koliko se ne bude smjelo javno znati, prešutjet ću i zadržat ću tajnu.“. Uz obvezu čuvanja podataka o zdravlju i bolesti pacijenata s kojima dolazi u kontakt, liječnici su se navedenom prisegom obvezivali čuvati i sve druge tajne koje im povjeri bilo tko.

Suvremena je inačica Hipokratove prisege Ženevska liječnička prisega poznata i kao Ženevska deklaracija. Od svog prihvaćanja 1948. godine na 2. skupštini Svjetskog liječničkog udruženja (WMA prema engl. *World Medical Association*) doživjela je više izmjena i dopuna, posljednja je bila 2017. godine. Ženevsku liječničku prisegu polažu studenti medicine nakon završetka studija na mnogim svjetskim medicinskim fakultetima, pa tako i na medicinskim fakultetima u Republici Hrvatskoj. U posljednjoj inačici Ženevske liječničke prisege također se nalazi rečenica koja liječnike obvezuje na čuvanje tajne (Parsa-Parsi, 2017): „Poštovat ću tajne koje su mi povjerene, čak i nakon pacijentove smrti.“ Za razliku od Hipokratove prisege u Ženevskoj liječničkoj prisezi podaci o zdravlju i bolesti pacijenta nisu posebno istaknuti, ali se podrazumijeva da su i oni povjerljivi.

Što je to u podacima o zdravlju pojedinca što izaziva potrebu da ih se drži u tajnosti i štiti? Ukratko, to je strah od mogućih posljedica koje bi osoba mogla doživjeti ukoliko bi podaci o njezinom zdravlju postali javno dostupni. U stara vremena bolest se često poistovjećivala sa slabošću što je uglednim osobama rušilo autoritet. S druge strane, ljudi nižih društvenih slojeva čija je egzistencija ovisila o poslu koji rade nisu si mogli priuštiti „luksuz“ da zbog svoga zdravstvenoga stanja budu udaljeni s posla.

Unatoč tomu što suvremeno društvo ulaže velike napore u izgradnju tolerancije i razumijevanja za one koji su po bilo čemu različiti od većine, potreba za zaštitom podataka o zdravlju pojedinca u sve je većoj mjeri prisutna. Nekada ne mora biti ni riječ o bolesti, nego o prirodnom stanju u kojemu se mnoge mlade žene reproduktivne dobi nađu – u trudnoći. Poslodavci će naći stotinu razloga da u radni odnos ne prime ženu koja je trudna jer to znači da će uskoro morati tražiti novu osobu koja će preuzeti njezin posao, očekuju da će po povratku na posao često izbivati (jer su mala djeca često bolesna) itd.

Zloporaba podataka o zdravlju pojedinaca česta je i u javnim medijima. Godinama su stupce internetskih portala i drugih javnih glasila u Hrvatskoj punile vijesti o HIV pozitivnim djevojčicama i njihovim problemima pri upisu i pohađanju škole. Zbog neprihvaćanja i pritiska okoline, cijela je obitelj preselila u drugo mjesto, praćeni medijskim natpisima u kojima su bila navedena njihova imena i prezimena, mjesto iz kojega dolaze i u koje su se preselili i niz drugih detalja iz njihovog osobnog života (Starčević, 2005).

Nažalost, stigmatiziranje oboljelih u društvu često je i nije ograničeno samo na zarazne bolesti. S mnogim problemima u društvenom i profesionalnom životu susreću se i oboljeli od drugih bolesti, a osobito psihičkih bolesti. Stigma psihičke bolesti jedna je od vodećih prepreka zapošljavanju i zadržavanju posla osobe oboljele od psihičke bolesti što dovodi do njihove socijalne isključenosti (Štrkalj-Ivezić, John, Sučec, Grgin i Halić, 2010).

Upravo zato što zloporaba podataka o zdravlju može naštetiti pojedincu pa i široj zajednici, podaci o zdravlju predstavljaju posebnu kategoriju u skupini osobnih podataka kojima se pri postupanju (prikupljanju, prenošenju, obradi i sl.) treba osigurati i posebna zaštita.

12.2. ZAŠTITA PODATAKA U BIOMEDICINI I ZDRAVSTVU

12.2.1. DOKUMENTI O ZAŠTITI OSOBNIH I MEDICINSKIH PODATAKA I PODATAKA O ZDRAVLJU

Temelji zaštite privatnosti postavljeni su u Općoj deklaraciji o ljudskim pravima koja je usvojena i proglašena na Općoj skupštini Ujedinjenih naroda u prosincu 1948. godine. U članku 12. deklaracije (Odluka o objavi Opće deklaracije o ljudskim pravima, NN 12/2009) stoji: „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."

Razvojem tehnologije i automatske obrade podataka informacijska privatnost pojedinca postala je ozbiljno ugrožena. Neki od razloga za to su postupci koji su u sustavima s automatskom obradom podataka postali mogući:

- jednostavno pribavljanje i uporaba podataka koji nisu nužni za obavljanje nekog zadatka
- obrada podataka za svrhu koja nije bila unaprijed predviđena
- krađa i prijenos podataka

- neovlašteno mijenjanje ili brisanje podataka
- prikupljanje i povezivanje podataka o pojedincu iz različitih izvora na temelju čega se moglo dobiti opsežno znanje o osobnom životu pojedinca.

Prvi obvezujući međunarodni dokument koji štiti pojedince od zloporaba koje mogu pratiti automatsko prikupljanje i obradu osobnih podataka je Konvencija za zaštitu osoba glede automatizirane obrade osobnih podataka, poznata i kao Konvencija Vijeća Europe broj 108 iz 1981. godine (Council of Europe, 1981). Konvencija definira osobni podatak kao „svaku obavijest koja se odnosi na određenog ili odredivog pojedinca" i postavlja temeljna načela zaštite osobnih podataka:

- zakonitost – osobni podaci trebaju biti pribavljeni i obrađeni u dobroj vjeri i zakonito
- svrha – osobni podaci trebaju biti pohranjeni s određenom i zakonitom svrhom i u druge se svrhe ne smiju koristiti
- opseg – osobni podaci moraju biti primjereni, relevantni i ne prekomjerni s obzirom na svrhe u koje su pohranjeni
- točnost – osobni podaci trebaju biti točni
- trajnost – osobni podaci trebaju biti pohranjeni u obliku koji omogućuje identifikaciju osobe onoliko dugo koliko je potrebno da se zadovolji svrha zbog koje su podaci pohranjeni.

Konvencija zdravstvene podatke svrstava u posebnu kategoriju podataka koji se ne mogu automatski obrađivati ukoliko nisu primjereno zaštićeni, no dozvoljava zakonski predviđena ograničenja prava osoba čiji su osobni podaci pohranjeni u automatskim zbirkama podataka u slučaju da se ti podaci koriste u statističke ili znanstvenoistraživačke svrhe kada očito nema rizika od zadiranja u njihovu privatnost.

Preporuku koja se osobito odnosi na zaštitu podataka u sustavu zdravstva donio je Odbor ministara Vijeća Europe 1997. godine (Council of Europe Committee of Ministers, 1997). U njoj su posebno definirani medicinski i genetički podaci, što u dotadašnjim dokumentima koji su se odnosili na zaštitu privatnosti nije bio slučaj. U Preporuci se, između ostaloga, uređuju pitanja:

- poštivanja privatnosti
- postupanja s medicinskim podacima pri čemu su posebno istaknuti medicinski podaci o nerođenom djetetu i genetički podaci
- obavješćivanja i pristanka osobe (subjekta podataka, „vlasnika izvora" podataka)

- prava osobe na pristup i ispravke svojih medicinskih podataka
- uporabe medicinskih podataka u znanstvenim istraživanjima.

S obzirom da su znanstvena istraživanja od ključne važnosti za napredak svake znanosti, pa tako i medicine, Preporuka donosi i uvjete pod kojima se legitimno znanstveno istraživanje u kojemu anonimizacija osobnih podataka nije moguća ipak može nastaviti uz korištenje osobnih podataka. Ti se uvjeti mogu sažeti u sljedeće točke:

- subjekt podataka je nakon informiranja dao svoju suglasnost
- znanstveno-istraživački projekt je od posebnog javnog interesa i odobren od nadležnih tijela, pri čemu se subjekt podataka izričito ne protivi uporabi svojih osobnih podataka, nije dostupan ili važnost projekta opravdava odobrenje,
- istraživanje je predviđeno zakonom i obuhvaća neophodne javnozdravstvene mjere.

Od vremena prihvaćanja Preporuke br. R(97)5 o zaštiti medicinskih podataka okruženje se zdravstvenih sustava umnogome promijenilo. Informacijska i komunikacijska tehnologija i razvoj interneta omogućili su digitalizaciju i razmjenu velikog broja podataka svih vrsta. Koliko god su prednosti upotrebe novih tehnologija prepoznate u svim segmentima zdravstva, od unapređenja javnog zdravstva i upravljanja zdravstvenim sustavima, liječenja i njege bolesnika do znanstvenih istraživanja, jednako je tako prepoznata i potreba za učinkovitom zaštitom svakog pojedinca. Stoga je Vijeće Europe u ožujku 2019. godine donijelo novu Preporuku CM/Rec(2019)2 (Council of Europe Committee of Ministers, 2019) koja zamjenjuje Preporuku iz 1997. godine.

U novoj Preporuci vlade zemalja članica pozivaju se da osiguraju primjenu danih smjernica zakonima i praksom, da s njima upoznaju sve odgovorne za zdravstveni sustav i da promoviraju njihovo prihvaćanje i primjenu dodatnim instrumentima (kao što su donošenje pravila ponašanja). Pri tome je potrebno osigurati da svi koji su na bilo koji način uključeni u obradu podataka o zdravlju (uključujući i sve koji su povezani s informacijskim i komunikacijskim tehnologijama u sektoru zdravstva) budu dobro upoznati sa smjernicama, da ih razumiju i primjenjuju.

Prva promjena koju uočavamo u novoj Preporuci promjena je naziva podataka na koje se Preporuka odnosi. Izraz „medicinski podaci" zamijenjen je izrazom „podaci o zdravlju" i na prvi pogled ne čini se da je razlika među tim izrazima osobito važna. Međutim, dok se „medicinski podaci" u staroj Preporuci definiraju kao osobni podaci koji se odnose ili su povezani sa zdravljem pojedinca, uključujući i genetičke podatke, izraz „podatci o zdravlju" obuhvaća „sve osobne podatke koji se odnose na fizičko ili

mentalno zdravlje pojedinca, uključujući podatke o pruženim zdravstvenim uslugama, a koji otkrivaju informacije o njegovom prošlom, trenutnom i budućem zdravlju."

Preporuka CM/Rec(2019)2 donosi smjernice podijeljene u sedam poglavlja. Prvo poglavlje obuhvaća opće odredbe u kojima su dani svrha, obuhvat i upotrebljene definicije. Uz definiciju osobnih podataka, genetičkih podataka i podataka o zdravlju definira se i niz drugih pojmova koji se u staroj Preporuci nisu pojavljivali, kao što su anonimizacija,[3] pseudonimizacija,[4] referenti okvir i drugo.

Drugo poglavlje donosi smjernice glede zakonskih uvjeta za obradu podataka o zdravlju. U njemu se iznose osnovna načela i zakonska utemeljenost obrade podataka o zdravlju, postupanje s podacima o nerođenoj djeci i genetičkim podacima o zdravlju, smjernice o dijeljenju podataka o zdravlju u situacijama koje se odnose na pružanje zdravstvene skrbi, prijenos podataka o zdravlju u svrhe različite od pružanja zdravstvene skrbi i pohranu podataka o zdravlju.

Treće poglavlje posvećeno je pravima osobe na koju se podaci o zdravlju odnose (subjekta podataka). Prvi dio trećeg poglavlja odnosi se na jasnoću (engl. *transparency*) obrade podataka o zdravlju, u smislu što potpunije informiranosti osobe čiji se podaci o zdravlju obrađuju. Drugi je dio posvećen pravima na pristup, ispravak i brisanje podataka te prigovor obradi i mogućnosti prijenosa podataka.

Uz sigurnost, o kojoj je bilo riječi i u staroj Preporuci, u novoj se Preporuci u četvrtom poglavlju daju i smjernice glede interoperabilnosti koja je u općim odredbama definirana kao sposobnost prijenosa i razmjene podataka između različitih informacijskih sustava.

Peto je poglavlje posvećeno smjernicama o obradi podataka o zdravlju u znanstvenim istraživanjima. Navedeni su uvjeti pod kojima se ta obrada može provoditi i iznimke u kojima se osobni podaci korišteni u znanstvenom istraživanju mogu objaviti u obliku koji omogućuje identifikaciju osobe.

Sva poglavlja, osim šestoga, imaju neke poveznice sa starijom inačicom Preporuke. Šesto poglavlje u Preporuci iz 2019. godine bavi se pitanjima uporabe mobilnih uređaja. Pri tome se smjernice o mobilnim uređajima odnose na sve mobilne uređaje na kojima se pohranjuju podaci o zdravlju uključujući i one koje su implantirane u

[3] Anonimizacija podataka postupak je obrade osobnih podataka kojim se nepovratno sprječava identifikacija pojedinca iz obrađenih podataka.

[4] Pseudonimizacija podataka postupak je obrade osobnih podataka, obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi.

pojedinca (kao što je, na primjer, elektrostimulator srca poznatiji pod svojim izvornim nazivom *pacemaker*).

Posljednje, sedmo poglavlje odnosi se na smjernice povezane s prekograničnim protokom podataka o zdravlju i oslanja se na mjere zaštite koje su dane u Konvenciji 108.

Niz je dokumenata koji se bave zaštitom podataka u zdravstvu doneseno u i zemljama izvan Europske unije (Asghar i sur., 2017). U Republici Hrvatskoj 2019. godine donesen je i zakon kojim se regulira upravljanje podacima i informacijama u zdravstvu (Zakon o podacima i informacijama u zdravstvu, NN 14/2019). S obzirom na brzi ritam promjena u tehnologiji koja se koristi u zdravstvenim sustavima očekivano je da će se takvi dokumenti usporedno nadopunjavati i mijenjati, a također i sve više međusobno usuglašavati jer je zbog velike mobilnosti ljudi povećana potreba za zdravstvenom zaštitom i izvan matične zemlje ili kontinenta, a time i ujednačenim pravilima glede zaštite podataka o zdravlju.

12.2.2. DIMENZIJE ZAŠTITE PODATAKA

Prema Bakkeru (1998) tri su dimenzije zaštite podataka:

- povjerljivost (engl. *confidentiality*)
- integritet (engl. *integrity*)
- dostupnost (engl. *availability*).

Povjerljivost (tajnost ili privatnost) odnosi se na zaštitu od neautoriziranog odavanja podataka. Neke od situacija u kojima može doći do narušavanja povjerljivosti u sustavima koji raspolažu podacima o zdravlju su:

- ne postoji autentikacija korisnika
- pristupna prava loše su definirana i moguć je pristup podacima koji nisu potrebni
- neodgovarajuća pravila upotrebe podataka o pacijentima u istraživačke svrhe
- nedostatak nadzora nad računalnim izlazom
- neautorizirani pristup računalnom centru.

Integritet (cjelovitost) podataka predstavlja zaštitu podataka od neovlaštene (neautorizirane) promjene podataka. Autorizirani korisnik mora imati uvid u podatke koji nisu mijenjani, brisani niti im je što dodano. Cjelovitost podataka može biti oštećena u slučajevima kao što su:

- pogreške u programskoj podršci
- kvar sklopovlja
- problemi i kvarovi u komunikaciji
- ljudska pogreška pri rukovanju tehničkom infrastrukturom
- zlonamjerne promjene podataka.

Dostupnost podataka izuzetno je bitna u provođenju zdravstvene skrbi. Za uspješan rad zdravstvenih djelatnika nužan je pristup podacima na temelju kojih donose odluke o liječenju i njezi pacijenata i prate njihove učinke, a nedostatak bitnih informacija može ozbiljno ugroziti pacijenta. Više je problema koji mogu uzrokovati nedostupnost podataka među kojima su:

- kvar računalnog sustava
- kvarovi u mreži i nedosljednosti u bazama podataka
- pogreške u programskoj podršci
- elementarne nepogode (požari, poplave i sl.)
- ljudska pogreška.

U izgradnji informacijskih sustava u zdravstvu potrebno je voditi računa o svim navedenim dimenzijama zaštite osobnih podataka, a osobito podataka o zdravlju u sklopu elektroničkog zdravstvenog zapisa (Kern i sur., 2017) kako bi se osigurao nesmetan protok informacija među svim autoriziranim sudionicima u pružanju zdravstvene skrbi i zdravstvenom planiranju.

12.3. ZAŠTITA "OD PODATAKA" IZ PODRUČJA BIOMEDICINE I ZDRAVSTVA

Koliko god je važno štititi podatke o zdravlju pojedinaca, jednako je važno i štititi pojedince „od podataka“ o zdravlju. Internet je nepresušan izvor informacija, a nerijetko i savjetnik za sve probleme, pa tako i zdravstvene (Lee, Hoti, Hughes i Emmerton, 2014), a „dr. Google“ uobičajeno je „drugo mišljenje“ (Fox, 2013). S obzirom na brzinu umnažanja internetskih izvora o zdravstvenim informacijama, korisnici interneta lako pronalaze informacije o simptomima i zdravstvenim problemima kako bi tumačili i svoje simptome (Marcu, Black i Whitaker, 2018).

U moru informacija o zdravlju koje postoje na internetu korisnicima je često teško razlučiti koje su informacije o zdravlju pouzdane (stručno i znanstveno utemeljene), a koje su pokušaji promocije i samopromocije proizvoda i stavova tvrtki i osoba koje ni na koji način nisu povezani sa sustavom zdravstva niti imaju ikakvo zdravstveno obrazovanje. Internetski portali i društvene mreže prepuni su savjeta o prehrani, čudesnim dijetama i vježbama koje će od nas napraviti manekene za mjesec dana, pripravcima koji će nas pomladiti za 20 godina, čak i lijekovima za različite bolesti koji su „100 %" prirodni i učinkoviti. Korisnicima interneta nude se neprovjerene i stručno i znanstveno neutemeljene informacije o zdravlju uz bombastične naslove koji ponekad sadrže i manje ili više prikrivenu zdravstvenu prijetnju (kao npr. da ako svaki dan jedete prženu hranu, možete prije umrijeti).

Koliki su razmjeri opasnosti lakog i brzog širenja nepouzdanih podataka o zdravlju na internetu, najbolje se može vidjeti u nedavnim događajima o cijepljenju. Pod utjecajem tzv. antivakserskog pokreta (pokreta protivnika cijepljenja) obuhvat cijepljenja u mnogim je područjima pao ispod razine koja je stanovništvu osiguravala zaštitu te su se ponovno aktivirale bolesti koje su, zahvaljujući cijepljenju, godinama bile gotovo iskorijenjene. U Republici Hrvatskoj, a i u nekim susjednim zemljama kao što su Republika Srbija i Bosna i Hercegovina, pojavilo se više žarišta u kojima je povećan broj oboljelih (negdje i do razmjera epidemije) od ospica, bolesti koja se desetljećima uspješno prevenirala cijepljenjem. Svjetska zdravstvena organizacija (WHO, prema engl. *World Health Organisation*) među 10 najvećih prijetnji globalnom svjetskom zdravlju u 2019. godini uvrstila je i neodlučnost u cijepljenju (engl. *vaccine hesitancy*) koju definira kao odbojnost prema cijepljenju ili odbijanje cijepljenja usprkos dostupnosti cjepiva (World Health Organisation [WHO], bez dat.). U istoj objavi WHO navodi upravo primjer ospica kao zaraznu bolest koja se može prevenirati cijepljenjem, a za koju se broj oboljelih u svijetu povećao za 30 %.

Iz navedenih je razloga važno razlučiti koje su zdravstvene informacije na internetu one kojima možemo vjerovati, a koje je bolje i ne čitati.

12.4. GDJE PRONAĆI POUZDANE ZDRAVSTVENE INFORMACIJE?

Ukoliko imate zdravstvenih problema, **PRVO se obratite svome liječniku**! Vaš je liječnik najpouzdaniji izvor informacija o vašemu zdravlju, nakon što ga u potpunosti i istinito informirate o svim tegobama koje osjećate.

U situacijama kada želite saznati više pojedinosti o tegobama koje imate (NAKON što ste posjetili svog liječnika!) ili bilo kojem drugom zdravstvenom problemu

ili pitanju koje se odnosi na zdravlje, zdravstvene informacije uvijek tražite na stranicama koje donose pouzdane zdravstvene informacije.

Stranice državnih i javnih ustanova te državnih agencija općenito su izvori pouzdanih informacija, pa tako i informacija o zdravlju. U Republici Hrvatskoj to su, među ostalima i:

- Ministarstvo zdravstva Republike Hrvatske (https://zdravlje.gov.hr/)
- Hrvatski zavod za zdravstveno osiguranje (https://www.hzzo.hr/)
- Hrvatski zavod za javno zdravstvo (https://www.hzjz.hr/)
- Hrvatski zavod za hitnu medicinu (http://www.hzhm.hr/)
- Hrvatski zavod za transfuzijsku medicinu (https://www.hztm.hr/)
- Imunološki zavod (http://www.imz.hr/)
- Agencija za lijekove i medicinske proizvode [HALMED] (http://www.halmed.hr/)
- bolnice i domovi zdravlja (poveznice na mrežne stranice bolnica i domova zdravlja mogu se pronaći na stranicama Ministarstva zdravstva).

Pouzdane i znanstveno utemeljene informacije iz područja biomedicine i zdravstva mogu se naći na stranicama zajednice Cochrane (https://community.cochrane.org/). Cochrane je neprofitna organizacija s više od 37 000 suradnika u više od 130 zemalja koji rade zajedno kako bi pripremili pouzdane i pristupačne informacije o zdravlju u obliku Cochrane sustavnih preglednih članaka bez ikakvog utjecaja komercijalnih sponzora i sukoba interesa. Svaki sustavni pregled odgovara na jasno postavljeno pitanje, a odgovor je dobiven pretragom i sažimanjem svih primarnih istraživanja koja odgovaraju postavljenim kriterijima uključenja. Sva se pronađena istraživanja potom procjenjuju uz korištenje strogih smjernica kako bi se utvrdilo postoje li dosljedni dokazi za odgovor na postavljeno pitanje.

Cochraneovi sustavni pregledi međunarodno su priznati kao najviši standard zdravstvene skrbi utemeljene na dokazima koji se objavljuju na mrežnim stranicama u Cochrane knjižnici (https://www.cochranelibrary.com/). Cochraneovi sustavni pregledi redovito se obnavljaju kako bi se uključile nove kliničke studije. Na taj su način zdravstvene informacije u skladu s najnovijom literaturom i pouzdanim dokazima. Cochrane objavljuje i posebno sačinjene sažetke, tzv. laičke sažetke, koji su napisani jednostavnim jezikom i pomažu ljudima razumjeti i interpretirati zaključke istraživanja.

Zajednica Cochrane aktivna je i u Hrvatskoj već više od 10 godina. Hrvatski Cochrane (https://croatia.cochrane.org/hr) osnovan je 2008. u Splitu i uključen je u

sve Cochrane aktivnosti. Velike napore ulažu u prevođenje Cochrane sažetaka kako bi pouzdane informacije o zdravlju bile dostupne i na hrvatskom jeziku.

U skupinu mrežnih izvora kojima možemo vjerovati kad su u pitanju informacije o zdravlju su i stranice koje posjeduju certifikat kvalitete HONCode. Izdaje ga neprofitna nevladina organizacija *Health On the Net* koja je osnovana s ciljem razvijanja korisnih i pouzdanih zdravstvenih informacija na interentu te omogućavanja njihove prikladne i učinkovite upotrebe. Sve stranice koje žele dobiti HONCode certifikat moraju u potpunosti ispuniti osam principa ("Health On the Net [HON]", bez dat.) i certifikat se mora obnoviti svake godine. HONCode ima više od 7 300 certificiranih mrežnih stranica s više od 10 000 000 povezanih stranica iz 102 države. Neke od stranica u Hrvatskoj koje nose HONCode certifikat kvalitete su: Hrvatskog kardiološko društvo (https://www.kardio.hr/), Pliva zdravlje (https://www. plivazdravlje. hr/) i Cybermed (https://www.cybermed.hr/).

12.5. LITERATURA

Asghar, M. R., Lee, T., Baig, M. M., Ullah, E., Russello, G. i Dobbie, G. (2017). A review of privacy and consent management in healthcare: A focus on emerging data sources. U *IEEE: 13th International Conference on e-Science* (str. 518-522). IEEE.

Bakker, A. (1998). Security in perspective; luxury or must?. *International journal of medical informatics*, *49*(1), 31-37.

Borovečki, A., Mustajbegović, J. i Jakšić, Ž. (2013). *Izborni predmet iz područja medicinske etike: Kako primijeniti Hipokratovu zakletvu?* Zagreb: Medicinski fakultet, Škola narodnog zdravlja „Andrija Štampar".

Council of Europe (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Preuzeto s https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37, 13.5.2019.

Council of Europe Committee of Ministers (1997). *Recommendation No. R (97) 5 of the Committee of Ministers to member states on the Protection of Medical Data*. Preuzeto s https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f0ed0, 13.5.2019.

Council of Europe Committee of Ministers (2019). *Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data.* Preuzeto s https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168093b26e, 13.5.2019.

Fox, S. (2013). After Dr Google: Peer-to-Peer Health Care. *Pediatrics, 131*(Supplement). doi:10.1542/peds.2012-3786k

Health on the Net [HON]. *HONcode: Principles - Quality and trustworthy health information.* (bez dat.). Preuzeto s https://www.hon.ch/HONcode/Webmasters/Conduct.html, 13.5.2019.

Hulkower, R. (2016). The History of the Hippocratic Oath: Outdated, Inauthentic, and Yet Still Relevant. *Einstein Journal of Biology and Medicine, 25*(1), 41. doi:10.23861/ejbm20102542

Kern, J., Bergman Marković, B., Pale, P., Heim, I., Trnka, B., Rafaj, G., . . . Vuletić, S. (2017). Smjernice za unaprjeđenje elektroničkog zdravstvenog zapisa. *Acta Medica Croatica*, *71*(2), 79-92.

Lee, K., Hoti, K., Hughes, J. D. i Emmerton, L. (2014). Dr Google and the Consumer: A Qualitative Study Exploring the Navigational Needs and Online Health Information-Seeking Behaviors of Consumers With Chronic Health Conditions. *Journal of Medical Internet Research, 16*(12), e262.. doi:10.2196/jmir.3706

Marcu, A., Black, G. i Whitaker, K. L. (2018). Variations in trust in Dr Google when experiencing potential breast cancer symptoms: Exploring motivations to seek health information online. *Health, Risk & Society, 20*(7-8), 325-341. doi:10.1080/13698575.2018.1550742

Odluka o objavi Opće deklaracije o ljudskim pravima. *Narodne novine*, br. 12/2009.

Parsa-Parsi, R. W. (2017). The revised Declaration of Geneva: a modern-day physician's pledge. *Jama*, *318*(20), 1971-1972.

Starčević, M. (2005). Ela i Nina u Kutini. *Hrvatski časopis za javno zdravstvo*, *1*(2).

Štrkalj-Ivezić, S., John, N., Sučec, J., Grgin, M. i Halić, M. (2011). *Zapošljavanje osoba sa psihičkom bolesti: Informacije za poslodavce*. Preuzeto s http://udruga-svitanje.hr/images/stories/PDF/Antistigma_PDF.pdf, 13.5.2019.

World Health Organization [WHO]. (bez dat.). *Ten health issues WHO will tackle this year*. Preuzeto s https://www.who.int/emergencies/ten-threats-to-global-health-in-2019, 13. 5. 2019.

Zakon o podacima i informacijama u zdravstvu. *Narodne Novine*, br. 14/2019.

izv. prof. dr. sc. Krešimir Grgić

Fakultet elektrotehnike, računarstva i informacijskih tehnologija
Sveučilišta Josipa Jurja Strossmayera u Osijeku

13. SIGURNOST I PRIVATNOST U KONTEKSTU INTERNETA STVARI I OKRUŽENJA PAMETNOG GRADA

Sažetak

Razvoj interneta započinje još krajem 60-ih godina prošlog stoljeća da bi danas on dosegao razmjere globalne svjetske mreže koja međusobno povezuje na milijarde različitih uređaja. Odavno to više nisu isključivo računala pa je globalna mreža zapravo mreža povezanih objekata, odnosno stvari, i predstavlja vrlo heterogenu strukturu u pogledu vrsta uređaja i komunikacijskih tehnologija. U brojčanom smislu danas najveći dio umreženih uređaja pripada internetu stvari (engl. Internet of Things, IoT) pa stoga danas problematika kibernetičke sigurnosti u takvom okruženju predstavlja jedan od najvažnijih izazova. Temelj interneta stvari predstavljaju bežične senzorske mreže (engl. Wireless Sensor Network, WSN) koje su izložene brojnim mogućim napadima i zlouporabama. Postojeće prijetnje i napade moguće je analizirati po slojevima primijenjenog slojevitog mrežnog modela. Razvoj i napredak interneta stvari dovodi do pojave koncepta pametnog grada (engl. Smart City) koji svojim stanovnicima i posjetiteljima pruža čitav niz naprednih usluga u različitim područjima kao što su: transport, zdravstvena skrb, zabava, zaštita okoliša, energetska učinkovitost, učinkovitost industrijske proizvodnje i druga. U svim područjima naprednih usluga pametnog grada prikuplja se, prenosi i obrađuje velika količina podataka kojima pripadaju često i osjetljivi podaci privatne prirode. Zbog toga je nužno u svim segmentima voditi računa o zaštiti sigurnosti i privatnosti pojedinaca i njihovih osobnih podataka. Odgovarajuća

razina sigurnosti ujedno je i jamac da će korisnici s povjerenjem koristiti nove napredne usluge te da će se time ujedno ostvariti i povećanje kvalitete života u okruženju pametnog grada.

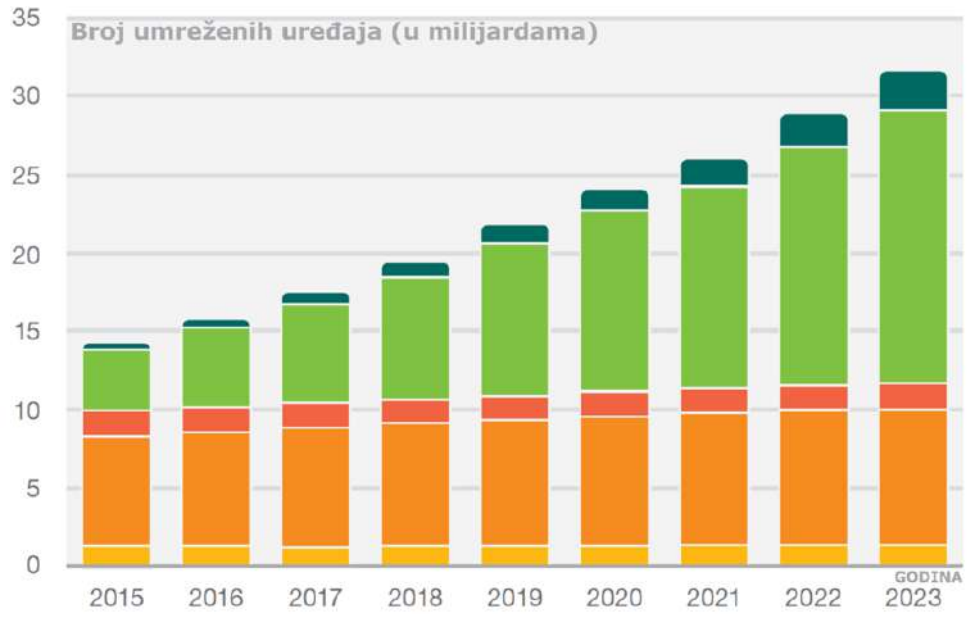
13.1. INTERNET OD KRAJA 1960-IH DO DANAS

Današnji internet, kao globalna svjetska mreža koja u jedinstvenu cjelinu povezuje veliki broj različitih mreža, doživljava svoj eksplozivni razvoj te je odavno prestao nalikovati svojim počecima. Promatrano povijesno, počeci razvoja interneta sežu još u 60. godine prošlog stoljeća, kada se u SAD-u u znanstvenim krugovima (uz pokroviteljstvo Ministarstva obrane) javlja ideja o udaljenom povezivanju većeg broja računala u svrhu komunikacije, razmjene podataka, ali i udaljenog pokretanja programa (Leiner i sur., 2009).Godine 1969. znanstveno-istraživački tim američke agencije ARPA (engl. *Advanced Research Project Agency*) kreira mrežu pod nazivom ARPANET koja se povijesno može smatrati pretečom današnjeg interneta. Do kraja 1969. godine ARPANET međusobno povezuje samo četiri čvorišta, no kasnije (tijekom 70-ih godina) njihov broj kontinuirano raste. U početku se komunikacija temeljila na komutaciji kanala (poput klasične telefonske mreže) što se nije pokazalo najboljim rješenjem. Stoga se razvija komunikacija temeljena na razmjeni pojedinačnih podatkovnih paketa (komutacija paketa) koji neovisno jedan o drugome putuju od izvora do odredišta. U tom slučaju računala pri međusobnoj komunikaciji (slanju i prijamu paketa) moraju poštivati strogo određena dogovorena pravila koja su definirana komunikacijskim protokolom. Dakle, razvoj komunikacijskih mreža prati i razvoj odgovarajućih komunikacijskih protokola. Paketski način prijenosa u skladu je i sa željama da ARPANET bude izuzetno tolerantan na kvarove, tj. ostatak mreže nastavlja funkcionirati čak i ako jedan njezin dio bude uništen. Ne treba zanemariti povijesni kontekst u kojem nastaje ARPANET – razdoblje je to hladnog rata – te je želja Ministarstva obrane SAD-a prilikom projektiranja bila da mreža može „preživjeti“ čak i nuklearni napad (Lukasik, 2011).

Tijekom 70-ih godina prošlog stoljeća mreža se širi, prelazi granice SAD-a te se međusobno u jednu cjelinu povezuju i druge mreže kojenastaju u tom razdoblju. Tijekom 70-ih razvijaju se (a početkom 80-ih prihvaćaju kao standard) protokoli TCP (engl. *Transmission Control Protocol*) i IP (engl. *Internet Protocol*) za komunikaciju između različitih mreža i umreženih računala koji su do danas ostali najvažniji internetski protokoli i temelj internetske protokolne arhitekture. Godine 1984. pojavljuje se i prva globalna mreža *WAN (*engl. *Wide Area Network*) koja od svojeg samog početka koristi TCP/IP protokole te stoga predstavlja važan korak u razvoju interneta. Riječ je o mreži NSFNET koju je utemeljila američka Nacionalna zaklada za znanost (engl. *National Science Foundation*). Ta mreža prvobitno je povezivala šest velikih američkih računalnih centara te veći broj manjih računala i bila je povezana sa ARPANET-om (Severance, 2014).

Usporedo s razvojem interneta razvijaju se i različite internetske usluge koje se uglavnom i danas koriste (npr. elektronička pošta, udaljeni rad na računalu, prijenos datoteka). Već početkom 90-ih godina internet povezuje više od milijun računala. Godine 1991. fizičar Tim Berners-Lee razvija internetsku uslugu WWW (engl. *World Wide Web*) koja je omogućila izradu mrežnih stranica koje sadržavaju različite vrste podataka (tekst, slika, zvuk, video), a međusobno su povezane tekstualnim poveznicama. Pojava te usluge predstavlja novu važnu prekretnicu u razvoju interneta budući da značajno doprinosi širenju interneta i povećanju broja njegovih korisnika. Pojavom mreže širenje interneta postaje eksponencijalno.

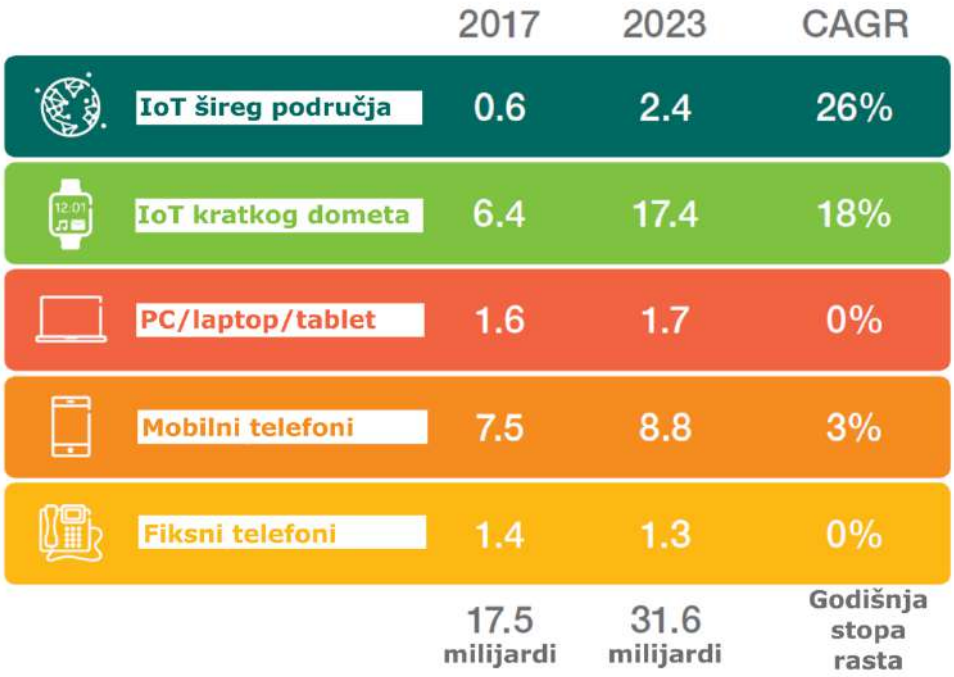
Danas internet kao globalna svjetska mreža u jednu jedinstvenu logičku cjelinu povezuje veliki broj različitih mreža (vrlo heterogenih po svojoj prirodi i tehničkim karakteristikama) i uređaja. Uređaji koji se mogu povezati na internet odavno više nisu samo računala. Osim stolnih i prijenosnih računala danas su tu i sveprisutni pametni telefoni, tableti, ali i sve veći broj raznih drugih uređaja u kućanstvu (npr. televizori, kamere). Slika 1 prikazuje trend kretanja broja umreženih uređaja (u milijardama), uključujući i predviđanja za sljedećih nekoliko godina (Ericsson, 2017).



Slika 1. Broj umreženih uređaja izražen u milijardama (Ericsson, 2017)

Slika 2 detaljnije pojašnjava udio pojedinih vrsta uređaja u ukupnom broju umreženih uređaja. Sa slike je vidljivo da najbrže raste broj različitih „pametnih“

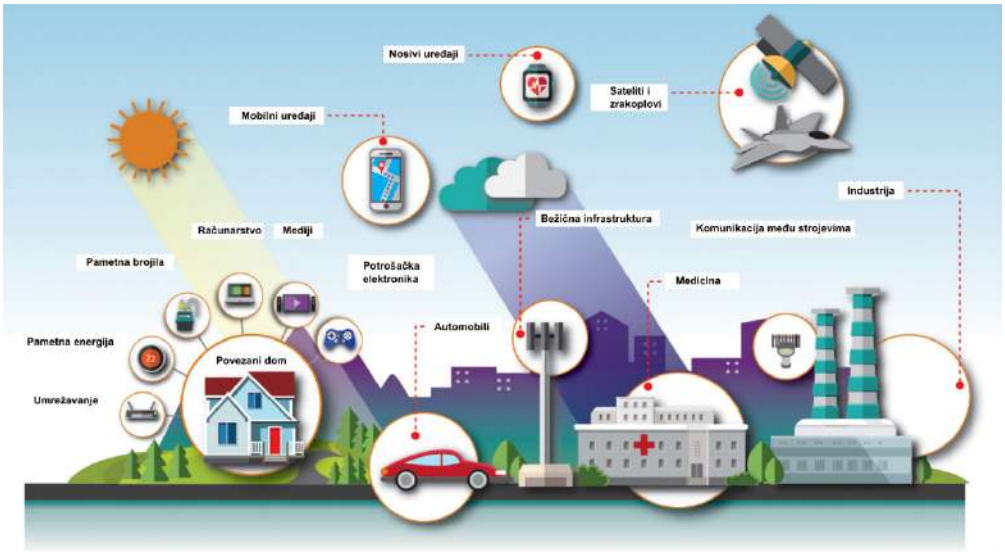
uređaja koji ne pripadaju u skupinu računala (stolnih, prijenosnih ili tableta) i telefona (mobilnih i fiksnih). CAGR predstavlja godišnju stopu rasta (engl. *Compound Annual Growth Rate*).



Slika 2. Vrste umreženih uređaja i njihov udio u ukupnom broju (Ericsson, 2017)

13.2. INTERNET STVARI (INTERNET OF THINGS, IoT) - SIGURNOSNI ASPEKTI

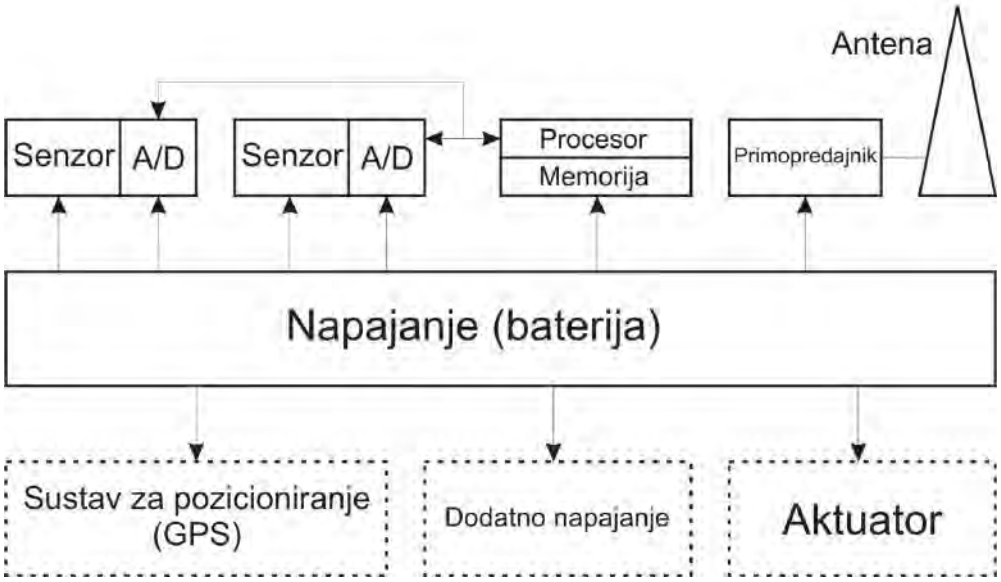
Prethodne brojke pokazuju da globalna mreža prilično brzo evoluira prema mreži povezanih objekata (stvari) kojima je zajedničko da se pri komunikaciji oslanjaju na standardne internetske komunikacijske protokole i moguće ih je jedinstveno adresirati. Takvi umreženi objekti u mogućnosti su prikupljati informacije iz svoje okoline (različitim senzorima) i ostvarivati interakciju s fizičkim svijetom (aktuacija/komanda/kontrola). Takva vrsta globalne mreže predstavlja *Internet of Things (IoT)* paradigmu (internet stvari, internet objekata) (slika 3).



Slika 3. Internet stvari (Internet objekata) (Skyworks, 2019)

U IoT okruženju neki od najvažnijih izazova odnose se na problematiku kibernetičke sigurnosti. Veliki izazov predstavlja pronalazak kvalitetnih rješenja za zaštitu privatnosti, kontrolu pristupa, sigurnu pohranu podataka te verifikaciju i autentifikaciju uređaja i korisnika. Dinamika daljnjeg razvoja interneta stvari u velikoj mjeri ovisi o implementaciji odgovarajućih rješenja glede problematike sigurnosti (Al-Fuqaha, Guizani, Mohammadi, Aledhari i Ayyash, 2015).

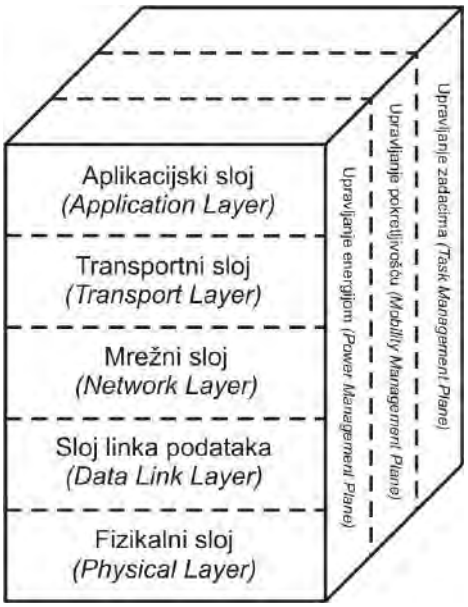
Temeljni dio interneta stvari predstavljaju bežične senzorske mreže (BSM) (engl. *Wireless Sensor Network*, WSN). One se sastoje od velikog broja minijaturnih „pametnih" senzorskih čvorova. Tipična struktura senzorskog čvora prikazana je na slici 4. Tipičan senzorski čvor uključuje senzorski dio (koji je u mogućnosti mjeriti neki parametar iz okruženja), računalni dio (provodi jednostavniju obradu i pohranu podataka) te komunikacijski dio (koji omogućava bežičnu komunikaciju s ostalim čvorovima). Prema tome, bežična senzorska mreža prikupljat će podatke iz svojeg okruženja te ih dostavljati udaljenim korisnicima i ostalim udaljenim uređajima unutar IoT ekosustava. Pri tome komunikacija između senzorskih čvorova i ostatka interneta mora udovoljiti svim sigurnosnim zahtjevima (Grgić, 2011).



Slika 4. Struktura bežičnog senzorskog čvora (Grgić, 2011)

Problematika sigurnosti (u pogledu tehnologije i implementacije određenih rješenja) unutar IoT okruženja u većoj se mjeri razlikuje od problematike sigurnosti u konvencionalnim žičnim i bežičnim mrežama. Uzrok su tomu znatna ograničenja u pogledu energetskih resursa i računalne snage kod velikog broja čvorova u IoT mreži (budući da se često radi o malim baterijski napajanim čvorovima). Zbog tih ograničenja u IoT okruženju nisu izravno primjenjiva mnoga sigurnosna rješenja koja se inače primjenjuju u konvencionalnim mrežama.

Slojeviti mrežni model koji se primjenjuje u IoT okruženju zapravo je vrlo sličan slojevitom TCP/IP modelu koji se susreće u konvencionalnim mrežama (slika 5).



Slika 5. Protokolni stog bežične senzorske mreže (Grgić, 2011)

Fizički sloj (engl. *Physical Layer*), kao najniži sloj, definira modulacijske postupke i tehnike prijama i predaje radiosignala. Na sloju podatkovnog linka (engl. *Data Link Layer*) izvode se protokoli koji reguliraju pravo pristupa dijeljenom prijenosnom mediju (engl. *MAC, Medium Access Control*). Mrežni sloj (engl. *Network Layer*) podatke (podatkovne pakete) koji pristižu s transportnog sloja usmjerava na odgovarajuće rute prema odredištu. Transportni sloj (engl. *Transport Layer*) omogućava uspostavu i očuvanje podatkovnog toka pružajući uslugu transporta podataka ukoliko to zahtijevaju korisničke aplikacije. Na najvišem, aplikacijskom sloju (engl. *Application Layer*) izvode se korisničke aplikacije kreirane u skladu s konkretnom primjenom mreže i zahtjevima korisnika (Akyildiz, Su, Sankarasubramaniam i Cayirci, 2002).

Promatrano s upravljačkog aspekta moguće je razlikovati tri upravljačke plohe (ravnine): upravljanje energijom, upravljanje pokretljivošću i upravljanje zadacima. Upravljačkim ravninama za upravljanje energijom (engl. *Power Management Plane*) regulira se način na koji mrežni (senzorski) čvor iskorištava raspoložive energetske resurse. Budući da su ti resursi obično vrlo ograničeni (obično se radi o bateriji koja bi senzorski čvor trebala napajati dulje vrijeme), s njima se treba raspolagati krajnje racionalno kako bi se produljio životni vijek senzorskog čvora. Na primjer, ukoliko mu je baterija pri kraju, senzorski čvor može obavijestiti susjedne čvorova da više ne može pružati uslugu usmjeravanja i prosljeđivanja podatkovnih paketa. Upravljačkom ravninom za upravljanje pokretljivošću (engl. *Mobility Management Plane*) vrši

se praćenje i nadzor kretanja senzorskih čvorova kako bi u bilo kojem trenutku bilo moguće uspostavljanje rute od senzora do krajnjeg odredišta podataka. Upravljačka ravnina za upravljanje zadacima (engl. *Task Management Plane*) služi za planiranje i upravljanje zadacima te raspoređivanje zadataka na pojedine senzorske čvorove (s obzirom da na nekom području ne moraju svi senzorski čvorovi biti istodobono aktivni).

Takav složeni slojeviti model omogućava senzorskim čvorovima da kooperativno izvršavaju svoje zadatke na energetski učinkovit način te da se primjenom kolaborativnih algoritama informacija u konačnici prenese do krajnjeg korisnika. Međusobna suradnja senzorskih čvorova i primjena kooperativnih algoritama povećavaju učinkovitost, a s povećanjem učinkovitosti produljuje se i životni vijek senzorskih čvorova (a time i kompletne senzorske mreže).

Bežične mreže donose čitav niz prednosti u odnosu na žične mreže. Ponajprije, to je iznimna fleksibilnost (kako iz perspektive krajnjeg korisnika, tako i iz perspektive mrežnih operatera). Nadalje, bežična mrežna rješenja omogućavaju sveprisutnu pokrivenost i dostupnost na užem ili širem području, uz relativno niske troškove implementacije i održavanja (postavljanje i održavanje fiksne infrastrukture u pravilu je značajno skuplje, a ponekad čak i nemoguće zbog konfiguracije terena ili administrativnih zabrana). Prema tome, bežična mreža predstavlja elegantno i ekonomično rješenje koje omogućava potpunu pokretljivost korisnika. Međutim, zbog otvorene prirode komunikacijskog medija sve vrste bežičnih mreža znatno je teže osigurati od napada i zlouporabe nego što je to slučaj sa žičnim mrežama. Budući da se i u većini bežičnih mreža primjenjuje TCP/IP protokolni stog, gotovo sve postojeće sigurnosne prijetnje poznate u žičnim mrežama mogu se pojaviti i u bežičnim. U bežičnim mrežama javlja se dodatno i čitav niz drugih prijetnji (koje nisu prisutne u žičnim mrežama), a povezane su sa specifičnostima bežičnog okruženja (otvorenost i nepouzdanost prijenosnog medija, ograničena propusnost i sl.) (Kavitha i Sridharan, 2010).

Bez obzira na njihovu raznolikost, svi napadi mogu se razvrstati u jednu od dviju kategorija: pasivni i aktivni napadi. Pasivni napadi u bežičnim mrežama podrazumijevaju prisluškivanje radiokomunikacije te praćenje (i prikupljanje) paketa koji se prenose mrežom. S druge strane, aktivni napadi podrazumijevaju da napadač na određeni način modificira podatkovne tokove u mreži ili kreira nove. Prema izvoru napada napadi se mogu podijeliti na vanjske i unutrašnje. Vanjski napadi inicirani su od strane čvorova koji ne pripadaju napadnutoj mreži, dok unutrašnji napadi podrazumijevaju da se postojeći (legitimni) mrežni čvor počne ponašati maliciozno (zlonamjerno) (Krauss, Schneider i Eckert, 2008).

Zbog iznimno velikog broja različitih mogućnosti napada vrlo je teško, gotovo nemoguće, napraviti sustavni prikaz svih mogućih postojećih sigurnosnih prijetnji.

Jedan od mogućih pristupa problemu jest promatrati sigurnosne prijetnje po slojevima mrežnog modela na koji su primarno usmjerene (Saxena, 2007).

Fizički sloj u bežičnim mrežama odgovoran je za izbor frekvencije, generiranje frekvencije nosioca, detekciju signala, modulacijske postupke i enkripciju podataka. Napadi koji su izravno usmjereni na taj sloj predstavljaju zapravo neku vrstu elektroničkog ometanja (engl. *jamming*). U tom slučaju napadač koristi vlastiti predajnik koji može emitirati većom snagom od predajnika na legitimnim mrežnim čvorovima. Pomoću njega napadač namjerno izaziva smetnju na radijskim frekvencijama koje se koriste u bežičnoj mreži te tako značajno otežava ili onemogućava komunikaciju (u manjem ili većem dijelu mreže). Mogući način obrane od takve vrste napada bila bi primjena naprednijih tehnika emitiranja (koje koriste više frekvencija i širi spektar). Međutim, takve su tehnike kompleksnije i zahtijevaju više resursa (računalnih i energetskih) pa ih često nije ni moguće implementirati na neke jednostavne uređaje u IoT okruženju. U bežičnim mrežama često je slučaj da mrežni čvorovi nemaju neku posebnu fizičku zaštitu pa su onda takvi uređaji izravno izloženi i mogućem fizičkom pristupu neke neovlaštene osobe. U slučaju fizičkog pristupa napadač može doći do povjerljivih informacija pohranjenih na mrežnom čvoru (npr. kriptografski ključevi). Osim samog pristupa podacima napadaču se otvara mogućnost izmjene podataka ili programskog koda i preuzimanja potpune kontrole nad mrežnim čvorom. Tako kompromitiran mrežni čvor napadač može zlorabiti u svojim daljnjim malicioznim aktivnostima. U IoT okruženju, posebice u dijelu senzorske mreže, gotovo je nemoguće fizički zaštititi svaki mrežni čvor. Zbog toga je važno da svi mrežni sigurnosni mehanizmi koji se implementiraju u takvu mrežu moraju predvidjeti mogućnost kompromitacije određenog broja čvorova te u tom slučaju imati mogućnost isključivanja kompromitiranih čvorova i omogućavanja daljnjeg rada mreže.

Sloj podatkovnog linka unutar slojevitog modela zadužen je za multipleksiranje podatkovnih tokova, detekciju okvira, pristup dijeljenom mediju i kontrolu pogrešaka. Na tom se sloju ostvaruje pouzdana konekcija od točke do točke (engl. *point-to-point*) ili od točke do više točaka (engl. *point-to-multipoint*) unutar mreže. Prilikom napada na taj sloj napadaču je često cilj namjerno izazvati koliziju paketa. Do kolizije dolazi ukoliko dva ili više mrežnih čvorova pokušavaju istodobno emitirati na istoj frekvenciji. U tom slučaju doći će do pogrešaka prilikom prijenosa (paket pristiže na odredište ali s greškom) ili do potpunog gubitka paketa. Namjernim izazivanjem kolizije napadač će prouzročiti zastoj u radu mreže. Implementacija i uporaba kodova za ispravljanje pogrešaka (engl. *error correcting codes*) može pomoći u slučaju rjeđe pojave kolizija (što je u mrežama uobičajeno zbog utjecaja smetnji iz okoline i samoga sklopovlja), no u slučaju sustavnog i namjernog izazivanja kolizije neće se pokazati učinkovitom. Takvu vrstu napada moguće je detektirati, no iznimno je teško obraniti

se. Namjernim izazivanjem kolizija napadač može izazvati i iscrpljivanje resursa mrežnih čvorova (gubitak napajanja uslijed pražnjenja baterije) i njihovo isključenje (budući da će u slučaju nastanka kolizije čvorovi kontinuirano pokušavati izvesti retransmisiju paketa što će iscrpiti bateriju). Jedno od mogućih rješenja problema predstavlja ograničenje učestalosti pristupa mediju čime bi se onemogućilo uzastopno bezuspješno slanje paketa (koje bi dovelo do pražnjenja baterije).

Mrežni sloj senzorske mreže unutar IoT okruženja u velikoj mjeri sliči mrežnom sloju u klasičnim mrežama, no uz posebnu orijentiranost prema maloj potrošnji energije i energetskoj učinkovitosti. Budući da na mrežnom sloju funkcioniraju neki od najvažnijih mrežnih mehanizama (npr. usmjeravanje, adresiranje), o njemu u velikoj mjeri ovisi ispravan rad cjelokupne mreže. Stoga je taj sloj najizloženiji do sada zabilježenim i poznatim napadima.

Česta meta napada jest usmjerivački kontrolni promet (kontrolne poruke vezane uz mehanizam usmjeravanja podatkovnih paketa u mreži koje mrežni čvorovi međusobno razmjenjuju). Ukoliko napadač uspije lažirati ili izmijeniti te poruke, može narušiti normalni tijek mrežnog prometa (što mu je i cilj). Na taj način napadač može namjerno kreirati usmjerivačke petlje, promijeniti (produljiti ili skratiti) originalne rute, privlačiti ili odbijati mrežni promet, namjerno povećavati kašnjenje prilikom prijenosa te generirati lažne poruke o greškama. Odgovarajuće protumjere obično podrazumijevaju dodavanje autentifikacijskog koda svakoj poruci (engl. *Message Authentication Code, MAC*) te uvođenje brojača i vremenskih oznaka kako bi se moglo utvrditi „starost" poruke.

Temeljna pretpostavka u mrežama kod kojih se komunikacija odvija kroz više skokova (engl. *multihop*) jest da svi čvorovi koji sudjeluju u prijenosu dosljedno prosljeđuju primljene poruke dalje prema njihovom odredištu. Nažalost, ta pretpostavka često je predmetom zlouporabe od strane napadača pri čemu dolazi do selektivnog prosljeđivanja paketa (engl. *Selective Forwarding*). U tom slučaju zlonamjerni čvor odbija proslijediti poruke (pakete) prema njihovom odredištu te ih jednostavno odbacuje. Najjednostavnija inačica takvog napada jest situacija kad zlonamjerni čvor odbacuje sve pakete, tj. ne želi proslijediti ni jednog – ponaša se kao „crna rupa" (engl. *Black Hole Attack*). Na sreću, ta inačica selektivnog prosljeđivanja najlakše se otkriva pri čemu najvažniji dio zadaće otkrivanja malicioznog čvora leži na njegovim susjedima koji „osluškuju" njegovo ponašanje. U slučaju uspješnog otkrivanja napada crne rupe, engl. *black hole*, provodi se rekonfiguracija mrežnih ruta pri čemu se maliciozni čvorovi iz njih izostavljaju.

Sofisticiraniji oblik toga napada je onaj kod kojeg napadač uklanja ili modificira poruke nekolicine čvorova pri čemu poruke preostalih čvorova uredno prosljeđuje na uobičajeni način. Takvo zlonamjerno ponašanje znatno se teže otkriva budući da se

dio prometa odvija „regularno“, pa će susjedni čvorovi teže „posumnjati“ na maliciozni čvor.

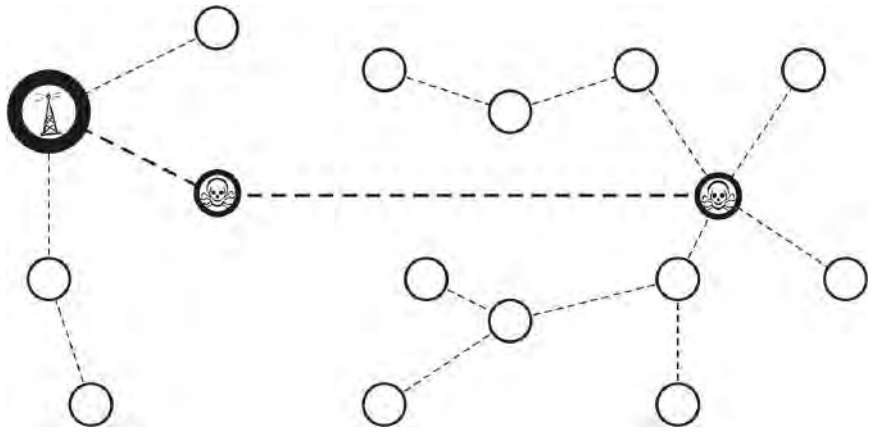
Često je cilj napadača privući sav mrežni promet iz određenog dijela mreže prema zlonamjernom čvoru koji je u tom slučaju središte figurativnog „ponora“ (engl. *Sinkhole*). Taj će učinak napadač najčešće postići krivotvorenjem usmjerivačkih informacija (kontrolne poruke usmjerivačkog protokola). Otpornost na takve vrste napada pokazuju tzv. geografski usmjerivački protokoli s obzirom da se prilikom usmjeravanja oslanjaju na geografsku lokaciju čvorova, a ne samo na kontrolne poruke razmijenjene sa susjednim čvorovima (Ngai, Liu i Lyu, 2007).

S obzirom da obično raspolaže značajnijim resursima, napadač se mreži može predstavljati s više različitih identiteta. Ta vrsta napada naziva se *Sybil* napad. U tom slučaju ostali čvorovi napadača vide kao nekoliko legitimnih čvorova. Kod te vrste napada napadač može „preoteti“ već postojeće identitete nekih čvorova ili se mreži predstaviti kao skup novih čvorova. Zato je u senzorskim mrežama često iz sigurnosnih razloga onemogućeno samostalno dodavanje novih čvorova, a time i uvođenje novih identiteta. U tom slučaju napadaču bi preostala isključivo mogućnost preuzimanja postojećih identiteta pri čemu bi postojeće čvorove morao isključiti ili onesposobiti (Newsome, Shi, Song i Perrig, 2004).

Na *Sybil* napad najosjetljiviji su mehanizmi usmjeravanja i mehanizmi za distribuiranu pohranu podataka. Ozbiljno ugrožen može biti i postupak agregacije podataka budući da napadač namjernim umetanjem lažnih podataka može u većoj mjeri negativno utjecati na rezultat agregacije. *Sybil* napad ugrožava i distribuirane mrežne mehanizme koji se temelje na „glasovanju“ svih čvorova i većinskom odlučivanju. Zahvaljujući imanju višestrukih identiteta, napadač može značajnije utjecati na rezultat glasovanja, a time izravno utjecati na postupak odlučivanja.

Zaštita od *Sybil* napada mora podrazumijevati izravnu ili neizravnu mogućnost provjere identiteta čvorova. Izravna provjera podrazumijeva da čvor provjerava identitet čvora s kojim uspostavlja komunikaciju. Neizravna provjera podrazumijeva da prethodno provjereni čvorovi vrše provjeru identiteta ostalih čvorova.

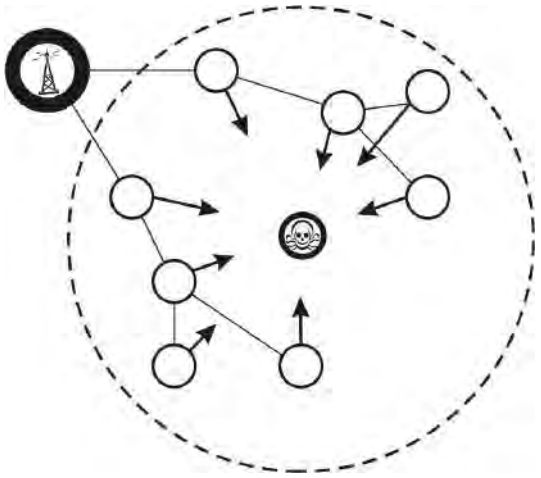
Za *wormhole* napad karakteristično je da napadač uspostavlja brzi link niske latencije između dvaju udaljenih dijelova mreže („crvotočina“). To mu omogućava da „tunelira“ poruke iz jednog u drugi dio mreže, a da legitimni čvorovi toga nisu ni svjesni. Time napadač može izravno utjecati na topologiju mreže i mehanizam usmjeravanja.



Slika 6. *Wormhole* napad (Grgić, 2011)

Mjera prevencije protiv *wormhole* napada mogu biti geografske i vremenske oznake koje se dodaju paketima. Geografske oznake osiguravaju da se primatelj paketa mora nalaziti unutar određene maksimalne udaljenosti od pošiljatelja. Vremenske oznake ograničavaju maksimalno „vrijeme života" paketa čime se posredno limitira udaljenost na koju ga je moguće prenijeti. Preduvjet za takav mehanizam je da čvorovi znaju svoju točnu geografsku lokaciju te da imaju međusobno sinkronizirane satove (Hu, Perrig i Johnson, 2003).

Većina usmjerivačkih protokola oslanja se na razašiljanje (engl. *broadcasting*) poruka kojima čvorovi svoje susjede izvještavaju o svojem statusu – pozdravne (HELLO) poruke. Čvor koji primi takvu poruku zaključit će da se nalazi u radijskom dometu s pošiljateljem, tj. da su susjedi. Napadač može te poruke slati većom snagom nego što to može legitimni čvor te tako može pokriti veći dio mreže (ili čak cijelu mrežu) i lažno uvjeriti veći broj legitimnih čvorova da je njihov susjed. Na taj će način navesti legitimne čvorove da mu uzaludno pokušavaju slati pakete (dok im je u stvarnosti izvan dometa) i na taj način izazvati konfuziju u mreži (Hamid, Rashid i Hong, 2006).



Slika 7. Poplavljivanje HELLO porukama (Grgić, 2011)

Moguće su protumjere protiv tog napada provjera dvosmjernosti pojedinih linkova, implementacija protokola za provjeru autentičnosti i enkripcija prometa (što implicira i implementaciju rješenja za distribuciju ključeva).

13.3. PAMETNI GRAD - SIGURNOSNI ASPEKTI

Razvoj i napredak koncepta interneta stvari (IoT) omogućio je i pojavu paradigme pametnog grada (engl. *Smart City*). Koncept pametnog grada podrazumijeva sveprisutne senzore (različite po svojoj vrsti i namjeni) koji se povezuju na razvijenu i razgranatu heterogenu mrežnu infrastrukturu. Ti senzori generiraju ogromne količine podataka koji se na inteligentan način procesiraju što rezultira informacijama nužnim za pametno upravljanje različitim vrstama usluga. Pametni grad omogućava kontinuirani nadzor (u stvarnom vremenu) različitih parametara iz fizičkog okruženja te pružanje čitavog niza pametnih usluga (kako svojim stanovnicima tako i gostima) u domeni transporta, zdravstvene skrbi, zaštite okoliša, energetske učinkovitosti, zabave… U takvom okruženju sigurnost i privatnost igraju značajnu ulogu budući da se prikuplja i manipulira velikom količinom osjetljivih privatnih podataka (Zhang i sur., 2017).

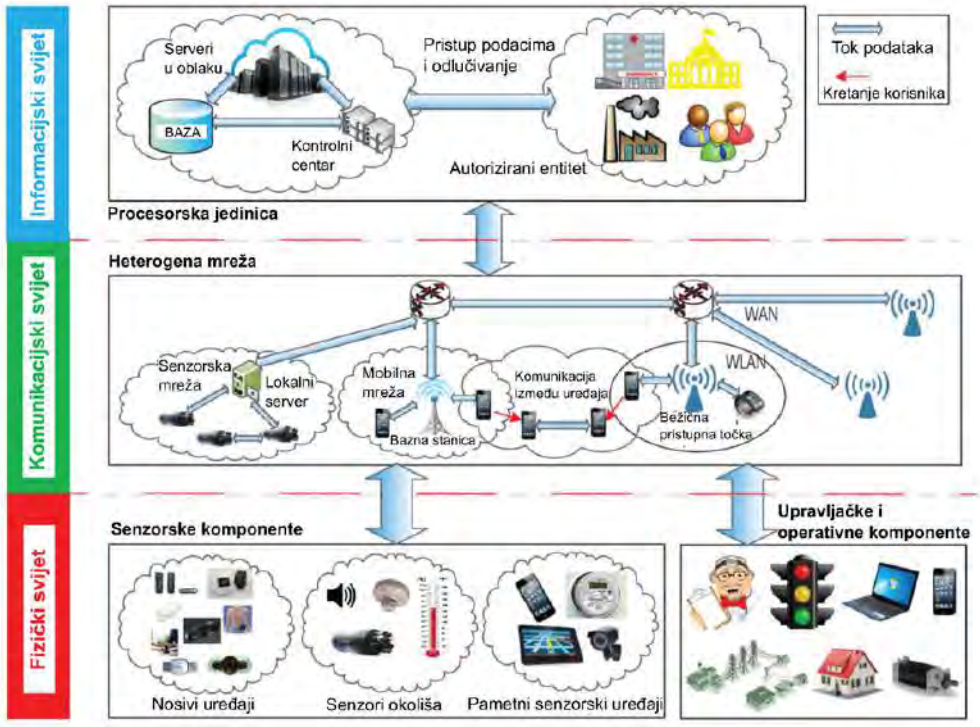
Koncept pametnog grada pruža gradovima mogućnosti daljnjeg društvenog i gospodarskog razvoja, posebice u kontekstu sve većeg stupnja urbanizacije i porasta broja urbane populacije. Bez primjene pametne tehnologije komunalna infrastruktura znatno bi teže pratila takav rast i razvoj. Koncept pametnog grada predstavlja poveznicu između fizičkog svijeta (senzori i aktuatori) i informacijskog svijeta (velike

količine podataka pohranjene u bazama podataka i u oblaku) koji su povezani heterogenom komunikacijskom mrežom (koja upotrebljava različite žične i bežične komunikacijske tehnologije). Slika 8 prikazuje neke aplikacije pametnog grada.

Slika 8. Aplikacije pametnog grada (Zhang i sur., 2017)

U pametnom gradu odgovarajućim senzorima kontinuirano se prati tijek i potrošnja energije (uključujući proizvodnju električne energije, njezin prijenos i distribuciju pametnom elektroenergetskom mrežom te potrošnju kod krajnjih potrošača). Primjenom napredne tehnologije smanjuje se ukupna potrošnja te pomaže u prevenciji kvarova (engl. *Smart Energy*). Kontinuirano se prate i klimatski te ostali parametri okruženja (npr. buka, ispušni plinovi i druge vrste zagađenja) te se pametnim upravljanjem podiže razina kvalitete neposrednog okruženja (engl. *Smart Environment*). Tehnologija pametnih senzora i aktuatora ima ogroman potencijal primjene i u industrijskoj proizvodnji tako da pametna industrija (engl. *Smart Industry*) predstavlja važnu cjelinu u konceptu pametnog grada. Postupak se proizvodnje optimizira kako bi potrošnja resursa bila što učinkovitija uz što manji stupanj negativnog djelovanja na okoliš. Jedan od glavnih ciljeva pametnog grada jest unapređenje kvalitete života njegovih stanovnika kao i osiguranje ugodnog boravka njegovim posjetiteljima. Stoga koncept pametnog življenja (engl. *Smart Living*) podrazumijeva napredno pametno upravljanje različitim uređajima u kućanstvima (npr. daljinsko upravljanje pojedinim uređajima, napredni sustavi za klimatizaciju, informacijsko-zabavni multimedijalni sadržaji i sl.) uz maksimalnu energetsku učinkovitost. U pametnom gradu stanovnicima su dostupne mnogobrojne pametne usluge (engl. *Smart Service*), od inteligentnog transportnog sustava (npr. navigacija, izbjegavanje gužvi) preko pametne zdravstvene skrbi (npr. kontinuirano praćenje vitalnih parametara nosivim uređajima, daljinska dijagnostika, alarm u slučaju nezgode i sl.) pa sve do pametnih javnih i komunalnih usluga.

Kako bi sve spomenute aplikacije bilo moguće realizirati, potrebno je u jedinstvenu arhitekturu integrirati tri „svijeta“: fizički svijet, informacijski svijet i komunikacijski svijet (slika 9).



Slika 9. Arhitektura pametnog grada (Zhang i sur., 2017)

Senzorske komponente prikupljaju informacije iz fizičkog svijeta te se one pohranjuju, procesiraju i prenose različitim vrstama komunikacijskih mreža. U senzorske komponente mogu se uvrstiti i različite vrste nosivih uređaja, industrijskih senzora i pametnih uređaja (npr. pametni telefoni, nadzorne kamere i sl.). U okruženju pametnog grada susreću se i različite vrste komunikacijskih tehnologija: bežične lokalne mreže (engl. *Wireless Local Area Network, WLAN*), pokretne mreže (trenutačno najviše četvrte generacije, a uskoro će uslijediti širenje i komercijalizacija pokretnih mreža pete generacije), različite komunikacijske tehnologije namijenjene pametnim senzorima i senzorskim mrežama. Za procesiranje informacija, odlučivanje i upravljanje koriste se napredni distribuirani računalni sustavi kojima autorizirani pristup ostvaruju odgovarajuća nadležna tijela.

U složenom heterogenom okruženju pametnog grada kruži velika količina podataka od kojih je velik dio privatne prirode i osjetljiv te je nužno osigurati odgovarajuću

razinu sigurnosti i privatnosti. U svakom pogledu i na svim razinama nužno je zadovoljiti najvažnije sigurnosne paradigme: povjerljivost, integritet, autentičnost, dostupnost, neporecivost, privatnost i kontrolu pristupa podacima (Cui, Xie, Qu, Gao i Yang, 2018).

Činjenica jest da se u okruženju pametnog grada prikupljaju raznovrsni podaci privatne prirode (npr. podaci o lokaciji i kretanju pojedinaca, njihovom zdravstvenom stanju, životnim navikama, kontaktima s drugim ljudima). Ukoliko takvi podaci završe u neovlaštenim rukama, riječ je o ozbiljnom narušavanju privatnosti i svakako je nužno poduzeti odgovarajuće mjere da se takvo što spriječi. To podrazumijeva primjenu odgovarajućih mehanizama za kontrolu pristupa podacima, osiguranje anonimnosti korisnika gdje god je to moguće te šifriranje (kriptiranje) podataka prilikom prijenosa i pohrane. Problem također može predstavljati činjenica da se do određenih privatnih informacija može doći i posrednim putem, npr. praćenjem potrošnje energije u kućanstvu može se zaključiti u koje su doba dana stanari uobičajeno kod kuće ili se nadzorna kamera za otkrivanje upada može zlorabiti i za praćenje stanara.

Većina napada na sigurnost i privatnost podataka dolazi „izvana", od strane neovlaštene osobe koja pokušava „ukrasti" podatke. Međutim, ne treba zanemariti činjenicu da do napada može doći i „iznutra", od strane entiteta koji ima pristup sustavu i podacima (pri čemu šteta može biti i daleko veća). To treba imati u vidu te prilikom pohrane i prijenosa podataka obavezno koristiti neku metodu enkripcije.

Na temelju prikupljenih podataka nakon njihove analize donose se odluke o odgovarajućim akcijama koje kontrolni sustav usmjerava prema aktuatorima koji provode određene radnje. Zbog toga su upravo kontrolni sustavi (posebice ako pripadaju javnoj ili industrijskoj infrastrukturi) najizloženiji mogućim napadima. Modificiranjem postojećih podatkovnih tokova ili umetanjem lažnih informacija napadač je u mogućnosti poremetiti normalno funkcioniranje takvih sustava. Stoga je nužno štititi integritet podataka, najčešće primjenom tehnike digitalnoga potpisivanja.

Pametna zdravstvena skrb jedna je od najistaknutijih aplikacija pametnog grada koja omogućava kontinuirani nadzor i prikupljanje podataka o zdravstvenom stanju pacijenata (praćenjem niza vitalnih parametara različitim nosivim uređajima). U sigurnosnom smislu radi se o vrlo osjetljivom području budući da su podaci o zdravstvenom stanju po svojoj prirodi vrlo osobni i imperativ je sačuvati njihovu privatnost. S druge strane, kombinacijom tih podataka s drugim podacima mogu se implementirati i druge napredne usluge. Tako, primjerice, kombiniranjem medicinskih podataka s podacima o lokaciji pacijenata i podacima s društvenih mreža (iz kojih se može zaključiti s kime osoba ostvaruje socijalne kontakte) može se prevenirati širenje i epidemija zaraznih bolesti. O sigurnosti i privatnosti osjetljivih podataka poseb-

no je važno voditi računa kada više različitih entiteta ostvaruje pravo pristupa (Papageorgiou i sur., 2018).

Usluga pametnog transporta od velike je važnosti za funkcionalnost pametnog grada. Ona zapravo obuhvaća čitav niz različitih usluga – od usluge pametne navigacije (koja u obzir uzima i trenutačno stanje na prometnicama u pogledu mogućih gužvi ili zastoja), pronalaženja slobodnih parkirnih mjesta, preporuke obližnjih zanimljivih odredišta i slično. Precizni podaci o poziciji vozila obično se dobivaju pomoću sustava za satelitsku navigaciju (kakav je, primjerice, GPS sustav). Većina ostalih podataka koja se prikuplja u stvarnom vremenu prenosi se komunikacijom između vozila kao i komunikacijom vozila s fiksnom cestovnom infrastrukturom. Prema tome, kod usluge pametnog transporta postoji velika potreba za „horizontalnom" razmjenom podataka (izravno među vozilima) za razliku od ,primjerice, sustava pametne zdravstvene skrbi, gdje dominira „vertikalna" komunikacija (sa senzora prikupljeni podaci o zdravstvenom stanju šalju se nadređenoj zdravstvenoj ustanovi). U takvom okruženju izazov je sačuvati privatnost i anonimnost vozila (i putnika), a u isto vrijeme omogućiti im da sudjeluju u distribuiranom sustavu razmjene informacija (Heijden, Dietzel, Leinmuller i Kargl, 2019).

13.4. ZAKLJUČAK

Okruženje pametnog grada, kao i druge složene strukture koje se oslanjaju na paradigmu interneta stvari, otvaraju brojne sigurnosne izazove. Sigurnosna rješenja i mehanizmi poznati iz različitih konvencionalnih mreža često u tim slučajevima nisu izravno primjenjiva. Zbog toga je nužna njihova prilagodba kao i razvoj potpuno novih inovativnih sigurnosnih mehanizama što otvara mnogo prostora za daljnja istraživanja i razvoj. Mogući smjerovi istraživanja mnogobrojni su: razvoj novih i inovativnih metoda enkripcije (po mogućnosti uz što niže zahtjeve za resursima), razvoj naprednih rješenja za zaštitu integriteta podataka i za provjeru autentičnosti, razvoj sustava za otkrivanje zlonamjernog ponašanja i mogućih napada. Razvoj i implementacija odgovarajućih sigurnosnih rješenja podiže razinu sigurnosti što rezultira većim povjerenjem korisnika u suvremena tehnološka rješenja, a time i njihovim sve širim prihvaćanjem i uporabom što zasigurno dovodi do krajnjeg cilja – povećanja razine kvalitete života.

13.5. LITERATURA

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. i Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer Networks, 38*(4), 393-422.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. i Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and *Applications. IEEE Communication Surveys & Tutorials, 17*(4), 2347-2376.

Cui, L., Xie, G., Qu, Y., Gao, L. i Yang, Y. (2018). Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access, 6*, 46134-46145.

Ericsson (2017). Ericsson Mobility Report. Preuzeto s https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-november-2017.pdf, 1.5.2019.

Grgić, K. (2011). *Sustav za otkrivanje zlonamjernih čvorova u bežičnim senzorskim mrežama temeljenim na IPv6 protokolu*. Doktorska disertacija, Sveučilište J. J. Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija, Osijek.

Hamid, A., Rashid, M. i Hong, C. S., (2006*). Routing Security in Sensor Network: HELLO Flood Attack and Defense*. ICNEWS.

Heijden, R., Dietzel, S., Leinmuller, T. i Kargl, F. (2019). Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems. *IEEE Communications Surveys & Tutorials 21*(1), 779-811.

Hu, Y. C., Perrig, A. i Johnson, D. B. (2003). *Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks*. IEEE INFOCOM.

Kavitha, T. i Sridharan, D. (2010). Security Vulnerabilities In Wireless Sensor Networks: A Survey. *Journal of Information Assurance and Security 5*, 31-44.

Krauss, C., Schneider, M. i Eckert, C. (2008). On handling insider attacks in wireless sensor networks. *Information Security Technical Report*, *13,* 165-172.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G. i Wolff, S. (2009). A Brief History of the Internet. *ACM SIGCOMM Computer Communication Review, 39*(5), 22-31.

Lukasik, S. (2011). Why the Arpanet Was Built. *IEEE Annals of the History of Computing, 33*(3), 4-21.

Newsome, J., Shi, E., Song, D. i Perrig, A. (2004). *The Sybil Attack in Sensor Networks: Analysis and Defenses*. IPSN (Information Processing in Sensor Networks).

Ngai, E., Liu, J. i Lyu, M. R. (2007). An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. *Computer Communications, 30*, 2353-2364.

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A. i Patsakis, C. (2018). Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access, 6*, 9390-9403.

Saxena, M. (2007). *Security in Wireless Sensor Networks – A Layer Based Classification*. Cerias Tech Report.

Severance, C. (2014). Doug Van Houweling: Building the NSFNet. *Computer, 47*(4), 7-9.

Skyworks (2019). Enabling the Internet of Things – Solutions for a Connected World. Preuzeto s http://www.skyworksinc.com/downloads/literature/IoT_brochure.pdf, 1.5.2019.

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J. i Shen, X. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine, 55*(1), 122-129.

Zaključak

Novim sveučilišnim udžbenikom željeli smo educirati prosječnog korisnika informacijsko-komunikacijskih računalnih sustava, ali još više od toga – htjeli smo pobuditi svijest o važnosti zaštite sustava i digitalnih podataka zaštitom osobne privatnosti samog korisnika. Osim toga, izuzev samog pitanja informacijske sigurnosti, željeli smo upozoriti korisnike i na druge potencijalno štetne posljedice uporabe interneta, od zlostavljanja na internetu do štetnosti prekomjernog igranja računalnih igara na internetu što ostavlja trajne posljedice za zdravlje pojednica. Međutim, lažni osjećaj anonimnosti koju pruža internet, a koji je omogućio kršenje zakona i zloporabu korisnika, konačno je dobio odgovarajuće sankcije u zakonima i regulativama Republike Hrvatske i Europske unije te postoje jasno propisane kazne za počinitelje elektoriničkog zločina bilo da se radi o krađi identiteta ili novaca pa sve do psihičkog zlostavljanja pojedinca.

Rezultati dosadašnjih istraživanja pokazali su zabrinjavajuću razinu rizičnog ponašanja računalnih korisnika kao i različite nepoželjne posljedice neodgovarajuće upotrebe interneta te su pokazali veliku potrebu za ovakvim *udžbenikom* koji će biti osnova za različite vrste edukacija, od stručnih radionica pa sve do poslijediplomske razine u vidu specijalističkih studijskih programa koji će se sustavno baviti navedenom problematikom. U svakoj prevenciji prvi je korak razvoj svijesti i širenje znanja o problemima s kojima se treba suočiti, a upravo nam to omogućuje ovaj *udžbenik*.

Internetom se učestalo koristi sve mlađa i mlađa populacija. Studije na razini Europske unije jasno pokazuju da su srednjoškolci i osnovnoškolci vrlo česti korisnici interneta, s velikom količinom vremena koju provode na internetu (često i bez nadzora), a sve više su i predškolci upoznati s uporabom interneta, najčešće uporabom roditeljskih pamentih telefona i tableta. Buduća istraživanja, kao i prevencija, morat će uključiti i te najmlađe skupine računalnih korisnika ukoliko žele postići dugoročne pozitivne učinke. Osim edukacije korisnika, koja se pokazala važnom, ali nedovoljnom mjerom intervencije, ključna je odrednica intervencijskih programa izrada psiholoških profila različitih rizičnih korisnika računala kako bi se mjere i strategije mogle ciljano primijeniti na određene skupine i u konačnici postići veću učinkovitost u zaštiti digitalnih podataka.

Zaključujemo kako opreza nikad dosta, a neopreznost i lakovjernost na internetu kod mnogih korisnika interneta sve češće dolazi na naplatu. Doslovno na naplatu, jer sve prevare, lažna predstavljanja, zlostavljane i nasilje na internetu, krađa osobnih i drugih podataka na kraju se svode na financijski ili zdravstveni gubitak. Najbolja zaštita na internetu je obrazovani korisnik koji se zna zaštiti od potencijalnih opasnosti.

ŽELIMO VAM USPJEH U EDUKACIJI RAČUNALNIH KORISNIKA!

doc. dr. sc. Krešimir Šolić
izv. prof. dr. sc. Tena Velki

O AUTORIMA

Ivana Borić Letica, mag. psych., doktorandica

Fakultet za odgojne i obrazovne znanosti
Sveučilišta Josipa Jurja Strossmayera u Osijeku

e-pošta: ivanaboric9@yahoo.com

Ivana Borić Letica rođena je 1991. godine u Osijeku. Diplomirala je psihologiju 2015. godine na Filozofskom fakultetu u Osijeku s odličnim akademskim uspjehom. Dobitnica je Rektorove nagrade za akademsku godinu 2015./2016. za rad pod nazivom *Analiza stanja upravljanja ljudskim resursima*. Godine 2015. završila je Pedagoško-psihološko-didaktičko-metodičku izobrazbu na Učiteljskom fakultetu u Osijeku, a 2017. godine završila je četiri modula edukacije „Čarobna svjetiljka" za stručnjake koji rade s djecom podržanu od strane Međunarodne akademije za terapiju igrom i psihosocijalne projekte pri Centru za terapiju igrom u Zagrebu. Od 2017. godine u edukaciji je iz bihevioralno-kognitivnih terapija (trenutno 2. stupanj). Godine 2015. radila je kao stručni suradnik psiholog u OŠ Vladimira Becića u Osijeku, a trenutno radi kao nastavnik Psihologije, Psihologije prodaje, Poslovne psihologije i Primijenjene komunikacije u Tehničkoj školi i prirodoslovnoj gimnaziji Ruđera Boškovića Osijek, Ekonomskoj i upravnoj školi Osijek i Trgovačkoj i komercijalnoj školi „Davor Milas" Osijek. Od 2017. godine sudjeluje u radu Društva za psihološku pomoć Sunce u Osijeku, a od 2018. godine radi kao vanjski suradnik na Fakultetu za odgojne i obrazovne znanosti u Osijeku na kolegijima Razvojne psihologije, Psihologije učenja i poučavanja, Psiholoških osnova poremećaja u ponašanju i Odabranih tema iz psihologije odraslih. Sudjelovala je na jedanaest stručnih i znanstvenih domaćih i međunarodnih konferencija te za sada objavila šest radova na temu prevencije vršnjačkog nasilja, metakognicije, samoreguliranog učenja te rizičnog ponašanja na internetu. Od 2019. godine doktorandica je psihologije na Filozofskom fakultetu u Zagrebu.

doc. dr. sc. Tijana Borovac

Fakultet za odgojne i obrazovne znanosti
Sveučilišta Josipa Jurja Strossmayera u Osijeku

e-pošta: tborovac@foozos.hr

Tijana Borovac rođena je u Osijeku. Godine 2002. diplomirala je na Visokoj učiteljskoj školi u Osijeku stekavši zvanje odgojitelj predškolske djece. Tijekom školovanja 2000. godine dobila je Rektorovu nagrada za izniman uspjeh na studiju. Godine 2004. diplomirala je na Ekonomskom fakultetu u Osijeku, smjer marketing management stekavši zvanje diplomirani ekonomist. Doktorirala je u studenom 2014. godine obranom rada *Socijalna interakcija djece u dobno mješovitim skupinama ustanova ranoga i predškolskoga odgoja* na Poslijediplomskom sveučilišnom doktorskom studiju pedagogije smjer Rani odgoj i obrazovanje u obiteljskom i institucionalnom okruženju na Filozofskom fakultetu Sveučilišta u Zagrebu i time stekla akademski stupanj doktorice znanosti iz područja društvenih znanosti, polja pedagogije. Radno iskustvo stjecala je od 2000. godine radeći u nevladinim organizacijama na projektima koji se bave odgojem i obrazovanjem (Catholic RelIef Sevices, Udruga za rad s mladima „Breza") sve do 2007. kada je zaposlena na Fakultetu za odgojne i obrazovne znanosti u Osijeku, u znanstvenom području društvenih znanosti, znanstveno polje pedagogija, znanstvena grana opća pedagogija. Na Odsjeku za društvene znanosti Fakulteta za odgojne i obrazovne znanosti Sveučilišta J. J. Strossmayera u Osijeku sudjeluje u izvedbi nastave više pedagoških kolegija na preddiplomskom i diplomskom studiju Ranoga i predškolskoga odgoja i obrazovanje. Autorica je više znanstvenih radova, sudjelovala na brojnim međunarodnim i domaćim konferencijama, mentorica na diplomskim i završnim radovima studenata Ranog i predškolskog odgoja, suradnica na projektima („116000 Hotline for Missing Children Croatia", „Safer Internet Centre Croatia: Making Internet a good and safe place", „Kognitivna otpornost djece u riziku od siromaštva u Istočnoj Slavoniji", „Mikrosimulacijsko modeliranje pješačkog kretanja djece sa ciljem povećanja sigurnosti pješačkog kretanja djece") te glavna istraživačica na projektu „Problemi u ponašanju djece školske dobi: Uloga izvršnih funkcija, individualnih, obiteljskih i genetskih čimbenika" financiranog od Hrvatske zaklada za znanost (HRZZ- IP-2016-06-3917).

Ivana Duvnjak, asistentica psihologije
Filozofski fakultet Sveučilišta Josipa Jurja Strossmayera u Osijeku
e-pošta: iduvnjak@ffos.hr

Ivana Duvnjak završila je Filozofski fakultet u Osijeku, smjer diplomirani psiholog/ profesor psihologije. Tijekom studija dodijeljena joj je državna i županijska stipendija. Godinama je radila u praksi kao stručna suradnica psihologinja i profesorica psihologije u više osnovnih i srednjoj školi. Položila je psihološki stručni ispit u Hrvatskoj psihološkoj komori i stekla osnovnu dopusnicu te položila stručni ispit za stručne suradnike psihologe. Trenutačno radi kao asistentica iz područja opće psihologije na Odsjeku za psihologiju Filozofskog fakulteta Sveučilišta J. J. Strossmayera u Osijeku. Izvodi nastavu iz kolegija koji se odnose na područja razvojne, opće psihologije i prevencije. Sudjelovala je na više projekata o sigurnosti djece na internetu i sličnim temama o djeci i mladima („Sigurnost djece na Internetu“ – Sigurnih pet za sigurniji net, istraživački projekt „Djeca (0–8) i digitalna tehnologija“, projekt "Safer Internet Centre Hrvatska – Making internet a good and safe place"). Aktivno je sudjelovala na preko 20 međunarodnih i domaćih znanstveno-stručnih skupova i konferencija. U koautorstvu je objavila desetak radova te poglavlja u monografiji i priručnicima. Aktivno se uključuje i sudjeluje kao suradnica u aktivnostima znanstveno-stručnih projekata. Koautorica je znanstvenih radova o razvojnim karakteristikama djece i mladih, djece s teškoćama u razvoju i rizičnih ponašanja. Pohađa poslijediplomski doktorski studij psihologije na Filozofskom fakultetu Sveučilišta u Rijeci. Članica je Hrvatske psihološke komore i Hrvatskog psihološkog društva. Tajnica je i članica upravnog odbora Društva psihologa Osijek od 2018. godine. Aktivno je sudjelovala kao članica u organizaciji dosadašnjih znanstveno-stručnih skupova Odsjeka za psihologiju te je članica organizacijskog odbora 27. godišnje konferencije hrvatskih psihologa.

izv. prof. dr. sc. Krešimir Grgić

Fakultet elektrotehnike, računarstva i informacijskih tehnologija
Sveučilišta Josipa Jurja Strossmayera u Osijeku

e-pošta: kresimir.grgic@ferit.hr

Dr. sc. Krešimir Grgić radi kao izvanredni profesor na Zavodu za komunikacije Fakulteta elektrotehnike, računarstva i informacijskih tehnologija u Osijeku. Na istom fakultetu diplomirao je 2005. godine, a doktorsku disertaciju na temu *Sustav za otkrivanje zlonamjernih čvorova u bežičnim senzorskim mrežama temeljenim na IPv6 protokolu* obranio je 2011. godine. Aktivno sudjeluje u izvođenju nastave (predavanja, auditorne i laboratorijske vježbe) iz više kolegija na preddiplomskom, diplomskom i stručnom studiju. Kao mentor i sumentor vodio je veći broj studenata kroz izradu diplomskih i završnih radova. Područje znanstvenog istraživanja su mu računalne i komunikacijske mreže, internetski protokoli, sigurnost u računalnim i komunikacijskim mrežama, zaštitno kodiranje, bežične senzorske mreže. Objavio je više članaka u domaćim i stranim znanstvenim i stručnim časopisima te na međunarodnim i domaćim stručnim skupovima i konferencijama. Sudjelovao je i u provedbi nekolicine znanstvenih i stručnih projekata: „Širokopojasni pristup i internetske usluge u ruralnim područjima“, „Postupci raspoređivanja u samoodrživim raspodijeljenim računalnim sustavima“ (projekti MZOŠ), ITEA-ESNA (*European Sensor Network Architecture*), CryptoChaos (BICRO PoC). Član je strukovne udruge IEEE.

izv. prof. dr. sc. Barbara Herceg Pakšić
Pravni fakultet Sveučilišta Josipa Jurja Strossmayera u Osijeku
e-pošta: barbara.herceg@pravos.hr

Barbara Herceg Pakšić rođena je u Osijeku 8. svibnja 1984. Tijekom fakultetskog obrazovanja bila je višestruko nagrađivana, a diplomirala je na Pravnom fakultetu u Osijeku 28. veljače 2008. godine diplomom *magna cum laude*. Doktorsku disertaciju pod naslovom *Ispričavajući razlozi u kaznenom pravu* obranila je 11. lipnja 2014. na Pravnom fakultetu u Zagrebu. Za uspjeh na doktorskom studiju primila je diplomu *summa cum laude*. Od travnja 2016. godine docentica je na Katedri kaznenopravnih znanosti Pravnog fakulteta u Osijeku. Tijekom svoje znanstvene karijere sudjelovala je u nekoliko projekata kao aktivni istraživač, izlagala je na brojnim domaćim i međunarodnim znanstvenim skupovima u Hrvatskoj i inozemstvu (Slovačka, Srbija, Mađarska, Turska, Litva…). Studijski posjeti, gostujuća predavanja i stručna usavršavanja uključuju Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg im Breisgau, Njemačka; Institut für Recht- und Kriminalsoziologie, Vienna, Austrija, Department of Law University of Mannheim, Njemačka; Hochschule für öffentliche Verwaltung Kehl, Njemačka; Rechtswissenschaftlichen Fakultät, Albert-Ludwigs-Universität Freiburg im. Br., Njemačka; Faculté de Droit de Sciences Politiques et de Gestion, Université de Strasbourg, Francuska; Universia Niccolo Cusano Rome, Italija, Università degli Studi dell'Insubria, Como, Italija. Dobitnica je istraživačke stipendije na Europa Institutu, Saarbrücken, Njemačka. Izvršna je urednica časopisa *Pravni vjesnik* koji izdaje Pravni fakultet u Osijeku. Članica je uredničkog odbora publikacije *EU and comparative law issues and challenges,* (ECLIC) series. Predsjednica je Povjerenstva za osiguranje i unapređenje kvalitete na Pravnom fakultetu u Osijeku. Članica je Hrvatskog udruženja za kaznenopravne znanosti i praksu, International Association of Penal Law, European Group for the Study of Deviance and Social Control. Upisana je u upisnik znanstvenika pod brojem 316534. Objavila je veći broj znanstvenih radova te je cjelovita publikacijska lista dostupna na službenoj stranici Hrvatske znanstvene bibliografije.

Ivan Horvat
OTIS d.o.o, Osijek
e-pošta: ivan@otis-os.hr

Ivan Horvat, bacc. oec. rođen je u Osijeku 1976. godine. Nakon osnovne škole upisuje 1. gimnaziju (opću) te nakon nje Elektrotehnički fakultet u Osijeku koji napušta nakon upisa apsolventske godine i zaposlenja. Godine 2014. upisuje Veleučilište Baltazar Zaprešić te nakon tri godine stječe zvanje stručni prvostupnik ekonomije. Od 2002. godine posebno područje interesa su mu računalne mreže, serveri i sigurnost podataka. Vrši usluge projektiranja, izgradnje i održavanja informacijskih sustava za male i srednje tvrtke te neprofitne organizacije (više udruga, Katolička crkva). Aktivni je član open-source zajednice, promotor programa otvorenog koda te ljubitelj Linux operacijskih sustava. Autor i koautor je nekoliko članaka o računalnoj sigurnosti, uputstava za sigurnu uporabu računala te Priručnika za informacijsku sigurnost i zaštitu privatnosti Fakulteta za odgojne i obrazovne znanosti Osijek. Intenzivno se bavio odnosima s kupcima (CRM), položio je tečaj austrijske tvrtke Mesonic, napisao završni rad na Veleučilištu na tu temu te radio implementaciju i prilagodbu CRM rješenja za poslovne subjekte. Od 2017. godine bavi se i Općom uredbom o zaštiti podataka (GDPR) te njezinom implementacijom u poslovnim subjektima. Zaposlen je u tvrtki OTIS d.o.o. kao prokurist i CTO, vlasnik je obrta BIT – za poslovno i informatičko savjetovanje te tehnički savjetnik i član nadzornog odbora Centra za nestalu i zlostavljanu djecu (CNZD). Tajnik je i osnivač Udruge Dekanter – za promicanje etno-gastro kulture te jedan od suorganizatora Festivala vina, delicija i ugodnog življenja WineOS.

izv. prof. dr. sc. Vesna Ilakovac

Medicinski fakultet Sveučilišta Josipa Jurja Strossmayera u Osijeku

e-pošta: vesna.ilakovac@mefos.hr

Izv. prof. dr. sc. Vesna Ilakovac rođena je 1962. godine u Osijeku. Profesorica je matematike i fizike, magistrirala je na Medicinskom fakultetu Sveučilišta u Zagrebu, a doktorirala na Medicinskom fakultetu Sveučilišta J. J. Strossmayera u Osijeku. Od 1987. do 1996. godine radila je u Odsjeku za informatiku KBC Osijek kao projektant, a od 1996. godine stalno je zaposlena na Medicinskom fakultetu Sveučilišta J. J Strossmayera u Osijeku. Voditelj je više kolegija iz područja medicinske statistike i medicinske informatike na studijima medicine, medicinsko-laboratorijske dijagnostike, poslijediplomskom specijalističkom studiju i poslijediplomskom doktorskom studiju. Bila je voditelj i suradnik na više projekata financiranih od strane Ministarstva znanosti i obrazovanja i Europske unije. Članica je Hrvatskog društva za medicinsku informatiku i Hrvatskog biometrijskog društva od njihova osnutka. Od 2009. godine članica je Odbora za e-zdravlje Akademije medicinskih znanosti Hrvatske. U 2012. godini imenovana je članicon Povjerenstva za strategiju informatizacije sustava zdravstva pri Ministarstvu zdravlja Republike Hrvatske. Od 2016. godine redoviti je član Akademije medicinskih znanosti Hrvatske.

Kristina Kralik, prof., predavač

Medicinski fakultet Sveučilišta Josipa Jurja Strossmayera u Osijeku

e-pošta: kristina.kralik@mefos.hr

Kristina Kralik rođena je 1964. godine u Osijeku. Zvanje profesora matematike i fizike stječe 1988. godine na Pedagoškom fakultetu Sveučilišta Josipa Jurja Strossmayera u Osijeku. Nakon rada u obrazovnim ustanovama 1992. godine zapošljava se u Kliničkoj bolnici Osijek. Od srpnja 2012. godine izabrana je u naslovno suradničko zvanje asistenta, a od listopada 2013. radi kao predavačica na Medicinskom fakultetu Sveučilišta Josipa Jurja Strossmayera u Osijeku na Katedri za medicinsku statistiku i medicinsku informatiku. Posebno joj je područje interesa biostatistika. Autorica je dvaju poglavlja sveučilišnog udžbenika te autorica ili koautorica u više od 40 znanstvenih radova (od kojih je 8 objavljeno u časopisima zastupljenim u bibliografskoj bazi Current Contents). Trenutno je polaznica poslijediplomskog doktorskog studija Biomedicina i zdravstvo. Članica je Hrvatskog biometrijskog društva (HBMD) i Hrvatskog društva za medicinsku informatiku (HDMI).

izv. prof. dr. sc. Krešimir Nenadić

Fakultet elektrotehnike, računarstva i informacijskih tehnologija
Sveučilišta Josipa Jurja Strossmayera u Osijeku

e-pošta: knenadic@ferit.hr

Krešimir Nenadić rođen je 12. srpnja 1975. godine u Požegi. Osnovnu školu pohađao je u Kutjevu te nakon završetka upisuje Matematičku gimnaziju u Požegi. Nakon srednjoškolskog obrazovanja 1994. godine upisuje studij na Elektrotehničkom fakultetu u Osijeku. Na drugoj godini studija upisuje smjer elektronika i automatizacija. Diplomirao je 2000. godine te se iste godine zapošljava na Elektrotehničkom fakultetu u Osijeku, prvo kao stručni suradnik, a ubrzo nakon toga dobiva status znanstvenog novaka. Godine 2001. upisuje se na poslijediplomski magistarski studij. Nakon kratkog prekida zbog odlaska na služenje vojne obveze u OS RH 2002. godine, prebacuje se na poslijediplomski doktorski studij računarstva. Doktorirao je 2010. godine. Uspješno obranivši doktorsku disertaciju pod nazivom *Mogućnost primjene diferencijalne digitalne holografije u kontroli kvalitete* pod mentorstvom prof. dr. sc. Franje Jovića, a sljedeće godine, 2011., dobiva izbor u znanstveno/nastavno zvanje docenta. Trenutno radi na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku kao izvanredni profesor na Katedri za programske jezike i sustave u sastavu Zavoda za programsko inženjerstvo. Sudjeluje u izvođenju nastave kao nositelj i izvođač predavanja na kolegijima iz područja osnova programiranja (programski jezici C, C++), tehnologija web programiranja (klijentske i poslužiteljske tehnologije: HTML, CSS, JavaScript, PHP) i programiranja mobilnih uređaja (Android platforma i programski jezik Java). Završio je Cisco edukaciju za instruktore 2003. godine u Zagrebu i radio kao Cisco CCNA instruktor/predavač na lokalnoj Cisco akademiji mrežnih tehnologija na FERIT-u. Područja u kojima se bavio znanstvenim istraživanjima su: digitalna holografija, procjena rizika informacijskih sustava, postupci razvrstavanja podataka, izrada i primjena upitnika sigurnog ponašanja korisnika informacijskog sustava. Sudjelovao je na nekoliko LABUS sajmova i sveučilišnih smotri čiji je cilj popularizacija znanosti.

doc. dr. sc. Ksenija Romstein

Fakultet za odgojne i obrazovne znanosti
Sveučilišta Josipa Jurja Strossmayera u Osijeku

e-pošta: kromstein@foozos.hr

Dr. sc. Ksenija Romstein radi kao docentica iz područja edukacijsko-rehabilitacijskih znanosti na Fakultetu za odgojne i obrazovne znanosti u Osijeku. Suradnica je na nekoliko europskih projekata koji se bave problematikom inkluzivnog obrazovanja, prava djece čiji su roditelji u zatvoru i sigurnosti na interentu djece i mladih. Autorica je više znanstvenih radova na temu inkluzivnog odgoja i obrazovanja. Tijekom 2015. i 2016. godine surađivala je s UNESCO Janusz Korczak Chair of Interdicsciplinary Studies on Child Development and Well-being (Varšava, Poljska) gdje je vodila radionice i seminare na međunarodnim ljetnim školama na temu integracije izbjeglica i azilanata te inkluzije i participacije djece s posebnim potrebama. Tijekom 2017. i 2018. surađivala je s Uredom pravobraniteljice za djecu Republike Hrvatske na temu zaštite i zagovaranja prava djece čiji su roditelji u zatvoru. U posljednjih godinu dana aktivna je na istraživačkim projektima interdisciplinarne naravi koji se bave prenatalnim čimbenicima rizika te kvalitativnim metodama istraživanja djetinjstva.

dr. sc. Valentina Ružić
Zagreb
e-pošta: vruzic12@gmail.com

Dr. sc. Valentina Ružić diplomirala je na Filozofskom fakultetu Sveučilišta u Zagrebu 2006. godine, a na istom je Sveučilištu 2013. stekla akademski stupanj doktora znanosti iz znanstvenog područja društvenih znanosti, znanstveno polje psihologija. Od 2006. godine zaposlena je u Nakladi Slap ponajprije na poslovima psihometrijske provjere, adaptacije i normiranja psihodijagnostičkih sredstava te organiziranja i održavanja edukacija za stručnjake (pri čemu je predavačica na nekoliko njih). Do sada je objavila više znanstvenih radova na temu validacije psihodijagnostičkih instrumenata. Urednica je *Priručnika za Big Five upitnik za djecu* te koautorica nekoliko poglavlja u priručnicima i publikacijama o psihodijagnostičkim sredstvima namijenjenima ispitivanju inteligencije i ličnosti djece i odraslih. Bila je jedan od voditelja radionica za djecu u sklopu projekta Poticanje čitanja kroz učenje o toleranciji i nenasilju podržanog od strane Ministarstva poduzetništva i obrta Republike Hrvatske i urednica je zbornika proizišlog iz tog projekta. Predmet je njezina istraživačkog interesa ispitivanje uloge različitih kognitivnih faktora u doživljaju boli u eksperimentalnim uvjetima, a koautorica je rada koji je osvojio nagradu za mlade znanstvenike (*The role of experience in the assessment of pain in others*) u sklopu Alps Adria Psychology Conference 2010. Aktivno je sudjelovala i izlagala na više od 30 međunarodnih i domaćih skupova i konferencija. Vanjska je suradnica Odsjeka za psihologiju Filozofskog fakulteta u Zagrebu na kolegijima Psihologijski praktikum I, II i III. Od 2018. vanjska je suradnica Fakulteta za odgojne i obrazovne znanosti Sveučilišta Josipa Jurja Strossmayera u Osijeku gdje u sklopu izvanrednog diplomskog studija Ranoga i predškolskoga odgoja i obrazovanja sudjeluje u izvedbi nastave nekoliko kolegija, među kojima su *Psihologija dječje igre* i *Psihologija poticanja dječjeg razvoja*. U tom je području njezin istraživački interes usmjeren primarno na računalne igre i njihovu ulogu u razvoju djece. Članica je Hrvatskog psihološkg društva (HPD) i Hrvatske psihološke komore (HPK).

izv. prof. dr. sc. Daniela Šincek
Filozofski fakultet Sveučilišta Josipa Jurja Strossmayera u Osijeku
e-pošta: dsincek@ffos.hr

Diplomirala je 2000. godine, a magistrirala (magisterij znanosti) stekla 2009. godine na tema *Obilježja mladih s ranim i kasnim javljanjem devijantnog i delinkventnog ponašanja* i doktorirala 2011. godine na temu *Utjecaj vršnjaka i spremnost na rizično ponašanje mladih* u području socijalne psihologije na Filozofskom fakultetu u Zagrebu. Tijekom studija dodijeljena joj je državna stipendija u kategoriji A (za izrazito uspješne studente). Radila je kao psihologinja na zamjeni u osnovnoj školi (travanj 2001.), znanstveni novak na Pedagoškom fakultetu u Osijeku (svibanj 2001. – srpanj 2002.), psihoginja u Centru za socijalnu skrb u Osijeku (srpanj 2002. – veljača 2006.), a od ožujka 2006. godine počinje raditi kao asistentica na tadašnjoj Katedri za psihologiju Filozfoskog fakulteta u Osijeku. Izabrana je u zvanje docentice 2012., u zvanje više znanstvene suradnice 2018., a u zvanje izvanredne profesorice 2019. godine. Predaje na Odsjeku za psihologiju Filozofskog fakulteta u Osijeku, na Preddiplomskom studiju socijalnog rada te na Odjelima za matematiku, kemiju, biologiju i fiziku iz više metodoloških i kolegija iz socijalne i opće psihologije. Područje njezina znanstvenog interesa su: rizično ponašanje mladih, osobito u digitalnom okruženju (*sexting,* problematično igranje igrica, problematična uporaba interneta, vršnjačko nasilje na internetu, nezadovoljstvo vlastitim izgledom) te utjecaji vršnjaka, roditelja i medija (posebice interneta i IKT-a). Kao istraživačica ili ekspertica sudjelovala na više znanstvenih i stručnih projekata, a vodila je znanstveni projekt Istraživanje novijih oblika rizičnog ponašanja mladih i nacionalno istraživanje u okviru stručnog projekta "Safer Internet Centre Croatia – Making internet a good and safe place". Članica je Hrvatskog psihološkog društva i Hrvatske psihološke komore. Sudjelovala u organizaciji (kao članica, tajnica ili predsjednica) dosadašnjih znanstveno-stručnih skupova Odsjeka za psihologiju FFOS-a, bila gošća-urednica posebnog broja Života i škole, urednica knjiga sažetaka sa skupova Odsjeka te članica organizacijskih (2005. i 2012.) i programskog (2015.) odbora godišnje konferencije hrvatskih psihologa. Predsjednica je programskog odbora 27. godišnje konferencije hrvatskih psihologa (Psihologija i digitalni svijet, 2019.).

izv. prof. dr. sc. Goran Vojković
Fakultet prometnih znanosti Sveučilišta u Zagrebu
e-pošta: goran.vojkovic@fpz.hr

Izv. prof. dr. sc. Goran Vojković rođen je u Splitu 1971. godine. Pravni fakultet završio je u Splitu 1996. godine gdje je magistrirao 2003. godine na temu *Pomorsko dobro Republike Hrvatske*, a 2006. doktorirao na temu *Pravni status luka unutarnjih voda*. Napisao je dvije znanstvene monografije, dva priručnika i nekoliko poglavlja u knjigama, a ima i objavljen veći broj znanstvenih i stručnih radova. Goran Vojković ima više od 20 godina iskustva rada u državnoj službi i privatnom sektoru, na različitim poslovima, od savjetnika u Vladinom uredu do direktora službe za pravo u korporativnom upravljanju u kompaniji iz IT-sektora. Bio je u dva mandata predsjednik Upravnog vijeća Lučke uprave Vukovar, četiri godine član Nadzornog odbora JANAF-a, a sada je po drugi put vanjski put član Odbora za zakonodavstvo Hrvatskoga sabora. Također, ima veliko iskustvo na radu s EU projektima u Hrvatskoj i Bosni i Hercegovini. Osim općeprometnim i pomorskom pravom bavi se i pravom elektroničkih komunikacija te zaštitom osobnih podataka. Aktivan je radioamater. Trenutno radi kao izvanredni profesor na Fakultetu prometnih znanosti u Zagrebu i Sveučilištu Sjever te surađuje s nekoliko drugih učilišta. Također se bavi i novinarstvom. Živi u Ivanić-Gradu.

doc. dr. sc. Marin Vuković
Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu
e-pošta: marin.vukovic@fer.hr

Marin Vuković docent je na Zavodu za telekomunikacije Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu. Diplomirao je 2006. godine na smjeru Telekomunikacije i informatika Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu s diplomskim radom pod nazivom *Isporuka lokacijski specifičnog sadržaja pokretnim korisnicima*, a doktorirao 2011. godine na istom fakultetu s disertacijom pod nazivom *Adaptivno upravljanje lokacijskom informacijom za telekomunikacijske usluge s dodanom vrijednosti*. Objavio je više od 40 znanstvenih i stručnih radova na konferencijama i u časopisima. Aktivno je sudjelovao na panelima, okruglim stolovima te održao pozvana predavanja s ciljem popularizacije struke i znanosti. Koautor je patenta pod nazivom "Uređaj i postupak za prepoznavanje riječi i fraza te njihovog značenja iz slobodnog teksta u obliku elektroničkog sadržaja" pri Državnom zavodu za intelektualno vlasništvo. Kao voditelj, istraživač i sudionik sudjelovao je na domaćim znanstvenim projektima, projektima financiranim sredstvima Europske unije te na više projekata suradnje s gospodarstvom. Voditelj je projekta „WWW.HR - Početna stranica Republike Hrvatske" u suradnji s Hrvatskom akademskom i istraživačkom mrežom CARNet. Zamjenik je voditelja „Laboratorija za sigurnost i privatnost (SPL)" i „Laboratorija za asistivne tehnologije i potpomognutu komunikaciju (ICT-AAC)" na Fakultetu elektrotehnike i računarstva Sveučilišta u Zagrebu. Član je strukovnih udruga IEEE i KES International.

DR. SC.
TENA VELKI

Dr. sc. Tena Velki radi kao izvanredna profesorica iz područja razvojne psihologije na Fakultetu zaodgojne i obrazovne znanosti u Osijeku te trenutno obavlja i funkciju prodekanice za znanost. Vanjska je suradnica na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija i na Filozofskom fakultetu u Osijeku. Aktivna je članica Hrvatskog psihološkog društva (HPK), članica Hrvatske psihološke komore (HPK), dopredsjednica Društva psihologa Osijek (DPO), članica Hrvatskog udruženja za bihevioralno-kognitivne terapije (HUBIKOT), članica Europske federacije psiholoških udruga (EFPA) te jedna od osnivačica udruge Kluba studenata psihologije Filozofskog fakulteta u Osijeku (PSIHOS). Za značajan znanstveni rad primila je nekoliko priznanja: Fakultet za odgojne i obrazovne znanosti 2015. dodjeljuje joj priznanje za uspješan rad i izniman doprinos djelovanju i ugledu Fakulteta, 2016. primila je i stipendiju UNESCO-a Poljska za osobit doprinos u radu na promicanju prava djece s teškoćama u razvoju, 2017. godine Hrvatsko psihološko društvo dodijelilo joj je priznanje za osobito vrijedan doprinos „Tjednu psihologije u Hrvatskoj“, a 2018. godine Hrvatsko psihološko društvo dodijelilo joj je Društveno priznanje „Marulić: Fiat Psychologia“ za osobito vrijedan doprinos razvitku i promicanju hrvatske psihologije. Objavila je niz znanstvenih i stručnih radova kao i knjiga te aktivno sudjelovala na više od 60 međunarodnih konferencija. Nositeljica je i voditeljica *Programa osposobljavanja pomoćnika za djecu s teškoćama u razvoju i osobe s invaliditetom* te poslijediplomskog specijalističkog studija *Inkluzivnog odgoja i obrazovanja*. Područjem informacijske sigurnosti i rizičnog ponašanja računalnih korisnika aktivno se bavi posljednjih pet godina. Pisala je radove i bila predavačicom na temu elektroničkog vršnjačkog nasilja, uloge računalnih igara na internetu u nastavi, a sudjelovala je i u organizaciji okruglog stola „Tehnologijom lakše do dječjih prava“. Najznačajniji joj je doprinos u tom području izrada mjernog instrumenata *Upitnika znanja i rizičnog ponašanja računalnih korisnika* (Velki i Šolić, 2014) te prvog sveučilišnog udžbenika na temu informacijske sigurnosti *Priručnik za informacijsku sigurnost i zaštitu privatnosti* (Velki i Šolić, 2018).

DR. SC.
KREŠIMIR ŠOLIĆ

Dr. sc. Krešimir Šolić rođen je 1976. godine u Osijeku. Nakon Opće gimnazije studira na Elektrotehničkom fakultetu u Osijeku. Kao student bio je aktivni član međunarodne studentske organizacije za razmjenu IAESTE te tajnik lokalnog odbora navedene organizacije u Osijeku. Na stručnoj praksi u Švedskoj, u Ericssonu Mobile Data Design AB, u Geteburgu, piše dipolmski rad na temu povezanosti CRM i UMTS sustava *Odnos tehnologije mobilnih sustava (GSN) i kupcu orijentiranog menadžmenta (CRM) (CRM – Tools and Structure of the Support Organisations).* Prvo radno mjesto 2002. godine bilo je pripravnik, mrežni administrator u Tajništvu Osječko-baranjske županije, a nakon kraćeg rada u privatnoj tvrtki Bello na servisiranju računalne opreme te po završetku prvog stupnja CISCO akademije na Elektrotehničkom fakultetu, 2005. godine počinje raditi kao CARNet sistem inženjer i voditelj videokonferencijkog sustava na Medicinskom fakultetu u Osijeku. Od 2008. godine radi kao znanstveni novak na projektu o autorstvu i čestitosti u znanosti (HRZZ projekt: „Valjanost podataka objavljenih u znanstvenom časopisu“) te vodi vježbe iz više predmeta iz područja biostatistike i medicinske informatike. Doktorat brani 2013. godine na Elektrotehničkom fakultetu u Osijeku s modelom inteligentnog sustava *Model za procjenu razine sigurnosti računalnog sustava zasnovan na ontologiji i algoritmu za evidencijsko zaključivanje,* smjer komunikacije i informatika. Iste godine pokreće obrt za analizu i zaštitu podataka ANSY. Docentom je postao početkom 2016. godine. Krešimir je član Hrvatskog biometrijskog društva (HBMD), član je Hrvatskog društva za medicinsku informatiku (HBMD) te međunarodne organizacije IEEE. Posljednjih 10 godina sudjeluje u nastavi na više predmeta iz područja biostatistike i medicinske informatike, dok mu je uže područje znanstvenog rada informacijska i računalna sigurnost s naglaskom na utjecaj korisnika na cjelokupnu informacijsku sigurnost i zaštitu privatnosti. Do danas je objavio više od 40 znanstvenih radova. Ponosni je otac blizanaca te s obitelji živi na rubu Kopačkog rita u mjestu Bilje.

9 789536 965885