

MALOLETNICI I SAJBER KRIMINAL

Dr Dragan Prlja, naučni saradnik
Institut za uporedno pravo, Beograd

Dr Vanja Korać
Matematički institut SANU, Beograd

Mr Andrej Diligenski, istraživač saradnik
Spoljni saradnik Instituta za uporedno pravo

Razvoj novih informacionih tehnologija omogućio je neslućeni razvoj i napredak, ali je doneo i mnogobrojne probleme. Često realni svet maloletna lica zamenjuju sa virtuelnim svetom provodeći veliki broj sati pored računara deleći informacije, fotografije, poruke sa poznatim, a često i sa potpuno nepoznatim novim virtuelnim "prijateljima". Nažalost virtuelni "prijatelji" nisu uvek dobronamerni i žele da manipulišu maloletnicima, žele da ih seksualno iskorištavaju, da ih prevare, ili da im na drugi način nanesu štetu. Maloletnici u obrazovnom sistemu i u porodici ne stiču dovoljno informacija potrebnih da bi na bezbedan način koristili Internet i društvene mreže što može da ima izuzetno teške posledice. Sve veći broj slučajeva sajber kriminala u svetu i kod nas ukazuje na potrebu stalnog unapređivanja sistema zakonodavne regulative, sistema primena propisa, i sistema prevencije kada je u pitanju sajber kriminal, a posebno u slučajevima kada su maloletnici žrtve ili počinioci krivičnih dela sajber kriminala.

KLJUČNE REČI: sajber kriminal / pravo / krivična dela / maloletna lica / Internet / informacione tehnologije

UVOD

Nastanak računara i njihova široka upotreba osamdesetih godina dvadesetog veka i nastanak računarskih mreža i njihova globalna upotreba devedesetih godina dvadesetog veka promenili su način života ljudi širom planete. Prvi računari vrlo kratko vreme bili su izolovani od ostalih računara i iz tog razloga njihova upotreba nije donosila previše rizika i opasnosti. Sa razvojem računarskih mreža računari su prvo povremeno, a kasnije i stalno postali deo lokalnih mreža, a ubrzo i deo globalne računarske mreže Interneta. Danas gotovo da nema kompanije koja nije 24h povezana sa globalnom računarskom mrežom Internetom, a broj pojedinaca koji koriste svakodnevno neke servise globalne računarske mreže meri se stotinama miliona, pa i milijardama.

Tabela 1: Statistika upotrebe Interneta na svetskom nivou u odnosu na populaciju iz juna 2014. godine¹

Svetski regioni	Populacija (2014.)	Internet korisnici Dec. 31. 2000	Internet Korisnici Poslednji podaci	Penetracija (% Populacije)	Rast 2000-2014	Korisnici % prema tabeli
Afrika	1,125,721,038	4,514,400	297,885,898	26.5 %	6,498.6 %	9.8 %
Azija	3,996,408,007	114,304,000	1,386,188,112	34.7 %	1,112.7 %	45.7 %
Evropa	825,824,883	105,096,093	582,441,059	70.5 %	454.2 %	19.2 %
Bliski Istok	231,588,580	3,284,800	111,809,510	48.3 %	3,303.8 %	3.7 %
Severna Amerika	353,860,227	108,096,800	310,322,257	87.7 %	187.1 %	10.2 %
Latinska Amerika / Karibi	612,279,181	18,068,919	320,312,562	52.3 %	1,672.7 %	10.5 %
Okeanija / Australija	36,724,649	7,620,480	26,789,942	72.9 %	251.6 %	0.9 %
SVET UKUPNO	7,182,406,565	360,985,492	3,035,749,340	42.3 %	741.0 %	100.0 %

Jednostavni korisnički programi omogućili su velikom broju ljudi da brzo i lako savladaju osnovna znanja u vezi sa korišćenjem mnogobrojnih servisa na Internetu. Nažalost uz savladavanje osnovnih tehnika korišćenja računarskih mreže obično ne ide i upoznavanje sa opasnostima koje korišćenje novih tehnologija donosi. Prosečan korisnik obično ne razmišlja o posledicama koje mogu nastupiti neopreznim korišćenjem računarskih mreža, a posebno je to izraženo kod najmlađih korisnika računarskih mreža. Zbog toga oni postaju potencijalne žrtve iskusnih i mnogo bolje edukovanih pojedinaca sa nečasnim namerama.² Korišćenje računarskih mreža od strane maloletnih lica danas je uobičajena praksa. Oni koriste Internet najčešće da bi igrali igrice, da bi koristili društvene mreže kao što je Fejsbuk i time održavali kontakte, razmenjivali slike, muziku i video fajlove ili da bi na drugi način komunicirali sa ostalim korisnicima Interneta. Društvene mreže imaju velike zasluge kada je u pitanju povezivanje ljudi iz celog sveta. Deca se mogu povezivati sa prijateljima i porodicom koji žive daleko. Imajući pristup velikom broju edukativnih materijala mogu da uče i da se razvijaju, da vide različite delove sveta i druge kulture koje možda nikada neće imati prilike da vide. U poslednje vreme, s obzirom da su društvene mreže postale i deo društvenog života, kreirajući jedan novi tzv. virtuelni svet, sve je veći broj aktivnosti u okviru kojih su maloletnici žrtve ili počinioci krivičnih dela sajber kriminala upravo posredstvom društvenih mreža (Fejsbuk, Instagram, Pinterest, Tumblr, Twiter, LinkedIn, Majspejs).

Tabela 2. Statistika upotrebe interneta u Srbiji³

Republika Srbija - 7,209,764 populacija (2014)
Glavni grad: Beograd - populacija 1,764,650 (2007)
4,107,000 Internet korisnika 13.Decembra, 57.0 % penetracija (predstavlja broj internet korisnika jedne zemlje podeljen sa ukupnim brojem stanovnika iste), prema IWS.
3,377,340 Fejsbuk korisnika 31.Decembra, 46.8% procena penetracije.
11.91 Mbps Prosečna brzina preuzimanja (download) u martu 2015.g., prema Net Index ⁴

Često realni svet maloletnici zamenjuju sa virtuelnim svetom provodeći veliki broj sati pored računara deleći informacije, fotografije, poruke sa poznatim, a često i sa potpuno nepoznatim novim virtuelnim "prijateljima".

Razvoj novih informacionih tehnologija otvorio je vrata neslućenim, ali je doneo i mnogobrojne probleme uključujući i razne vrste zloupotreba i nanošenja štete pojedincima ili institucijama.

¹ Miniwatts Marketing Group, InternetWorldStats - statistika je bazirana na osnovu obuhvaćenih 3,035,749,340 Internet korisnika, www.internetworldstats.com/stats.htm, 22. 03. 2015.

² D. Prlja, M. Reljanović, *Pravna informatika*, Beograd 2014, 91.

³ Internetworldstats.com, <http://www.internetworldstats.com/europa2.htm>, 21.03.2015.

⁴ Netindex, <http://explorer.netindex.com/maps?country=Serbia>, 21.03.2015.

POJAM SAJBER KRIMINALA

Sajber kriminal nastaje istovremeno sa nastankom sajber prostora, odnosno sa razvojem Interneta kao globalne računarske mreže. Čim je devedesetih godina prošlog veka globalna računarska mreža povezala milione računara sa svih krajeva sveta došlo je do neverovatnog razvoja komunikacija i elektronskog poslovanja pa su se odmah potom pojavili i oni koji su želeli da zloupotrebe mogućnosti koje im virtuelni prostor pruža. Oni koji su i do tada činili krivična dela u realnom svetu nastojali su da svoje aktivnosti prenesu i u sajber prostor, ali nažalost i veliki broj onih koji se nisu do tada bavili izvršenjem krivičnih dela počeli su da ih vrše u sajber prostoru.

Termin sajber kriminal nije opšte prihvaćen, naprotiv danas postoji veliki broj termina kojima se pokušava definisati pojam sajber kriminala: kompjuterski kriminal, visokotehnološki kriminal, elektronski kriminal, računarski kriminal, digitalni kriminal, mrežni kriminal, kriminal elektronskih komunikacija, informaciono tehnološki kriminal, kibernetički kriminal, sajber kriminal, itd. Nećemo se ovom prilikom upuštati u raspravu o tome koji od ovih termina je najadekvatniji već ćemo za potrebe ovog rada koristiti termin "sajber kriminal" iz razloga što je on kao takav korišćen u Konvenciji Saveta Evrope o sajber kriminalu, donetoj 2001.g., a koju je prihvatilo 52 zemlje među kojima i Srbija.

Kada bi trebalo odrediti suštinu i značenje termina sajber kriminala to ni malo ne bi bilo lako iz razloga što postoji ogroman broj definicija sajber kriminala i veliki broj međunarodnih i nacionalnih dokumenata koji nastoje da definišu pojam sajber kriminala. Sve te definicije možemo svrstati u dve kategorije. Prvu kategoriju predstavljaju one definicije koje pokušavaju da odrede opšti pojam sajber kriminala, a drugu kategoriju predstavljaju definicije koje se služe metodom nabiranja dela koje se smatraju sajber kriminalom. U prvu kategoriju mogli bi svrstati definiciju sajber kriminala kao svakog nezakonitog ponašanja u sajber prostoru. Ovakva definicija je tačna, ali previše široka i nedovoljno precizna. Iz tog razloga opredelićemo se da definišemo sajber kriminal nabiranjem dela koje se smatraju sajber kriminalom. Ta dela ćemo svrstati u nekoliko kategorija:

- konvencionalni kriminal koji koristi informatička sredstva i sajber prostor kao podršku za nezakonite aktivnosti (trgovina drogom, oružjem, ljudima, ljudskim organima, itd);
- proizvodnja i širenje štetnog softvera (destruktivni virusi, trojanci, crvi ili adware/spyware programi);
- sajber piraterija (muzika, filmovi, softver, itd.);
- sajber prevare (plišing, spufing, spemovanje, krađa identiteta, finansijske prevare, elektronsko pranje novca, utaja poreza, transfer novca, akademske prevare od strane studenata i naučnika, varanje u školi, na fakultetima, na ispitima, nezakonito kockanje, krađe telefonskih usluga, prevarne Internet aukcije, nigerijske prevare, prevare kod ličnog plaćanja, bankarske prevare, prevare putnika, itd.);
- sajber manipulacija - uhođenje i nepristojne ponude najčešće seksualne prirode (slanje neželjenih slika, tekstova, video materijala, trgovina ljudima, proizvodnja pornografskog materijala, itd.);
- sajber provale (neovlašćeno upadanje u računare i mreže, otkrivanje lozinki, špijunaža, presretanje podataka, itd.);

- sajber maltretiranje (zlostavljanje, sramoćenje, šikaniranje, pretnje, klevete, širenje uvredljivog materijala, lažnih informacija, bombardovanje neželjenom poštom, itd.);
- sajber terorizam, sajber ratovanje, sajber vandalizam, i sajber sabotaza (pokušaj da se ostvare verski, politički ili drugi ciljevi širenjem straha ili uništenjem informacione infrastrukture).

Sigurno je da ovaj spisak kategorija nije konačan, jer se svakoga dana pojavljuju novi oblici zloupotrebe sajber prostora pa ga naravno treba proširivati u skladu sa razvojem situacije u sajber prostoru. Ovakav spisak kategorija sajber kriminala može pomoći u shvatanju obima i broja različitih ponašanja u sajber prostoru koja su protivna zakonskim propisima, a često se dešava da su ta ponašanja počinitelja sajber kriminala često mešovita, odnosno mogu obuhvatiti aktivnosti koje pripadaju većem broju različitih kategorija.

POJAM MALOLETNOG LICA

Za potrebe ovog rada definisaćemo maloletna lica na uobičajen način kao lica koja su u vreme izvršenja krivičnog dela navršila 14 godina života, a nisu navršila 18 godina života. Lica koja u vreme izvršenja krivičnog dela još uvek nisu navršila 14 godina života smatraju se decom, dok lica koja su u vreme izvršenja krivičnog dela napunila 18 godina života smatraju se punoletnim licima. Naravno pojam maloletnog lica nije isto definisan u svim nacionalnim zakonodavstvima, pa se punoletstvo u nekim zemljama stiže tek sa navršenom 21 godinom života, kao što je to slučaj u SAD. Naše zakonodavstvo prihvatilo je uobičajen način definisanja maloletnog lica uz određenje da se punoletstvo stiže sa navršavanjem 18 godina života. To možemo konstatovati na osnovu odredbi Krivičnog zakonika Srbije, Zakona o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica, Porodičnog zakona, itd.

Maloletna lica se mogu podeliti u dve kategorije: mlađi maloletnici i stariji maloletnici. Mlađim maloletnicima se smatraju lica sa navršenih 14 godina života koja nisu navršila 16 godina života, a starijim maloletnicima se smatraju lica sa navršenih 16 godina života koja nisu navršila 18 godina života.

Određivanje pojma maloletnih lica od izuzetnog je značaja za sprovođenje postupka u krivičnim stvarima gde su učesnici postupka i maloletna lica, bilo kao učinioci krivičnih dela, bilo kao žrtve krivičnih dela. Naravno krivičnopravna procedura koja se odnosi na maloletna lica definisana je Zakonikom o krivičnom postupku, Zakonom o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica, Zakonom o izvršenju krivičnih sankcija, i drugim propisima i predviđa posebne oblike zaštite ovih lica u krivičnopravnim postupcima. U ovim postupcima učestvuju i posebni organi koji treba da štite interese maloletnih lica, kao što je to javni tužilac za maloletnike, organ starateljstva, Centar za socijalni rad, sudija za maloletnike, veće za maloletnike itd. U celom krivičnom postupku u kome učestvuju maloletna lica neophodno je voditi računa o uzrastu i duševnoj razvijenosti maloletnog lica i po pravilu javnost je isključena iz postupka, postupak je hitan, a sve u interesu zaštite maloletnih lica.

Zakonodavna regulativa sajber kriminala u Srbiji

Veliki je broj pravnih propisa koji na neki način regulišu i problematiku vezanu za izvršenje krivičnih dela sajber kriminala. Najvažniji među njima su sledeći propisi: Krivični

zakonik – Službeni glasnik RS 85/2005, 88/2005, i 107/2005, Zakonik o krivičnom postupku – Službeni glasnik RS 72/2011, 101/2011, 121/2011, 32/2013, 45/2013., Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala – Službeni glasnik RS 61/2005 i 104/2009, Zakon o organizaciji i nadležnosti državnih organa u suzbijanju organizovanog kriminala, korupcije i drugih posebno teških krivičnih dela, Zakon o autorskim i srodnim pravima, Zakon o zaštiti podataka o ličnosti, Zakon o oglašavanju, Zakon o tajnosti podataka, Zakon o digitalnom potpisu, Zakon o elektronskoj trgovini, Zakon o elektronskom dokumentu, Zakon o tužilaštvu, Zakon o uređenju sudova, Zakon o policiji, itd.

Kada su u pitanju maloletna lica postoji veći set zakonskih propisa koji regulišu pojedine aspekta sajber kriminala u kome mogu učestvovati kao učinioци ili kao žrtve. Neki od tih propisa su: Zakon o posebnim merama za sprečavanje vršenja krivičnih dela protiv polne slobode prema maloletnim licima – Službeni glasnik RS, 32/2013, Zakon o potvrđivanju Konvencije Saveta Evrope o zaštiti dece od seksualnog iskorištavanja i seksualnog zlostavljanja – Službeni glasnik RS – međunarodni ugovori, 1/2010. Zakon o maloletnim učinioциma krivičnih dela i krivičnopravnoj zaštiti maloletnih lica – Službeni glasnik RS 85/2005, Pravilnik o protokolu postupanja u ustanovi u odgovoru na nasilje, zlostavljanje i zanemarivanje – Službeni glasnik RS, 30/2010 u okviru koga je definisano i elektronsko nasilje i zlostavljanje kao zloupotreba informacionih tehnologija koja može da ima za posledicu povredu druge ličnosti i ugrožavanje dostojanstva, a ostvaruje se slanjem poruka elektronskom poštom, SMS-om, MMS-om, putem veb sajta, četovanjem, uključivanjem u forume, društvene mreže i sl.

OBLICI SAJBER KRIMINALA U KOME UČESTVUJU MALOLETNA LICA

Maloletna lica, kod nas kao i svuda u svetu, učestvuju kao učinioци ili kao žrtve u velikom broju krivičnih dela sajber kriminala. Oni najčešće nezakonito preuzimaju softver, muziku ili druge datoteke, šire viruse i upadaju u računare i računarske sisteme, maltretiraju i plaše druga maloletna lica, postaju žrtve sajber prevare, sajber maltretiranja, sajber manipulacije, i konvencionalnog kriminala koji koristi informacione tehnologije i sajber prostor za praćenje potencijalnih žrtvi i stupanje u kontakt sa njima sa ciljem izvršenja nekih od krivičnih dela kao što su na primer trgovina ljudima, ili silovanje.

Odeljenje za borbu protiv visokotehnološkog kriminala u Srbiji je od 2009 do 31. januara 2014.g. dobilo 1345 krivičnih prijava protiv 1270 lica za razna krivična dela sajber kriminala.⁵ Od 2006. do 2014.g. Odeljenje za borbu protiv visokotehnološkog kriminala Službe za borbu protiv organizovanog kriminala Ministarstva unutrašnjih poslova RS i Odeljenje za borbu protiv visokotehnološkog kriminala Višeg javnog tužilaštva u Beogradu podneli su 156 krivičnih prijava protiv 168 lica koja su izvršila krivično delo prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju (čl. 185 Krivičnog zakonika RS), iskorišćavanje računarske mreže i komunikacije drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu (čl. 185b Krivičnog zakonika RS). U najvećem broju slučajeva radilo se o distribuciji inkriminisanog materijala putem Interneta, a zanimljivo je da su svi počinioci bili muškarci.⁶

⁵ V. Urošević, *Veze sajber kriminala sa iregularnom migracijom i trgovinom ljudima*, Beograd: Ministarstvo unutrašnjih poslova Republike Srbije, Beograd 2014., 243.

⁶ *Ibid.*, 289.

Odeljenja koja se bore protiv visokotehnološkog kriminala podnela su do 2014. godine 25 krivičnih prijava protiv lica koja su izvršila delo ugrožavanje sigurnosti (čl. 138 Krivičnog zakonika RS), uglavnom preko Internet sajtova, Fejsbuka i elektronskih poruka. Izvršioci su upućivali poruke čija sadržina predstavlja ozbiljnu pretnju pojedincima ili grupama.⁷

Konvencionalni kriminal u sajber prostoru putem društvenih mreža

Konvencionalni kriminal koristi sve češće sajber prostor kao podršku za izvršenje krivičnih dela putem informatičkih sredstva kao što su npr. Fejbuk i ostale društvene mreže. Gotova da nema konvencionalnog krivičnog dela koje se ne može u nekom segmentu pripremiti uz pomoć informacionih tehnologija i sajber prostora. Praćenje i upoznavanje navika budućih žrtava radi ubistva, trgovine ljudima, trgovine ljudskim organima često se izvodi i u sajber prostoru. Konvencionalna krivična dela trgovine drogom, trgovine oružjem, i mnoga druga krivična dela u nekom aspektima pripremaju se ili čak izvode korišćenjem sajber prostora.

Uz pomoć digitalno forenzičke istrage uočen je novi trend koji je u vezi sa nedozvoljenim aktivnostima, a to je prikupljanje informacija sa društvenih mreža u smislu pripremnih radnji za neka kasnija krivična dela u vidu sajber praćenja (eng. cyber tracking). Dok se tradicionalno praćenje može izraziti kroz fizičko praćenje, sajber praćenje podrazumeva prikupljanje korisničkih podataka i na osnovu ostavljenih slika, komentara, navika, može se pratiti kretanje određene osobe. Pogotovu je data mining olakšan uvođenjem servisa za prepoznavanje lica. Postoje slučajevi u praksi kada su otmice vršene na osnovu skeniranja društvenih mreže u potrazi za potencijalnim žrtvama⁸. Najnoviji slučaj planiranja otmice M. P. uz pomoć Fejsbuka doprinosi utisku da su društvene mreže upravo doprinele ciljanom odabiru žrtve⁹.

U Holandiji u mestu Arnheim je jedna petnaestogodišnja devojčica ubijena, pošto je putem Fejsbuka širila loše vesti o svojoj drugarici. Petnaestogodišnji dečak je izvršio ubistvo devojčice po nalogu dva mladića i uvređene devojčice, koji su mu za ubistvo platili 100 evra. Sve je počelo putem Fejsbuka gde je nesrećna devojčica napisala, da je njena drugarica imala seksualne odnose sa više mladića. Zbog ovih objava je njena drugarica htela da joj se osveti. Zajedno sa svojim drugarima je planirala ubistvo i za to platila 100 evra.¹⁰ Ubistvo je izvršeno ubodima u lice i vrat. Ubica je osuđen na godinu dana zatvora, što je najveća kazna za maloletnike u Holandiji i prinudno psihijatrijsko lečenje.¹¹ Otac ubijene devojčice je bio zgrožen ovako niskom kaznom za ubistvo i istakao da je on izgubio svoju ćerku, a da će ubica u zatvoru provesti svega godinu dana.¹² Apelovao je na političare da pooštre kazne za ovakve slučajeve. Opasnosti koje nose sa sobom društvene mreže i čet portalima se često podcenjuju istakao je otac ubijene devojčice. Na suđenje čekaju još uvek devojčica koja je dala nalog za ubistvo i još jedan mladić.

⁷ Ibid., 291.

⁸ Kidnappers Scanning Social Networks For Potential Victims, *technology.inquirer.net/ 39521/kidnappers-scanning-social-networks-for-potential-victims-pnp*, 06.04.2015.

⁹ Opasnost društvenih mreža: otmičari Mašu vidjeli na Facebooku!, *poskok.info/wp/?p=137427*, 06.04.2015.

¹⁰ Godinu dana zatvora za maloletnog "Fejsbuk ubicu" u Holandiji, *www.blic.rs/ Vesti/Svet/340972/Godinu-dana-zatvora-za-maloletnog-Fejsbuk-ubicu-u-Holandiji*, 11.08.2013.

¹¹ Mord an 15-Jähriger wegen Facebook-Postings, *www.heute.at/news/welt/art23661,771005*, 11.08.2013.

¹² Höchststrafe für "Facebook-Mörder", *www.heute.at/news/multimedia/art 23657,779686*, 11.08.2013.

U Holandiji se dogodio još jedan slučaj u kome je izvršilac krivičnog dela četrnaestogosišnja tinejdžerka, koja je pretila putem Tvitera kompaniji American Airlines. Nakon toga je American Airlines obavestio FBI i holandsku novinsku agenciju ANP a potom je policija i ona je uhapšena. Devojčica je na svom twitter profilu napisala "Čao, moje ime je Ibrahim i ja sam iz Afganistana. Član sam Al Kaide i 1. Juna napraviću nešto veliko." Aviokompanija reagovala je munjevito i shvatila ozbiljno ovu pretnju, pa je obavestila devojčicu da će njena IP-adresa biti prosleđena nadležnim organima. Njen profil na Tviteru @QueenDemetriax_ bio je blokiran a njeni tweetovi obrisani od strane ove društvene mreže. Predhodno je devojčica objasnila da ona nije ozbiljno ovo mislila i da je sve bila šala. Osim toga bilo joj je veoma žao i izjavila je takođe "Ja imam samo 14 godina, da li vi ozbiljno mislite, da ja jedan avion mogu da dignem u vazduh?".¹³

Obrenovačka policija 2009.g. uhapsila je A.N. (43) zbog sumnje da je M. M. (13) iz Obrenovca primorao na seksualni odnos. Prethodno su se upoznali preko Fejsbuka gde se on predstavio kao sedamnaestogodišnji Filip 007. A.N. je tokom dopisivanja devojčici prvo predložio da imaju seksualne odnose, a kada je to odbila, insistirao je da se sretnu i da na sastanak dođe sama. Odveo ju je u šumarak u blizini Obrenovca. Snimak seksualnog odnosa policija je pronašla u telefonu A.K.¹⁴

Niška policija je 2010. godine uspeła je da spreči masovnu tuču osnovaca u naselju Pantelej, koja je bila najavljena i organizovana na Fejsbuku. Rukovodilac grupe za suzbijanje maloletničke delinkvencije u niškoj policiji Bratislav Timotijević izjavio je da će ubuduće operativci ove službe motriti dešavanja na Fejsbuku.¹⁵

U Holandiji u gradiću Harenu se takođe desio slučaj gde je jedna 16 godišnja devojka pogrešnim klikom pozvala više od 30.000 ljudi na svoju rođendansku proslavu. Planiran je poziv za uži krug prijatelja. Toliki broj poziva usledio je jer su prijatelji obavestavali prijatelje o žurki, oni dalje svoje prijatelje, pa je tako došlo do ogromnog broja zvanica. Naravno i ovaj slučaj se desio zbog klika na javnu žurku. Pored toga nekoliko veb sajtova je pozvalo na žurku i doprinelo većem broju zvanica, a na jednom je stajalo "Projekat X Haren" i odbrojavalo se vreme do početka žurke uz navode da je pozvano 150.000 ljudi. Na istom veb sajtu je objavljena i adresa na kojoj je proslava, uz napomenu "Gledajte kako umete da sa sobom povedete i prijatelje".¹⁶ U Haren, gradić sa oko 18.000 stanovnika, došlo 4.000 gostiju. Tom prilikom intervenisala je i policija, a kada je pokušala da otera goste, zasuta je bila kamenicama, flašama, biciklima i saksijama za cveće. U centru grada su uništavani parkirani automobili, ulično osvetljenje, saobraćajni znaci, ograde od dvorišta privatnih kuća, kiosci i lokali. Bilans je da je 30 ljudi povređeno, od toga dvoje teško, a uhapšene su četiri osobe, a 500 pripadnika policije bilo je angažovano u intervenciji.¹⁷ Šteta je procenjena na milion evra.¹⁸

¹³ Teenager wegen Twitter-Drohung gegen Airline festgenommen, <http://futurezone.at/digital-life/teenager-wegen-twitter-drohung-gegen-airline-festgenommen/60.747.683>, 16.04.2015

¹⁴ M. Vidić, Mračna strana Fejsbuka, www.vreme.com/cms/view.php?id=929661, 03.04.2015.

¹⁵ M. Vidić, Mračna strana Fejsbuka, www.vreme.com/cms/view.php?id=929661, 06.04.2015.

¹⁶ Preko "Fejsbuka" greškom pozvala 4.000 gostiju na žurku, www.blic.rs/Slobodno-vreme/Zanimljivosti/344023/Preko-Fejsbuka-greskom-pozvala-4000-gostiju-na-zurku, 30.07.2013.

¹⁷ Facebook-Party endete mit Polizeieinsatz, futurezone.at/digitallife/11478-facebook-party-endete-mit-polizeieinsatz.php, 30.07.2013.

¹⁸ 1 Million Euro Schaden nach Facebook-Party, www.heute.at/news/welt/art23661%2c791737, 30.07.2013.

Sajber manipulacija i seksualno iskorištavanje maloletnika

Sajber manipulacija je vrsta psihološke manipulacije koja se obavlja na Internetu preko sinhronih i asinhronih komunikacionih platformi (javne čet pričaonice, Internet sajтови za upoznavanje, instant mesindžeri i VOIP servisi tipa ICQ i Skajp) i u novije vreme putem društvenih mreža (Fejsbuka, *Instagrama*, *Pinteresta*, *Tumblr*a, *Twitera*, *LinkedIna*). Žrtve manipulacije su uglavnom deca tj. maloletna lica od 11 do 17 godina i kao krajnji cilj ove manipulacije je sastanak koji se obično pretvara u seksualno zlostavljanje, fizičko nasilje, dečiju prostituciju i pornografiju.¹⁹

Prva stvar koju maloletna lica urade kada dobiju računar i pristup Internetu je da otvore profil na društvenoj mreži Fejsbuk. To im omogućava da se virtuelno druže sa svojim vršnjacima iz škole i neposrednog okruženja, da igraju igrice, da časkaju sa prijateljima, da razmenjuju fotografije i video snimke, da pripadaju virtuelnim interesnim grupama i povezuju se sa onima koji vole istu muzičku grupu ili isti sportski klub, mogu da razmenjuju linkove, viceve i razne druge zabavne sadržaje. Nažalost kada su u pitanju virtuelni prijatelji na Fejbuku nije uvek lako utvrditi ko je zaista vaš virtuelni prijatelj. Stavljanjem tuđe slike i prikazivanjem lažnih podataka o starosti ili pola vrlo lako odrasla osoba postaje maloletnik u želji da lažnim predstavljanjem zadobije poverenje neke osobe, kako bi sa njom stupila u kontakt sa namerom izvršenja krivičnog dela. Ovakvih slučajeva je već bilo i u Srbiji. Najčešći slučajevi lažnog predstavljanja na internetu vezani su za pedofiliju (seksualnu sklonost odraslih prema deci istog ili suprotnog pola). Pedofili su postojali i pre nastanka Interneta, ali im je sada drastično povećana i olakšana mogućnost stupanja u kontakt sa decom preko Fejsbuka i drugih društvenih mreža. Obično se lažno predstavljaju kao vršnjaci dece i stupaju u kontakt sa njima putem četa zadobijajući njihovo poverenje pribavljaju informacije o mestu stanovanja, školi, roditeljima, itd, pokušavaju da zakažu sastanak nudeći novac ili neke druge protivusluge. Pedofili često deci šalju pornografski materijal i nagovaraju decu da sama prave i pošalju im pornografski materijal na osnovu koja ih kasnije ucenjuju.

Određeni Internet sajтови i društvene mreže su takođe postale i *sredstvo za promovisanje maloletničke prostitucije*^{20 21 22}. S obzirom da je za izvođenje ovakve protivpravne aktivnosti dovoljan računar i veb kamera, nije ni čudo što je to postao problem svetskih razmera.

Rezultati istraživanja i studije MUP-a RS o sajber kriminalu, koja sadrže komparativnu analizu stanja u literaturi, praksi, zakonodavstvu, terminologiji i učiniocima, ukazuju da su potrebne dodatne zakonske izmene u vezi sa primenom Konvencije SE, ali i radi usklađivanja sa Deklaracijom o globalnoj alijansi protiv

¹⁹ K. Kopecký, Cyber grooming danger of cyberspace, study, www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=15%3Acybergrooming-danger-of-internet, 22.11.2011.

²⁰ Učenice zarađuju web pornografijom, www.vesti.rs/Novi-Sad/Ucenice-zaradjuju-web-pornografijom.html, 07.04.2015.

²¹ Devojčice iz Srbije uvučene u veb prostituciju, www.dw.de/devoj%C4%8Dice-iz-srbije-uvu%C4%8Dene-u-veb-prostituciju/a-14878354, 06.04.2015.

²² Maloletnička prostitucija sve prisutnija, www.novosti.rs/vesti/beograd.74.html:350432-Beograd-Maloletnicka-prostitucija-sve-prisutnija, 06.04.2015.

seksualne zloupotrebe dece onlajn,²³ koja je pokrenuta 2012. g. na inicijativu EU i SAD, a kojoj se priključila Srbija i još pedesetak zemalja.²⁴

Maloletna lica su pripadnici različitih socijalnih slojeva, a motivi su u većini slučajeva materijalno orijentisani. Jedan od primera ističe se od strane konsultanta za bezbednost elektronski sistema Aleksandra Arsenina: nisu uopšte retki sajtovi koji potpuno legalno naplaćuju svoje usluge i plaćaju svoje, grubo rečeno, striptizete, koje se putem Interneta svlače i pružaju tu vrstu usluga. Ono što je najviše poražavajuće u celoj priči jeste da su to uglavnom deca od 12 do 25 godina starosti. Za pedesetak evra mesečno spremne su da izvode kućni striptiz pred veb kamerama i da to plasiraju dalje na sajtove. Ti sajtovi skupo naplaćuju svoje usluge, a materijal kasnije distribuiraju preko CD-ova dalje u inostranstvo. Jedan CD sa takvim "autorskim" materijalom košta od 500 pa do 1.000 evra. Ove devojčice neretko završavaju u začaranom krugu ucene, nakon čega iz straha nastavljaju da se bave veb prostitucijom.²⁵

U policijskoj akciji "Armagedon" u nekoliko gradova Srbije uhapšeno je više desetina osoba kod kojih su pronađene fotografije i video-zapisi sa dečijom pornografijom i zaplenjeno je više od 4.000 DVD-ova na kojima se nalaze snimci iskorišćavanja i seksualnog zlostavljanja dece.²⁶

Saša Živanović, načelnik Odeljenja za visokotehnoški kriminal MUP-a Srbije, kaže da bi osnivači stranica sličnih skandaloznoj Fejsbuk grupi "Najveće drolje osnovnih i srednjih škola" mogli da odgovaraju za podstrekivanje na izvršenje krivičnog dela prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju. Nakon otkrivanja skandalozne Fejsbuk grupe "Najveće drolje osnovnih i srednjih škola"²⁷ na kojoj su objavljene provokativne obnažene fotografije maloletnih devojčica iz zemalja u regionu krije maloletni Renato E. iz Hrvatske²⁸, stigla je reakcija nadležnih iz Odeljenja za visokotehnoški kriminal MUP-a Srbije²⁹.

Ukoliko se utvrdi da ne postoje fotografije potpuno nagih maloletnih lica na osnovu nepristojnog i uvredljivih imena ove grupe na društvenoj mreži ne može se govoriti o krivičnom gonjenju. Međutim osnivač ovakve grupe bi mogao da odgovara za podstrekivanje na izvršenje krivičnog dela – prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju.

S obzirom na to da su se u međuvremenu na društvenim mrežama pojavile nove grupe identične sadržine, postavlja se pitanje kolike su kazne propisane u Srbiji za izvršenje krivičnog dela "prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju", i da li su one dovoljne za sprečavanje ovakvog vida zloupotrebe maloletnih lica.

²³ Global Alliance Against Child Abuse, ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/index_en.htm, 09.04.2015.

²⁴ Od piratskog raja do puta u EU, Sat, www.seecult.org/vest/od-piratskog-raja-do-puta-u-eu, 04.04.2015.

²⁵ Devojčice iz Srbije uvučene u veb prostituciju, www.dw.de/devoj%C4%8Dice-iz-srbije-u-vu%C4%8Dene-u-veb-prostituciju/a-14878354, 06.04.2015.

²⁶ Ibid.

²⁷ Pedofilski raj: skupili 40.000 lajkova na polugolim devojčicama, www.telegraf.rs/vesti/1038275-pedofilski-raj-skupili-40-000-lajkova-na-polugolim-devoj%C4%8Dicama-niko-ne-reaguje-foto, 04.04.2015.

²⁸ Telegraf otkrio ko stoji izapedofilske grupe, www.telegraf.rs/vesti/1039302-ekskluzivno-telegraf-otkrio-ko-stoji-iza-pedofilske-grupe-na-fejsbuku-foto, 05.04.2015.

²⁹ Osnivač pedofilske grupe na fejsbuku može dobiti 8 godina zatvora, <http://www.telegraf.rs/vesti/1040429-istradjemo-osniva%C4%8C-pedofilske-grupe-na-fejsbuku-mo%C5%BE-dobiti-8-godina-zatvora>, 05.04.2015.

Prema članu 185 Krivičnog zakonika Republike Srbije, onaj ko maloletniku proda, prikaže ili javnim izlaganjem ili na drugi način učini dostupnim tekstove, slike, audio-vizuelne ili druge predmete pornografske sadržine ili mu prikaže pornografsku predstavu, kazniće se novčanom kaznom ili zatvorom do šest meseci. Ko iskoristi maloletnika za proizvodnju slika, audio-vizuelnih ili drugih predmeta pornografske sadržine ili za pornografsku predstavu, kazniće se zatvorom od šest meseci do pet godina. Ako je pomenuto delo izvršeno prema detetu, učinilac će se kazniti za delo iz stava 1. zatvorom od šest meseci do tri godine, a za delo iz stava 2. zatvorom od jedne do osam godina. Pritom, onaj ko pribavlja za sebe ili drugog, poseduje, prodaje, prikazuje, javno izlaže ili elektronski ili na drugi način čini dostupnim slike, audio-vizuelne ili druge predmete pornografske sadržine nastale iskorišćavanjem maloletnog lica, kazniće se zatvorom od tri meseca do tri godine.

Nisu retki *slučajevi vrbovanja maloletnika radi seksualnog iskorištavanja* preko društvenih mreža. Ovo potvrđuje i slučaj Banjalučanina S. V. (34) koji je uhapšen 2013.g. zbog vrbovanja maloletnice uz pomoć Interneta i društvene mreže "Fejsbuk", a inspektori za "sajber kriminal" MUP-a RS uhapsili su ga zbog sumnje da je ugrozio bezbednost 12-godišnje devojčice, koju je vrbovao.³⁰

Imali smo slučaj da jedan pristojan Beograđanin, inženjer, otac dvoje dece, porodični čovek, zlostavlja devojčicu, svoju komšinicu šest meseci, kreirani video materijal nakon toga prodaje putem Interneta, potom je osuđen na četiri godine zatvora i onda nakon dobrog vladanja je pušten ranije.³¹

Evropski centar za sajber kriminal trenutno podržava 9 velikih policijskih operacija protiv seksualnog iskorišćavanja dece u okviru Evropske unije. Prve godine rada Evropski centar za sajber kriminal učinio je značajan napor, zajedno sa mnogim državama članicama i partnerima za saradnju koji ne pripadaju EU, u borbu protiv ilegalnih aktivnosti pedofila umešanih u onlajn seksualno iskorišćavanje dece uz pomoć skrivenih usluga. Evropski centar za sajber kriminal je uključen u mnoge operacije i zajedničke istrage usmerene na proizvodnju i distribuciju materijala sa zlostavljanjem dece na različitim Internet stranicama. Centar pruža operativnu i analitičku podršku u istragama o trgovanju nedozvoljenim materijalom sa zlostavljanjem dece na skrivenim forumima, kao i istragama o "seksualnom iznuđivanju". Seksualno iznuđivanje je termin kojim nazivamo pojavu gde zlostavljači dece dobijaju pristup neprikladnim slikama maloletnika i koriste te slike da primoraju žrtve na dalje radnje ili zlostavljač prosleđuje slike porodici ili prijateljima žrtve.³²

Zloupotreba tuđih fotografija i postavljanje fotografija bez znanja vlasnika pod punim imenom i prezimenom na društvenim mrežama takođe postaje jedan od širećih problema.

U akciji "Armagedon" otkriveno je šest osoba koje se sumnjiče za prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnika za pornografiju. Četvorica muškaraca su uhapšena, ali će protiv svih šestoro biti podnete krivične prijave. Policija je, u koordinaciji sa Tužilaštvom za visokotehnološki kriminal, a po

³⁰ Banjalučanin uhapšen zbog vrbovanja maloletnice, www.pressrs.ba/sr/vesti/hronika/story/42371/Banjalu%C4%8Danin+uhap%C5%A1en+zbog+vrbovanja+maloletnice.html, 03.04.2015.

³¹ *Ibid.*

³² Evropski centar za sajber kriminal: godinu dana rada, www.kick-me.co/evropski-centar-za-sajber-kriminal-godinu-dana-rada/, 23.03.2015.

nalogu sudije za prethodni postupak Višeg suda u Beogradu nakon pretresa pronašla veliku količinu elektronskog materijala sa seksualnim zlostavljanjem dece i maloletnika. Prema zvaničnom saopštenju osumnjičeni su to preuzimali sa Interneta i skladištili u svoje računare i na memorijske kartice svojih telefona. Uhapšeni B. B. je godinama radio kao nastavnik u osnovnoj školi, ali je svojevremeno izbačen zbog maltretiranja učenika. B. B. se predstavljao kao radnik modne agencije i tako vrbovao devojčice da mu šalju slike. Na njegovo insistiranje dve maloletnice su mu poslale obnažene fotografije, posle čega je on počeo da ih ucenjuje istaknuto je u saopštenju MUP-a.³³

Devojčice od 13 do 14 godina koje se za popularnost bore golišavim fotografijama po društvenim mrežama tokom 2015.g. saslušane su u MUP-u RS. Tužilaštvo za visokotehnoški kriminal je posle pisanja "Blica" o tinejdžerkama koje objavljuju svoje golišave fotografije naložilo hitnu istragu, pa su devojčice, zajedno s roditeljima, morale da odgovore na pitanja koja su im postavljali inspektori MUP-a za visokotehnoški kriminal i pedofiliju. Ovaj trend se širi društvenim mrežama, što potvrđuju i direktori osnovnih škola, kao i sociolozi, koji ističu da su u ovoj priči nemoćni, jer roditelji ne pružaju nikakav otpor deci. Priča će, međutim, dobiti epilog na sudu.³⁴

Tužilaštvo ima "prilično oštar stav" prema posedovanju i razmeni pornografskog materijala sa decom i maloletnim licima, koje je na osnovu Krivičnog zakonika kažnjivo i za koje je predviđena kazna zatvora od 3, 5 i 8 godina u zavisnosti od toga da li je oštećeno lice dete ili maloletnik, i ne dopušta da dođe do sklapanja sporazuma o priznavanju krivice, jer se radi o izuzetno opasnom krivičnom delu.³⁵

I u svetu postoji trend objavljivanja i ucenjivanja iz osвете pornografskih fotografija pre svega maloletnih devojčica (najčešće bivših devojaka) putem društvenih mreža. Stoga su neke zemlje kao Velika Britanija³⁶ i Nemačka³⁷ posebno regulisale ovu problematiku zakonima. U Velikoj Britaniji je nedavno donesena prva presuda zbog objavljivanja pornografskih fotografija u kojoj je osuđen 21-godišnji muškarac. Krivično delo obavljeno je na društvenoj mreži Votsap (WhatsApp), gde su objavljene intimne fotografije bivše devojke. Fotografije su bile dostupne za sve njene kontakte. Prethodno je ovaj momak već pretio bivšoj devojci, koja je kontaktirala policiju. Policija je takođe upozorila mladića, ali upozorenje nije dalo rezultata i krivično delo je izvršeno. Sud je Britanaca i pored priznanja krivičnog dela osudio na 12 meseci zatvora za ovo krivično delo.³⁸

³³ Pedofili vrbovali devojčice preko Interneta!, *www.novosti.rs /vesti/naslovna/ hronika/ aktuelno.291.html:531167-Pedofili-kao-modni-agenti-vrbovali-devojce-preko-interneta*, 05.04.2015.

³⁴ Z. Lazarević, Saslušavaju se golišave devojčice sa Fejsbuka, *www.blic.rs/Vesti/Drustvo/546508/Saslusavaju-se-golisave-devojce-sa-Fejsbuka*, 30. 03.2015.

³⁵ Od piratskog raja do puta u EU, Sat, *www.seecult.org/vest/od-piratskog-raja-do-puta-u-eu*, 04.04.2015.

³⁶ U Engleskoj za ovo krivično delo je zaprećena kazna od 2 godine zatvora. Novi Zakon o pornografskim osvetama stupio je u Februaru 2015. godine na snagu. England verabschiedet Gesetz gegen Rache pornos, *m.futurezone.at/netzpolitik/england-verabschiedet-gesetz-gegen-rachepornos/113.510.541*, 16.4.2015.

³⁷ U Nemačkoj je takođe krajem 2014. godine usvojen Zakon o pornografskim osvetama sa predviđenom maksimalnom kaznom do 2 godine zatvora. U zakonu nije jasno napravljena razlika u odnosu na krivična dela vezana za maloletničku pornografiju. Kritičari stoga tvrde da se na će na ovaj način svako naga fotografija biti proglašena za krivično delo. Stefan Kreml, Bundesrat stimmt für Gesetz gegen unbefugte Nacktbilder, *www. heise. de/ newsticker /meldung/ Bundesrat-stimmt-fuer-Gesetz-gegen-unbefugte-Nacktbilder-2504506.html*, 16.04.2015.

³⁸ Großbritannien: Erste Haftstrafe für Rache pornos verhängt. *m.futurezone.at/digital-life/grossbritannien-erste-haftstrafe-fuer-rachepornos-verhaengt/97.245.160*, 16.04.2015.

Primeri sajber maltretiranja (eng. cyber bullying)

Nasilje među vršnjacima koje je i do sada postojalo u školi i na ulici danas se seli na Internet. Vršnjačko nasilje u virtualnom svetu sastoji se u vređanju žrtve, neovlašćenom slanju fotografija ili video snimaka žrtve, pretnjama žrtvi, podsticanju govora mržnje, insinuiranju ili otvorenoj povredi seksualnosti žrtve. Na Fejsbuku se osnivaju grupe kojima je predmet da mrze nekog pojedinca ili neku grupu. Na Fejsbuku ima hiljade ovakvih grupa. Posledice po decu koja su predmet virtualnog nasilja se pre svega ogledaju u promeni u ponašanju, povlačenju u sebe, dobijanju loših ocena, itd. Psihičke posledice virtualnog nasilja mogu dovesti i do tragičnog ishoda. Virtualno nasilje, sajber zlostavljanje, sajber maltretiranje, sajber zastrašivanje je čak opasnije od onog klasičnog fizičkog nasilja zato što za njega nema granica. Žrtve su ovom nasilju izložene 24h dnevno i posledice su često trajno poremećeno psihološko zdravlje i samopoštovanje pojedinca. Napadi ovog tipa mogu biti toliko intenzivni i ponavljajući, da žrtva može da doživi mentalni slom, a posledice mogu da dovedu i do samoubistva.³⁹ Zabrinjavajući su podaci da je sajber maltretiranje sve više prisutno na društvenim mrežama i da za svoju posledicu može da nosi nepopravljive gubitke. Primeri kao što su: 13-godišnji dečak izvršio samoubistvo nakon što su ga nemilosrdno maltretirali na društvenim mrežama, 18-godišnja devojka se ubila nakon što je njen dečko postavio njene eksplicitne fotografije (namenjenih samo njemu) na društvenim mrežama, 14-godišnja devojka izbačena iz škole nakon što je drugarica napisala na društvenoj mreži da je trudna, postali su sve češći.

U svetu je zabeležen veliki broj slučajeva kada su maloletna lica nakon sajber maltretiranja izvršila samoubistvo. 2006. godine 13. godišnja devojčica Megan Meier iz Misurija, je izvršila samoubistvo nakon sajber maltretiranja na društvenoj mreži Majspejs od strane određene osobe za koju je mislila da je 16. godišnji dečak Josh Evans⁴⁰. 2005 godine 15. godišnji Jeff Johnston Halligan je izvršio samoubistvo nakon nemilosrdnog maltretiranja koja su ga pratila od škole do kuće tj. do njegovog računara. Sve je desilo nakon što mu je jedna "popularna" devojka iz škole postala devojka. Zbog toga je jedan dečak zbog ljubomore odlučio da pošalje okrutne izjave i klevetničke tračeve putem elektronske pošte i veb sajta. Trinaestogodišnji Ryan Halligan je 2003.g. izvršio samoubistvo nakon višemesečnog maltretiranja od strane školskih drugova. Otac John Halligan je potvrdio da je depresija kod njegovog sina nastala uticajem značajnih faktora sredine u vidu fizičkog i sajber maltretiranja.⁴¹

U nekim slučajevima nakon sajber maltretiranja maloletnici su napuštali školu i imali psihičkih problema. 2002. godine, 17. godišnji dečak David Knight, postao je žrtva klevete na jednoj Internet strani, nekoliko meseci. Optuživali su ga da je pedofil, da je homoseksualac, da koristi drogu za obljudu maloletnih dečaka. Tako predstavljen postao je antipatičan svima u školi i posledica je bila njegova izolacija i povučenost kao i napuštanje škole zbog poniženja i sramote koju je doživeo.⁴²

³⁹ V. Krejčí, Kyberšikana kybernetická šikana, www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=14%3Akysbersikana-studie, 22.11.2011

⁴⁰ ABCNEWS, abcnews.go.com/GMA/story?id=3882520, 04.04.2015.

⁴¹ News, www.schuylervilleschools.org/News/14-15/11_25_14_Halligan_Presentation.cfm, 0504.2015.

⁴² J. Leishman, Cyber-bullying, www.njbullying.org/CBCNewsInDepthBullying.htm, 04.04.2015.

Sajber provale - neovlašćen pristup računarima u sajber prostoru

Ova dela se obično realizuju uz pomoć fišinga, farminga, malicioznih programa, ranjivosti bežične mreže (Wi-Fi) kao i uz pomoć socijalnog inženjeringa. Maloletnici u Srbiji više puta su izvršili razne vrste hakerskih napada i neovlašćeno su pristupili tuđim računarima.

Dvojica maloletnika od 16 godina 2015. godine su neovlašćeno pristupili zaštićenom računarima i odatle skinuli podatke. Oni su ranije dostavili spiskove JMBG građana i objavili da "drže Srbiju u šaci" kao i "Imamo gotovo sve podatke o srpskim stanovnicima počevši od JMBG-a pa do toga šta rade, gde žive, brojeva telefona – napisali su u pismu." ^{43 44}

Protiv hakerske grupe "Srpski hakeri" podneta je krivična prijava zbog sumnje da su organizovali hakerske upade u baze podataka, među kojima su i podaci o platnim karticama, da su pribavili bazu jedne političke partije i prosledili je medijima, a glavnom organizatoru određen je pritvor do 30 dana prema saopštenju MUP-a RS. Policija je u njihovim računarima pronašla programe koji koriste hakeri, kao i dokaze za krivično delo za koje su osumnjičeni, kao što su podaci o platnim karticama u elektronskom obliku. Takođe su pronađeni i fajlovi sa korisničkim imenima i šiframa elektronskih naloga za koje se sumnja da pripadaju građanima Srbije. Računarska oprema, koja je služila za izvršenje krivičnog dela privremeno je oduzeta. Takođe su pronađeni i tekstualni fajlovi na kojima su se nalazila korisnička imena i šifre elektronskih naloga za koje postoji sumnja da pripadaju građanima Srbije. ⁴⁵

U svetu je takođe zabeležen veliki broj slučajeva kada su maloletna lica neovlašćeno upadala u računare i računarske mreže raznih institucija. Između avgusta 1999. i oktobra 1999. Jonathan Joseph James, kao maloletnik od 16 godina izvršio je upade na poznate organizacije. Jedna takva meta je bila i Agencija Ministarstva odbrane gde je postavio svoj bekdor (engl. backdoor) koji je omogućio da se vide osetljivi podaci kao što su elektronska pošta, korisnička imena i šifre zaposlenih. Takođe je upao i u NASA računare i ukrao program vredan 1.7 miliona dolara. Kao posledica NASA je bila prinuđena da privremeno isključi svoje računarske sisteme, čime je prouzrokovana velika finansijska šteta.

Sajber prevare i krađa identiteta u sajber prostoru

Broj i vrsta sajber prevara neverovatno je veliki. Ove prevare vezuju se za zahteve za transfer novca, spam, clickjacking⁴⁶ prevare kroz sajtove za upoznavanje. ⁴⁷ Kod ove

⁴³ Uhapšeni tinejdžeri od 16. godina osumnjičeni da su objavljivali zaštićene podatke, www.novosti.rs/vesti/naslovna/drustvo/aktuelno.290.html:528909-Uhapseni-tinejdžeri-od-16-godina-osumnjiceni-da-su-objavljivali-zasticene-podatke, 05.04.2015.

⁴⁴ Pali srpski hakeri: uhapšeni maloletnici koji su objavljivali zaštićene podatke, www.telegraf.rs/vesti/1390610-pali-srpski-hakeri-uhapseni-maloletnici-koja-su-objavljivali-zasticene-podatke, 05.04.2015.

⁴⁵ Privedena dvojica maloletnika zbog hakerisanja, www.politika.rs/rubrike/Hronika/Privedena-dvojica-maloletnika-zbog-hakerisanja.lt.html, 04.04.2015.

⁴⁶ Clickjacking predstavlja tehniku prevare veb korisnika iskorišćavajući neki sigurnosni propust na sistemu ili iskorišćavajući ranjivost nekog veb pretraživača sa ciljem otkrivanja poverljivih informacija ili preuzimanja kontrole nad računarom. To se realizuje tako što korisnik klikne na naizgled bezazlenu stranicu i počinje da se izvršava neki kod ili skripta bez znanja korisnika. Zapravo "dugme" odnosno link koji je bio kliknut počinje da obavlja neku drugu funkciju, a ne onu za koju je korisnik bio obavešten. Na primer, korisnik može da primi mail sa linkom za neki video zapis, ispod koje stoji skrivena druga stranica npr ebay.com. Kada korisnik pokuša da klikne na "play" zapravo

vrste sajber kriminala takođe su često žrtve maloletne lica, a ima i slučajeva kada sama maloletna lica pokušavaju, ili uspevaju da izvrše sajber prevare.

Krađa identiteta predstavlja još jedan oblik visokotehnoškog kriminala koji se manifestuje kroz krađu identiteta druge osobe u kojima zlonamerna osoba pretenduje da se predstavi kao neko drugi u cilju pristupanju resursima od materijalne koristi (npr. kredita) i drugih privilegija u ime te druge osobe. Žrtva krađe identiteta (znači lice čiji identitet pribavlja zlonamerni napadač) može trpeti štetne posledice, ako se smatra odgovornim za postupke počinioaca. Organizacije i pojedinci koji su prevareni na ovakav način od strane lopova, takođe mogu imati štetne posledice i gubitke u istoj meri kao i osobe čiji je identitet kompromitovan.

ZAKLJUČAK

Jedan od ciljeva ovog rada jeste i da ukaže na opasnosti koje mogu da proisteknu od neadekvatnog korišćenja Interneta i posebno društvenih mreža. Najčešće maloletna lica sama omogućavaju nesvesnim postupcima izvršenje krivičnih dela. Potrebno je istaći da se edukovanjem korisnika i prevencijom u vezi sa upotrebom društvenih mreža mogu smanjiti opasnosti po korisnike naročito maloletna lica. Za povećanje bezbednosti maloletnih lica na Internetu potrebno je vršiti edukaciju dece od strane roditelja, u školama, od strane nastavnika i uz pomoć medija i sredstava javnog informisanja, u smislu prisutnosti informacija o bezbednom korišćenju Interneta naročito društvenih mreža.

Država može i treba da uvede programe i obavezne predmete još od osnovne škole, kojima bi pored dece bili uključeni i roditelji. Roditelji zaostaju u ovoj oblasti, pošto tehnologija konstantno napreduje. Osim toga, moguće je uvesti i znakove upozorenja slično saobraćajnim znakovima na osnovu kojih bi i roditelji i deca bili upozoreni na opasnost od određenog računarskog krivičnog dela. Garancija i sertifikacija kvaliteta bila bi, takođe, jedna od mera, koju bi država mogla da preduzme, a na taj način bi deca znala da je određena firma, institucija ispoštovala određene standarde zaštite.

O bilo kom tipu sajber kriminala da je reč, moraju se pronaći odgovori na pitanja ko je izvršio zabranjenu radnju, kada se to desilo i kako, zašto je delo učinjeno, gde je mesto, šta je bio cilj, a na tužilaštvu je dalje da uz sve to dokaže i uzročno-posledičnu vezu između dela i učinioca kao i nameru da se to delo izvrši (krivica). Zato bavljenje digitalno forenzičkim procesima postaje nezaobilazna disciplina kada je reč o otkrivanju počinilaca dela sajber kriminala. Prikupljanje podataka može da podrazumeva prikupljanje podataka iz živog sistema da bi se sakupile osetljive tj. nestabilne informacije ili se vrši post-mortem prikupljanje podataka bez izmene ili oštećenja i u tom slučaju se vrši preuzimanje fizičkih

kliknuće na "buy" na ebay aukciji. Isto tako dešavale su se ove vrste prevara čime se omogućavalo uključivanje veb kamera i mikrofona kroz Adobe Flash Player za koji je ubrzo objavljena sigurnosna zakrpa.

⁴⁷ Radi se o psihološkim trikovima da bi se namamile potencijalne žrtve kroz sajtove za upoznavanje. Učinioci krivičnih dela upotrebljavaju lažne profile na tim sajtovima za upoznavanje, pretvarajući se da savršeno odgovaraju potencijalnoj žrtvi, korišćenjem takođe lažne fotografije koja je ukradena sa neke od društvenih mreža. Ljudi na tim fotografijama su takođe žrtve. Akcenat je stavljen na što većem zbližavanju sa potencijalnom žrtvom kroz korišćenje, viceva, poezije, poklona i drugih "romantičnih trikova", tako da se žrtvi učini da može da im veruje. Nakon uspostavljanja poverenja krajnji cilj je traženje od žrtve da pošalje novac, ček ili neki drugi oblik načina plaćanja, kako bi se napadaču pomoglo zbog navodnih finansijskih poteškoća kako su predstavili svojoj žrtvi. Dešava se da žrtva pošalje i svoje komprimovane slike (nakon uspostavljenog poverenja) tako da bi se kasnije učenom iznuđivao novac. Kao način borbe protiv ovakve vrste kriminala je obrazovanje što većeg broja ljudi po pitanju ovog načina prevare. Sajt <http://www.romancescam.com/> je jedan od sajtova koji doprinose borbi protiv ovakve vrste prevare.

dokaza (kao na primer hard diskovi, diskete ili drugi mediji). Nakon preuzimanja fizičkih dokaza vrše se forenzička dupliranja – uzimanje softverskog imidža ili kloniranje diska računarskih dokaza i utvrđuje se autentičnost između originalnog digitalnog dokaza sa forenzičkom kopijom. Post-mortem analiza ili kako se još u literaturi naziva statička analiza ima određena ograničenja, jer ne može da pruži potpunu sliku događaja. Alternativa post-mortem analizi jeste analiza uživo. U ovom slučaju digitalni dokazi se prikupljaju dok sistem radi. Kada se podaci prikupljaju iz "živog" operativnog sistema važno je znati koji su podaci lako promenljivi tj. podaci privremenog karaktera (eng. volatile), a koji podaci su postojanog karaktera (eng. non-volatile). Na prvom mestu "lako izmenljivi" podaci odnosno volatile podaci, su sistemski detalji koji istražiteljima pružaju uvid u način i prirodu protivpravne aktivnosti na sistemu i nekada mogu biti podaci od krucijalnog značaja. Od podataka koji neće lako biti izmenjeni na sistemu, na prvom mestu su oni koji daju informacije o statusu, setovanjima, konfiguraciji sistema i istorijske informacije na osnovu kojih se mogu potvrditi ili potkrepiti način izvršenja i prirodu dela sajber kriminala.

Možemo zaključiti na osnovu velikog broja primera iz prakse naših i stranih istražnih i sudskih organa da je zaista veliki broj maloletnika izložen raznim delima sajber kriminala, a da je jedan broj njih i učinilac nekih od krivičnih dela sajber kriminala. Kako svako društvo mora posebno da povede računa o maloletnim licima, kao posebno ranjivom delu društvo, može se konstatovati da je potrebno puno vremena i prostora posvetiti edukaciji i prevenciji u cilju smanjivanja broja maloletnika koji postaju žrtve ili su počinio krivičnih dela sajber kriminala.

LITERATURA

1. Diligenski A. Prlja D. (2014) *Fejsbuk i pravo*, Beograd: Institut za uporedno pravo.
2. Hay B., Bishop M., Nance K. (2009) "Live Analysis: Progress and Challenges", *IEEE Security and Privacy*, 3/2009.
3. Kopecký K. (2010) *Cyber grooming danger of cyberspace*, Olomouc.
4. Kopecký K. (2010) *Stalking a kyberstalking nebezpečné pronásledování*, Olomouc.
5. Leishman J. (2005) *Cyber-bullying*, CBC News Online.
6. Prlja D., Reljanović M. (2014) *Pravna informatika*, Beograd.
7. Sameer H., Patchin J. (2009) *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*, Corwin press.
8. Todorović D, Petrović D. Prlja D. (2014) *Internet i društvo*, Niš: Srpsko sociološko društvo.
9. Urošević, V. (2014) *Veze sajber kriminala sa iregularnom migracijom i trgovinom ljudima*, Beograd: Ministarstvo unutrašnjih poslova Republike Srbije.
10. Wilson C. (2003) *Computer attack and cyber terrorism: Vulnerabilities and policy issues for Congress*. Us Congressional Research Report RL32114, 2003.

Dragan Prlja, PhD, Research Associate
Institute of Comparative Law, Belgrade

Vanja Korać, PhD
Mathematical Institute, Belgrade

Andrej Diligenski, MSc, External Associate
Institute of Comparative Law, Belgrade

MINORS AND CYBERCRIME

Development of new information technologies has enabled an unimaginable development and progress to the society, but has brought many problems to the surface in the same time. Minors usually replace real for virtual world by spending long hours in a front of computer sharing their information, photos messages with known and often with completely unknown new virtual friends. Unfortunately, virtual friends do not always have good intention. They often want to manipulate with minors, abuse them sexually, deceive them or make them harm in some other way. Minors can not acquire sufficient level of information in established educational system and their families necessary for safe usage of Internet and social networks, which could lead to extremely serious consequences. Ever increasing number of cybercrime cases worldwide and in our own country indicates necessity for continues improvement of our legislative system, law enforcement system and prevention system when it comes to the question of cybercrime. This issue especially stands for cases when minors are victims or perpetrators of criminal offence related to cybercrime.

KEYWORDS: *cybercrime / law / criminal offenses / minors / Internet / information technologies*