VODIČ ZA SUDIJE I TUŽIOCE NA TEMU VISOKOTEHNOLOŠKOG KRIMINALA I ZAŠTITE MALOLETNIH LICA U REPUBLICI SRBIJI

Save the Children

Branko Stamenković
Saša Živanović
Bojana Paunović
Ivana Stevanović

ПРАВОСУДНА АКАДЕМИЈА

Save the Children veruje da svako dete zaslužuje budućnost. U zemljama severozapadnog Balkana radimo svaki dan kako bismo za decu osigurali zdrav početak života, priliku za učenje i zaštitu od nasilja. Kada se pojave krize i kada su deca najranjivija, mi smo uvek među prvima koji dođu pomoći i među poslednjima koji odlaze. Mi osiguravamo da se odgovori na specifične potrebe dece i da se njihov glas čuje. Postižemo dugotrajne rezultate za milione dece, uključujući onu decu do koje je najteže doći. Dajemo sve od sebe za decu - svaki dan i u vreme kriza – transformišući njihove živote i budućnost koja je pred nama.

Izdavač: Save the Children in North West Balkans
Autori: Branko Stamenković, Saša Živanović, Bojana Paunović, Ivana Stevanović
Vođa projekta: Vasilije Ljubinković
Grafički dizajn: Edin Bešlić
Štampa: Amos Graf Sarajevo
Tiraž: 1000

Ova publikacija urađena je u okviru projekta „Spojeni i sigurni - prema virtualnom okruženju sigurnom za decu“, čiju su realizaciju podržali Oak fondacija i Save the Children Norway.

Zajedno možemo učiniti više.
Recite nam šta mislite o našem radu?
RECI-NAM@savethechildren.org

SADRŽAJ

Prvo reagovanje na elektronske dokaze 43

Predgovor

Vodič za sudije i tužioce na temu visokotehnološkog kriminala i zaštite maloletnih lica u Republici Srbiji (u daljem tekstu: Vodič) namenjen je, kao što mu i samo ime kaže, tužiocima i sudijama polaznicima Osnovnog programa obuke Pravosudne akademije u Republici Srbiji i u tom smislu prati Kurikulum, razvijen i usvojen na Programskom odboru ove institucije, koja je ovlašćena za realizaciju specijalizovanih programa obuke za sudije i tužioce nosioce sertifikata za rad sa maloletnicima kao učiniocima krivičnih dela, odnosno maloletnim licima oštećenim, tj. žrtvama krivičnih dela.

Autori Vodiča prevashodno imaju u vidu da je informatička revolucija donela kvalitativni napredak u životima svih ljudi, toliko jak da je praktično više nemoguće zamisliti civilizaciju bez informatičke podrške u svim oblicima koju nam pružaju informacione tehnologije, ali da je, sa druge strane, ovakav eksplozivan razvoj neumitno proizveo i određene prateće posledice negativnog karaktera. Iz tog razloga, u Vodiču se posebna pažnja upravo poklanja osnovnim pojmovima visokotehnološkog kriminala, ukazuje na njegove pojavne oblike, daje prikaz savremenih trendova u izvršenju krivičnih dela iz ove oblasti i analizira normativni okvir koji reguliše ovu oblast u Republici Srbiji, prevashodno u sferi krivičnopravne reakcije.

Takođe, uvažena je i činjenica da je u poslednjih nekoliko decenija naročita pažnja na međunarodnom planu posvećena uspostavljanju delotvorne zaštite dece žrtva savremenih oblika kriminaliteta, posebno imajući u vidu neophodnost preduzimanja zakonodavnih i drugih mera za sprečavanje svih vidova seksualne eksploatacije i seksualnog zlostavljanja dece, kao i potrebu njihove zaštite, uvažavajući da najbolji interesi deteta i pravo deteta da se njegovo mišljenje čuje i uzme u razmatranje predstavljaju jedan od osnovnih principa u ostvarivanju, poštovanju i zaštiti njihovih prava. Države ugovornice, svesne obima i karaktera ovih pojava, posebno povećane međunarodne trgovine decom, iskorišćavanja dece u prostituciji i pornografiji, odnosno sve izražene zloupotrebe računarskih sistema i mreža u cilju regrutovanja dece u pomenute svrhe, pored ostalog, reagovale su i uspostavljanjem novih normi i standarda, koji će biti posebno istaknuti, i data su jasna uputstva za njihovu neposrednu primenu od strane nosioca pravosudnih funkcija.

Vodič sadrži i jasna uputstva i smernice za postupanje u slučajevima krivičnih dela na štetu dece i maloletnika u delu zloupotreba na internetu (odnosno, u sferi zloupotreba savremenih tehnologija), način reagovanja na elektronske dokaze i detaljne informacije o oduzimanju, rukovanju i ispitivanju elektronskih uređaja i uređaja povezanih sa njima. Posebna pažnja posvećena je i praktičnim primerima iz oblasti visokotehnološkog kriminala uz poseban naglasak na neophodnost unapređenja međunarodne i međuresorne saradnje među akterima u sferi zaštite dece i ojačavanja sistema.

Sve navedeno, autori Vodiča uobličili su u četiri tematske celine:
- Uvod u visokotehnološki kriminal i savremeni trendovi u izvršenju krivičnih dela iz ove oblasti (Branko Stamenković, posebni tužilac za visokotehnološki kriminal);
- Prvo reagovanje na elektronske dokaze (Saša Živanović, načelnik Odeljenja za visokotehnološki kriminal UKP MUP RS);
- Visokotehnološki kriminal kao krivično delo u domaćem zakonodavstvu sa posebnim osvrtom na tzv. cyberbullying i grooming (Bojana Paunović, sudija Apelacionog suda u Beogradu;
- Opšte mere zaštite i iskaz deteta u krivičnom postupku (dr Ivana Stevanović, viši naučni saradnik Instituta za kriminološka i sociološka istraživanja).

Poštovane koleginice i kolege, poštovani čitaoci, nadamo se da će Vodič biti od koristi za bolje razumevanje složene problematike o kojoj smo pisali i predstavljati još jedan iskorak ka uspostavljanju „pravosuđa po meri deteta" u Republici Srbiji(*).

«Pravosuđe po meri deteta» označava pravosudni sistem koji jemči poštovanje i delotvorno sprovođenje svih prava deteta na najvišem mogućem nivou, … To je, pre svega, pravosuđe koje je dostupno, primereno uzrastu, efikasno, prilagođeno potrebama i pravima deteta i usredsređeno na te potrebe i prava, uz poštovanje prava deteta, uključujući pravo na postupak u skladu sa zakonom, pravo da učestvuje u postupku i da razume postupak, na poštovanje privatnog i porodičnog života i na integritet i dostojanstvo. Ostvarivanje „pravosuđa po meri deteta» podrazumeva pravosuđe prilagođeno na način da bude primerenije detetu i efikasne postupke dostupne deci uz obezbeđenje neophodne nezavisne pravne reprezentacije. Na ovaj način, deci se omogućava da, kada dođu u kontakt sa pravosudnim sistemom, bilo kao svedoci, žrtve (oštećeni) ili kao učinioci krivičnih dela, tužioci i podnosioci pritužbi budu u mogućnosti da na adekvatan način zaštite svoja prava i interese.

Prilagođavanje pravosuđa da bude primerenije deci u Evropi deo je Agende Evropske unije o pravima deteta i predstavlja jedan od najvažnijih standarda u oblasti prava deteta. Uvažavanje osnovnih načela „pravosuđa (pravde) po meri deteta" podrazumeva primenu osnovnih principa: principa participacije, uvažavanje najboljih interesa deteta, poštovanje dostojanstva deteta, zaštitu od diskriminacije i vladavinu prava (Smernice Komiteta ministara Saveta Evrope o pravosuđu po meri deteta – III Osnovna načela – od A. do E).

Uvažavanje navedenih principa od posebne je važnosti u svetlu zaštite maloletnih lica kao oštećenih/svedoka savremenih oblika kriminaliteta od posledica sekundarne viktimizacije u krivičnom postupku.

* Smernice Komiteta ministara Saveta Evrope o pravosuđu po meri deteta, usvojene 17. novembra 2010. godine na 1.098. zasedanju zamenika ministara Saveta Evrope - Redigovana verzija od 31. maja 2011.

2 Agenda Evropske unije o pravima deteta usvojena od strane Evropske komisije Evropske unije 52011DC0060 od 15. februara 2011. godine 52011DC52011) ,0060DC0060,15. februar 2011. godine).

Uvod u visokotehnološki kriminal i savremeni trendovi u izvršenju krivičnih dela iz ove oblasti

1. Uvod

Revolucija u informacionim tehnologijama je suštinski promenila društvo i nastavljaće da ga menja i ubuduće. Mnogi poslovi su postali jednostavniji za obavljanje. Doskora i u samo određenim delovima društva, radi racionalizacije radnih procedura, informacione tehnologije korišćene su u svakodnevnom radu. Danas je teško zamisliti bilo koji deo društva bez uticaja primene računara i računarskih sistema. Informacione tehnologije su na sveobuhvatan način danas umešane i iskorišćene u svakom aspektu ljudske aktivnosti.

Ovakav razvoj je direktno uticao na, do sada, neviđeni ekonomski napredak, ali i društvene promene koje su, u okviru svog nastanka i postojanja, došle i u kontakt sa tamnijom stranom ljudske prirode. Nastajanje novih tipova i vrsta kriminala, kao i izvršenje tradicionalnih krivičnih dela upotrebom novih tehnologija, postalo je standardni deo realnosti državnih organa koji postupaju u ovoj oblasti.

Štaviše, posledice izvršenja krivičnih dela i ponašanja izvršilaca danas mnogo više i dublje obuhvataju tkivo svakog društva, pa i našeg, s obzirom da danas ne postoje geografske ni nacionalne granice, kada govorimo o upotrebi informacionih tehnologija i izvršenju krivičnih dela.

Nove tehnologije postavljaju izazov pred postojeće pravne koncepte. Tok informacija i komunikacija je danas na planetarnom nivou u potpunosti olakšan. Granice više nisu granice za ovakvu vrstu razmene. Kriminalci su sve više locirani na mestima odakle njihove radnje mogu da proizvedu značajniji efekat, tj. posledicu, ne samo po njih, već i po druge.

Ipak, domaći zakonodavni okvir je generalno ograničena teritorija nacionalnog zakonodavstva. Iz navedenih razloga, problemi u ovoj oblasti morali su da budu rešeni na međunarodnom nivou kroz međunarodno pravni okvir, koji je iznedrio usvajanje adekvatnih međunarodnih pravnih instrumenata. Danas takav instrument predstavlja Konvencija o „sajber“ kriminalu Saveta Evrope (CETS 185), čiji je cilj da se suprotstavi ovoj vrsti izazova, uz dužno poštovanje ljudskih prava, u novom informatičkom i post-informatičkom društvu.

2. Međunarodni značaj računarskog kriminala

Prema nekim izvorima(*) koji prate globalni trend izvršenja krivičnih dela u oblasti računarskog, to jest„ sajber“ kriminala, motivaciju koja stoji iza izvršenja ovog, ali i drugih oblika protivpravnog društvenog ponašanja, moguće je podeliti na pet glavnih grupa, i to kao motivaciju uperenu ka:

* www.hackmageddon.com

- „sajber“ špijunaži,
- „sajber“ ratovanju,
- ostalim oblicima sankcionisanog ili neprihvatljivog ponašanja.

U tom smislu, interesantno je da podaci iz navedenih javnih izvora ukazuju na to da na godišnjem nivou dolazi do značajnih promena u odnosu između ovih grupa, što je moguće videti već na uporednom prikazu podataka koji su obrađeni u junu 2015. i novembru 2016. godine, a koji ukazuju na to da prostor koji zahvata računarski kriminal raste iz godine u godinu značajnom stopom. Tako, na primjer, 2015. godine, procenjeni udeo računarskog, to jest, visokotehnološkog kriminala, u odnosu na druge grupe iznosio je %59,5, dok je već u 2016. godini taj udeo porastao na %82,7. Najveći pad su doživele aktivnosti koje pripadaju tzv. „haktivizmu“, o čemu će biti više reči biti u daljem tekstu, dok su grupe kojima pripadaju „sajber“ špijunaža i ratovanje, kao i ostali oblici izvršenja ovih dela ili događaja, ostali na približno istim nivoima.

Što se pravaca izvršenja ovih krivičnih dela tiče, primećeno je da je dosta prisutno uverenje da su žrtve, tj. oštećeni u ovoj oblasti ponajviše fizička lica. Ipak, podaci govore drugačije i ukazuju na to da, u stvari, najveću grupu oštećenih čine pravna lica, tj. preduzeća koja obavljaju komercijalnu delatnost. Odmah iz ove grupe - i to sa vrlo sličnim procentom (oko %21) - dolaze državni organi kao mete i žrtve „sajber“ napada. Tek nakon ove dve grupe (koje zajedno zauzimaju skoro %44 od ukupnog broja izvršenja ovih krivičnih dela), dolazi grupa koja pripada fizičkim licima, i to sa procenjenim procentom od oko %12 od ukupnog broja. Nakon ove tri glavne grupe meta napada (ujedno i žrtava), skoro ravnomerno raspoređeno dolaze razne organizacije, obrazovne institucije, finansijski sektor, itd.

Prilikom analize podataka koji se odnose na sredstva i pravce koji su iskorišćeni za izvršenje ovih krivičnih dela, kao i događaja koji možda nemaju odmah krivičnopravnu konotaciju, interesantno je primetiti da najveći udeo od skoro jedne četvrtine pripada sredstvima koja su nepoznata, tj. da tragovi izvršenja dela nisu sa sigurnošću mogli da ukažu na to koji je maliciozni softver konkretno korišćen u određenoj prilici.

Što se prepoznatih sredstava i pravaca tiče, najveći deo pripada raznim oblicima malicioznog softvera koji je korišćen za napade na komercijalne usluge koje pružaju razna pravna lica sa namerom ostvarivanja zarade. Nakon malicioznog softvera, pojavljuje se tzv. „otimanje naloga“, tj. neovlašćeno preuzimanje korisničkih naloga na raznim platformama, uključujući one koje pripadaju društvenim mrežama, elektronskoj pošti, bankarskim uslugama i sl. Za ovim kategorijama slede specifični oblici, kao što su SQL injekcije, distribuirani DoS napadi, izmena naslovnih strana određenih internet prezentacija („defacement“) i sl.

Kada govorimo o šteti koja nastaje protivpravnim ponašanjem putem korišćenja računara i računarskih mreža, a posebno krivičnih dela koja se mogu označiti kao visokotehnološka, treba imati na umu procenu određenih javnih izvora(*) da šteta koja na ovaj način nastaje na globalnom godišnjem nivou može doseći iznos od preko 388 milijardi USD. Ovaj iznos predstavlja zbir stvarne štete koja je nastala izvršenjem navedenih dela, kao i novčanih i materijalnih sredstava koja su fizička i pravna lica uložila u otklanjanje štete i dodatnu preventivnu zaštitu nakon ovakvih događaja. Stvarna šteta je procenjena na iznos od 114 milijardi USD, dok je otklanjanje štete i podizanje nivoa bezbednosti koštalo 274 milijardi USD.

Poređenja radi, svetska trgovina najpopularnijim nelegalnim narkoticima, tj. opojnim drogama, kao što su marihuana, kokain i heroin, procenjena je na godišnjem nivou na iznos od 288 milijardi USD, dok je ukupna svetska trgovina nelegalnim narkoticima procenjena zbirno na iznos od 411 milijardi USD.
Iz jednostavnog poređenja iznosa procenjene štete od računarskog kriminala i vrednosti trgovine opojnim drogama, proizilazi jasan zaključak da trgovina potonjim tek za nekih 23 milijarde USD prevazilazi prethodni iznos, što u svetskim razmerama zaista ne predstavlja značajnu brojku. Ovaj podatak je značajniji tim pre što izvršenje krivičnih dela koje za svoj objekat imaju opojne droge podrazumeva prisustvo izuzetnog rizika po izvršioce ovih krivičnih dela, kako u vidu reakcije državnih organa pojedinačnih zemalja, tako i u vidu koordinisanog nastupa i saradnje ovih organa na svetskom nivou radi suzbijanja ove vrste kriminaliteta, koji u velikom broju slučajeva podrazumeva i upotrebu fizičke sile i vatrenog oružja.

Sa druge strane, u svom najvećem delu izvršenje krivičnih dela tzv. „sajber“ kriminala podrazumeva upravo suprotno, tj. još uvek prisutno odsustvo značajnijeg angažovanja državnih organa kao i, skoro sigurno, odsustvo primene jakih mera represivne državne sile.
Navedeni primeri, u stvari, dodatno pojašnjavaju prisutni trend koji se kreće u pravcu pomeranja aktivnosti pripadnika kriminogenih sredina iz oblasti visokorizičnih krivičnih dela, koja su do sada imala visoke prinose protivpravne imovinske koristi u raznim oblicima, u oblast visokotehnološkog kriminala, koji, uz značajno manje ulaganje i sigurno manje prisutnu opasnost po fizički integritet, donosi praktično istu, ako ne u određenim slučajevima i veću protivpravnu imovinsku korist izvršiocima. Ovaj trend je uočen kako na globalnom, tako i lokalnom nivou.

* http://resources.infosecinstitute.com

3. Razvoj računarskog kriminala u Srbiji

Kada govorimo o razvoju računarskog kriminala u Republici Srbiji, možemo razlikovati više faza kroz koje je ovaj oblik kriminaliteta prolazio u poslednjih skoro 40 godina. Naime, iako i danas mnogi javni tužioci i sudije i dalje smatraju da je tzv. „sajber“ kriminal - kriminal budućnosti i da će njegove posledice, a time i neophodnost angažovanja javnih tužilaštava i sudova, tek postati činjenica u vremenu koje je pred nama, statistički podaci kojima raspolaže Posebno tužilaštvo za visokotehnološki kriminal u potpunosti razvejavaju ovu zabludu i pokazuju da je ova vrsta kriminaliteta itekako prisutna na našim prostorima i da trend izvršenja ovih krivičnih dela beleži stalni uspon.

GODINA	Upisnik KT	Upisnik KTR	Upisnik KTN	UKUPNO
2006	19			19
2007	75	68	11	154
2008	110	60	14	184
2009	91	114	42	247
2010	116	443	13	572
2011	130	502	28	660
2012	114	609	65	788
2013	160	558	243	961
2014	294	770	352	1416
2015	198	1306	570	2074
2016	240	1237	580	2058
UKUPNO	1547	5667	1918	9132

Tabela 1: pojedinačni i zbirni statistički prikaz primljenih krivičnih prijava i izveštaja u Posebnom tužilaštvu za visokotehnološki kriminal u periodu od 2006. do 2016. godine.

Imajući navedeno u vidu, bitno je napomenuti i to da visokotehnološki, tj. računarski kriminalitet, ne predstavlja novinu na prostorima Republike Srbije. Naime, još početkom osamdesetih godina prošlog veka, prvi slučajevi ove vrste kriminaliteta bili su zabeleženi u tadašnjem krivičnopravnom sistemu, koji, sasvim razumljivo, nikako nije bio spreman za pravilno reagovanje, ali je ipak iznašao način da u okviru mogućeg odgovori ovom izazovu. Konkretno, navedeni primer odnosi se na činjenično stanje u kome je tadašnji računarski operater u jednoj od poznatijih banaka Socijalističke Republike Srbije svojim radnjama uticao na obradu računarskih podataka tako što je preradio računarski program koji je obrađivao položena sredstva na dinarske račune komitenata banke, a sa ciljem zaokruživanja iznosa položenog novca na računima građana na niže vrednosti u malim iznosima (na primer, sa 1 dinar i 10 para na 1 dinar), i tako ostvarenu novčanu razliku korišćenjem programskih naredbi automatski prebacivao na više bankovnih računa koje je, kršeći pravila procedure za otvaranje računa, otvorio na svoje ime, te je tako u dužem vremenskom periodu na opisani način uspeo da akumulira značajan dinarski iznos na svojim računima, koji je na kraju i podigao i iskoristio za svoje lične potrebe.

Iz navedenog primera može se videti da su računari i računski programi već značajan vremenski period u upotrebi u našoj zemlji, prvobitno u preduzećima, državnim organima i institucijama, a nakon toga i među građanima. Naravno, svaka društvena pojava ili situacija skoro sigurno biva iskorišćena i u negativnom kontekstu, pogotovo kada govorimo o izvršenju krivičnih dela. U opisanom slučaju - za pribavljanje značajne protivpravne imovinske koristi, koja je kao motivacija prisutna i danas, i to kao jedan od lajtmotiva najvećeg broja izvršilaca ovih krivičnih dela.

Razvoj računarskog kriminala u Srbiji je tokom narednih godina dosta precizno pratio dešavanja na međunarodnoj kriminogenoj sceni i pored poteškoća koje su postojale u vidu međunarodnih ekonomskih sankcija tokom devedesetih godina. U ovom periodu, praktično je vladalo odsustvo krivičnopravne represije računarskog kriminaliteta, i to iz nekoliko razloga, od kojih se najviše izdvajaju nedostatak zakonskog okvira, potpuna nespremnost državnih organa da se suprotstave ovom obliku kriminaliteta, kao i spomenuto isključenje Republike Srbije iz međunarodnih odnosa, time i iz međunarodne saradnje u suzbijanju izvršenja ovih krivičnih dela. Računarski kriminalitet, u najvećem broju slučajeva, podrazumeva učešće međunarodne komponente u nekom delu izvršenja krivičnog dela, ili tokom primene materijalnopravnog ili procesnopravnog okvira krivičnog postupka. Ukoliko nije moguće ostvariti efektivnu međunarodnu saradnju, onda su skoro svi napori u tom postupanju vrlo verovatno predodređeni da budu neuspešni. Od krivičnopravnih događaja (namerno se ne koristi izraz „krivičnih dela“, s obzirom da ona kao posebna krivična dela računarskog kriminala nisu ni postojala u tadašnjem Krivičnom zakonu), u periodu devedesetih devedesetih godina prošlog veka najviše su zabeležene takozvane „krađe vremena“, tj. prava pristupa internetu zloupotrebom korisničkog imena i lozinke pojedinačnih

pretplatnika, razni drugi oblici imovinskog kriminala zloupotrebom platnih kartica i drugih sredstava plaćanja na internet portalima i tzv. „web" prodavnicama, kao i DDoS (Distributed Denial of Service) napadi radi onemogućavanja korišćenja internet-pristupa određenom pravnom ili fizičkom licu, pojedinačno ili u većem obimu. Za taj period je karakteristično i to da su motivi izvršilaca bili podeljeni između namere da se stekne protivpravna imovinska korist, sa jedne strane, i namere za dokazivanjem „značaja" ili „snage" pojedinca na internet-servisima, kao što su to bili „IRC" (Internet Relay Chat) i drugi, među istomišljenicima i drugim osobama koje su formirale društvene „online" zajednice određenih interesovanja. U vremenu koje dolazi, taj trend će se promeniti.

Tokom prve decenije 21. veka dolazi do određenih promena u načinu izvršenja krivičnih dela i motivaciji njihovih izvršilaca. Sve je prisutniji trend izvršenja radi sticanja imovinske koristi, dok ostali oblici ovog kriminaliteta počinju da budu motivisani drugim ciljevima, kao što je aktivizam na internetu radi postizanja određenih društvenih ili političkih ciljeva. Ukoliko se takav aktivizam ispoljavao kroz neovlašćeno pristupanje zaštićenim računarima i računarskim sistemima, tj. takozvanim „hakovanjem", onda se takav način ponašanja nazivao (i danas se naziva) „haktivizmom".

Na međunarodnom planu, kraj devedesetih godina prošlog veka i početak dvehiljaditih ovog, obeležava pojavljivanje jednog novog međunarodnog pravnog akta, koji će suštinski promeniti način na koji međunarodna stručna, ali i laička javnost prihvata postojanje računarskog kriminaliteta, kao i njegovo regulisanje kroz postojanje specifičnih materijalnih i procesnih odredbi, uz jednu dodatnu specifičnost, koja se ogleda u dosta detaljnom regulisanju odnosa međunarodne pravne pomoći u krivičnim stvarima. Taj međunarodni akt je Konvencija Saveta Evrope o visokotehnološkom („sajber") kriminalu (ETS 185).

4. Konvencija Saveta Evrope o visokotehnološkom („sajber") kriminalu (CETS 185)

Konvencija o visokotehnološkom („sajber") kriminalu Saveta Evrope je prvi međunarodni sporazum, tj. pravni akt, koji reguliše materijalni, procesni i međunarodni pravni okvir za krivična dela izvršena putem računara, računarskih mreža, kao i korišćenjem Interneta i drugih računarskih mreža međunarodnog ili lokalnog karaktera. Konvencija postavlja osnove pravnih normi koje se tiču kršenja prava intelektualne svojine, prevara izvršenih korišćenjem računara, zloupotrebe maloletnika u pornografske svrhe, protivpravnog pristupa zaštićenom računaru i računarskoj mreži, presretanju podataka, itd.. Ovom konvencijom su propisane i radnje i mere, kako materijalno, tako i procesnopravne prirode, koje su usmerene ka negativnom sankcionisanju društveno štetnog

ponašanja u ovoj oblasti i koje primenjuju savremene istražne metode prilikom otkrivanja i gonjenja izvršilaca krivičnih dela, kao što su pretraga računarskih mreža i presretanje računarskih podataka, čiji je glavni cilj gonjenje izvršilaca krivičnih dela i uspostavljanje zajedničke krivičnopravne politike, koja je usmerena ka zaštiti društva od svih oblika visokotehnološkog, tj. „sajber" kriminala, posebno kroz usvajanje odgovarajućih pravnih normi i uspostavljanje operativne međunarodne saradnje u ovoj oblasti.

Konvencija o „sajber" kriminalu Saveta Evrope je, nakon višegodišnjeg perioda usaglašavanja izvornog teksta, otvorena za potpisivanje od strane članica Saveta Evrope 23. novembra 2001. godine, kao i za potpisivanje od strane zemalja koje nisu članice ove organizacije, a koje imaju interes da primenjuju odredbe Konvencije i učestvuju u međunarodnoj saradnji.

Činjenica je da ova konvencija trenutno predstavlja jedini međunarodno pravno priznati i kontinentalno raširen pravni instrument u oblasti visokotehnološkog kriminala, koji u svom tekstu objedinjuje precizno određene i, što je još bitnije, upotrebljive savremene metode postupanja državnih organa, ali ne samo njih, već i drugih institucija i organizacija u ovoj oblasti, sve u cilju uspostavljanja delotvornog međunarodnog mehanizma, koji je sastavljen od više organskih celina na nivou pojedinih zemalja koje su potpisale ili ratifikovale ovu konvenciju.

Ove zemlje, kroz tako uspostavljenu planetarnu mrežu za prvo kao i rano reagovanje, te vođenje daljih pretkrivičnih i krivičnih postupaka, imaju mogućnost da na odgovarajući način, u skladu sa svojim tehničkim mogućnostima, odgovore na izazove visokotehnološkog, tj. „sajber kriminala" koje pred njih stavljaju izvršioci ovih krivičnih dela.

Do 1. jula 2017. godine, Konvenciji je pristupilo, potpisalo je ili ratifikovalo više od 59 zemalja. Osam zemalja nisu članice Saveta Evrope. U te zemlje spadaju: Australija, Kanada, Čile, Dominikanska Republika, Izrael, Japan, Mauricijus, Južnoafrička Republika, Panama, Senegal, Šri Lanka, Tonga i Sjedinjene Američke Države.

Od zemalja članica Evropske unije, kojih je ukupno 28 u ovom momentu, samo Republika Irska i Švedska nisu i ratifikovale ovu konvenciju, ali je jesu potpisale, dok su je sve ostale zemlje članice Evropske unije i ratifikovale, te se Konvencija, u skladu sa unutrašnjim pravnim poretkom svake zemlje, aktivno primenjuje kroz domaće materijalne i procesne i međunarodno pravne odredbe.

4.1. Cilj i struktura Konvencije Saveta Evrope o visokotehnološkom kriminalu

Konvencija Saveta Evrope o visokotehnološkom kriminalu za svoj cilj ima, na prvom mestu, harmonizaciju domaćih materijalnih krivičnopravnih odredbi u oblasti računarskog kriminala, omogućavanje domaćem krivičnom procesnopravnom okviru da nadležnim državnim organima pruži ovlašćenja koja su neophodna

za efektno otkrivanje i gonjenje izvršilaca ovih krivičnih dela, kao i uspostavljanje brzog i efektivnog okvira međunarodne saradnje u ovoj oblasti.
Imajući navedeno u vidu, Konvencija se sastoji iz četiri glave i to:

I. Upotreba termina,
II. Mere koje treba da budu preduzete na domaćem nivou – materijalno i procesno pravo,
III. Međunarodna saradnja, i
IV. Završne odredbe.

Prvi odeljak Glave druge predviđa odredbe o sankcionisanju kriminala koji je izvršen pomoću računara i računarskih mreža i određuje 9 opštih krivičnih dela koja su podeljena u 4 različite kategorije.
Krivična dela koja su određena konvencijom su:
1. neovlašćeni (protivpravni) pristup,
2. neovlašćeno (protivpravno) presretanje,
3. ometanje toka podataka,
4. ometanje računarskog sistema,
5. zloupotreba uređaja,
6. falsifikovanje izvršeno pomoću računara,
7. prevara izvršena pomoću računara,
8. krivična dela dečje pornografije, i
9. krivična dela autorskih i srodnih prava.

U drugom odeljku Glave druge, kada govorimo o procesnim odredbama, predviđeno je:
1. hitno čuvanje pohranjenih podataka,
2. hitno čuvanje i delimično otkrivanje podataka o saobraćaju,
3. naredbu za dostavljanje,
4. pretragu i zaplenu računarskih podataka,
5. prikupljanje podataka o saobraćaju u realnom vremenu,
6. presretanje podataka o saobraćaju.

U trećem odeljku, Konvencija sadrži odredbe koje se odnose na tradicionalne i računarski povezane pravne instrumente međusobne saradnje, tj. međunarodne saradnje u krivičnom pravu, kao i pravila za

uspostavljanje takozvane „7/24“ mreže za hitno reagovanje radi omogućavanja brze i efektivne saradnje između nadležnih organa strana potpisnica.

4.2. Pojmovna određenja

U okviru Poglavlja 1, Konvencija na opšti način definiše pojmove kao što su računarski sistem, računarski podaci, pružalac usluga, podaci o saobraćaju, itd., što je transponovano u značajnom obimu i u domaće zakonodavstvo.

Imajući navedeno u vidu, Konvencija u širem smislu definiše računarski sistem kao uređaj koji se sastoji od hardvera, tj. fizičkih uređaja, i softvera, tj. računarskih programa, koji se zajedno koriste za automatsko procesuiranje digitalnih podataka. Navedeni zbirni uređaj može uključiti ulazne, izlazne, kao i uređaje za pohranjivanje. Takođe, može biti sačinjen kao samostalan uređaj koji nije povezan na računarsku mrežu ili kao uređaj koji je povezan na mrežu sa drugim sličnim uređajima.

Pod automatskom obradom podataka podrazumeva se obrada podataka bez neposredne, tj. direktne ljudske intervencije, dok se procesuiranje podataka opisuje kao skup podataka u kompjuterskom sistemu koji se koristi kroz izvršavanje određenog kompjuterskog programa.

Nadalje, računarski program je set instrukcija koje računar izvršava radi postizanja određenih, tj. željenih rezultata. Računari mogu koristiti različite programe.

Računarski sistem se obično sastoji od različitih uređaja koji se međusobno razlikuju kao obrađivači ili centralne obrađivačke jedinice uz upotrebu takozvanih periferijskih jedinica. Periferijska jedinica je uređaj koji može obaviti određene specifične funkcije u saradnji sa glavnom procesorskom jedinicom, kao što su štampači, video bimovi, CD/DVD čitači i pisači i drugi slični uređaji.

U smislu Konvencije, računarsku mrežu predstavljaju dva ili više međusobno povezana računarska sistema. Međusobna povezanost može biti zemaljska, tj. putem žice ili kabla, bežična (putem radio, infracrvenog ili satelitskog emitovanja) ili kombinovana. Mreža može geografski biti ograničena na malu oblast (lokalna mreža) ili se može pružati preko velike teritorijalne oblasti (kao što su takozvane „WAN“ mreže). Ovakve mreže, takođe, mogu biti međusobno povezane na opisane načine.

Internet predstavlja globalnu mrežu koja se sastoji od mnoštva međusobno povezanih mreža koje sve koriste isti komunikacioni protokol, tj. način komunikacije. Drugi tipovi mreža takođe postoje, bez obzira da li su ili nisu povezane na internet, i međusobno su osposobljene da komuniciraju razmenom računarskih podataka između računarskih sistema.

Pojedinačni računari ili računarski sistemi mogu biti povezani na mrežu kao završne tačke komunikacije ili mogu u okviru takvih mreža služiti kao pomoć u prosleđivanju podataka između drugih računara i računarskih

sistema. Esencijalno je da se podaci upotrebom ovakvih sistema razmenjuju i mogu razmenjivati putem mreže, tj. međusobne povezanosti.

Konvencija se, prilikom definisanja računarskih podataka, oslanja na definiciju takvih podataka prema takozvanom „ISO" standardima. Ova definicija sadrži izraze koji su pogodni za procesuiranje, tj. korišćenje. Ovo znači da su podaci, da bi imali kvalitet računarskih, sastavljeni u takvoj formi da mogu biti direktno obrađeni – procesirani u računarskom sistemu.

Da bi bilo potpuno jasno da podaci na koje se odnosi Konvencija treba da budu podvedeni pod podatke u elektronskoj ili u drugoj formi podobnoj za računarsko procesiranje, uveden je i definisan izraz „računarski podaci".

Na osnovu ove definicije, računarski podaci su oni podaci koji su, u smislu krivičnopravnog zakonodavstva, automatski procesirani i mogu biti meta, tj. predmet izvršenja krivičnih dela koja su definisana navedenom Konvencijom, kao i objekat primene neke od istražnih mera koje su predviđene istom.

4.3. Pružalac usluga

Termin pružalac usluga tj. „Internet service provider" („ISP"), obuhvata široku kategoriju fizičkih i pravnih lica koja imaju određene uloge u odnosu na komunikaciju ili procesuiranje podataka u računarskim sistemima. Pod ovom definicijom je jasno navedeno da kako javni, tako i privatni subjekti koji pružaju ovakvu vrstu usluga jesu i moraju biti uključeni u krivičnopravni zakonodavni okvir zemalja potpisnica Konvencije.

Prema tome, nebitno je da li korisnici međusobno formiraju tj. čine zatvorenu grupu koja ne pruža ovakvu vrstu usluga prema spoljašnosti, da li takozvani „provajder usluga" svoje usluge pruža ka javnosti, kao i da li je ovo pružanje usluga besplatno ili uz naknadu. Primer zatvorene grupe mogu biti zaposleni u okviru privatnog preduzeća kojima ovakvu vrstu komunikacije omogućava kompanijska mreža.

U okviru ove definicije jasno je da se izraz „servis provajder" tj. pružalac usluga takođe odnosi i na one entitete, tj. subjekte koji pohranjuju ili na drugi način obrađuju podatke u ime i za račun prethodno navedenih subjekata. Nadalje, izraz obuhvata i one subjekte koji pohranjuju ili na drugi način procesiraju podatke u ime i za račun korisnika servisa koji su pomenuti pod ovom definicijom.

Na primer, u okviru ove definicije, pružalac usluga obuhvata podjednako usluge takozvanog „hostinga" i „kešinga", tj. trajnijeg ili privremenog čuvanja podataka i usluga, kao i usluge koje omogućavaju povezivanje na određenu mrežu. Ipak, običan pružalac usluga prezentovanja određenog sadržaja, kao što je, na primer, osoba koja sklopi ugovor sa kompanijom za takozvano „web hosting" radi „hostovanja", tj. čuvanja i prikazivanja veb-sajta – prezentacije, nije obuhvaćen ovom definicijom ukoliko entitet kod kog se navedeni sadržaj nalazi takođe ne pruža usluge povezivanja i obrade podataka komunikacione ili obrađivačke usluge podataka.

4.4. Podaci o saobraćaju

Pojam podataka o saobraćaju je definisan u članu 1. Konvencije, u okviru stava D, i predstavlja kategoriju računarskih podataka koji su predmet posebnog pravnog režima. Ovu vrstu podataka generiše - stvara računar (kompjuter) u tzv. „lancu komunikacije", radi usmeravanja komunikacije od mesta nastanka do krajnje destinacije. U tom smislu, podaci o saobraćaju predstavljaju pomoćno sredstvo samoj komunikaciji.

U slučaju vođenja istrage za krivično delo koje je izvršeno u vezi sa računarom ili računarskim sistemom, podaci o saobraćaju su neophodni radi praćenja izvora komunikacije kao početna tačka za prikupljanje daljih dokaza, kao deo samog dokaznog materijala u prilog postojanja osnovane sumnje da je izvršeno krivično delo, ili, u kasnijem toku krivičnog postupka, radi dokazivanja postojanja krivičnog dela i krivičnopravne odgovornosti njegovog izvršioca. Zbog svoje prirode, koja se ogleda u vrlo kratkom trajanju, podaci o saobraćaju moraju da budu sačuvani - obezbeđeni na najbrži mogući način.

Posledično, njihovo brzo otkrivanje može biti od ključne važnosti za lociranje komunikacionog pravca radi daljeg prikupljanja dokaza za koje postoji opasnost da će biti izbrisani, ili koji mogu poslužiti za otkrivanje identiteta izvršioca krivičnog dela.

S tim u vezi, uobičajene procedure, radnje i mere, koje u standardnom vođenju krivičnog postupka preduzima nadležni organ otkrivanja ili gonjenja radi utvrđivanja postojanja krivičnog dela i eventualne krivičnopravne odgovornosti njegovog izvršioca, mogu se u ovom slučaju pokazati kao nedovoljne. Štaviše, uporedna pravna praksa, kako redovnih tako i specijalizovanih organa otkrivanja i gonjenja, tj. službi i jedinica Ministarstva unutrašnjih poslova kao i nadležnih državnih, tj. javnih tužilaštava, upravo pokazuje da vremenski okviri koji prate primenu standardnih istražnih metoda mogu predstavljati jednu od ključnih prepreka za uspešno gonjenje u ovoj krivičnopravnoj oblasti.

Konvencija taksativno nabraja kategorije podataka o saobraćaju i to u vidu porekla - izvora komunikacije, njenog odredišta, puta, vremena, datuma, veličine, trajanja i vrste pružene usluge. Vredno je pomenuti da neće sve ove kategorije biti uvek tehnički dostupne, posebno kada imamo u vidu raznolikost tehničke opremljenosti i obučenost zaposlenih u raznim preduzećima koja se bave uslugom pružanja pristupa internetu ili omogućavanju korišćenja određenih kategorija usluga koje su vezane za korišćenje računarskih mreža, kako međunarodnih tako i lokalnih, javnih i privatnih.

Poreklo komunikacije se odnosi na broj telefona, internet protokol adresu ili sličnu identifikaciju komunikacione opreme kojoj internet servis provajder pruža usluge. Odredište predstavlja uporedivu indikaciju o uređajima koji služe za komunikaciju i način same komunikacije, tj. kako su podaci usmereni, transmitovani ili isporučeni.

Pojam vrste servisa se odnosi na vrstu usluge koja se koristi unutar same mreže i ostvaruje kroz razmenu tzv. fajlova, elektronsku poštu ili razmenu instant poruka.

Definicija, na ovaj način opisana, ostavlja nacionalnim zakonodavstvima mogućnost da primene u datim okvirima različit pristup pravnoj zaštiti podataka o saobraćaju, u skladu sa njihovom osetljivošću. U ovom smislu, u članu 15. Konvencije, postoji obaveza strana potpisnica da pruže uslove i garancije radi adekvatne zaštite ljudskih prava i sloboda.

U tom smislu, materijalnopravne odredbe, kao i procesnopravne odredbe koje se primenjuju ili mogu biti primenjene, mogu biti različite, tj. varirati u odnosu na osetljivost samih podataka.

4.5. Krivična dela

Konvencija u Drugoj glavi u okviru trećeg dela reguliše materijalnopravni okvir i to u članovima od 2. do 13., procesnopravni okvir od članova 14. do 21., kao i nadležnost u članu 22.

Cilj propisivanja materijalnopravnog okvira Konvencijom, u svakom slučaju, leži u unapređenju zakonskih odredbi radi sprečavanja i gonjenja specifičnog oblika, tj. vrste kriminaliteta koji se izvršava pomoću računara i u računarskom okruženju uz korišćenje računarskih mreža.

Uspostavljanjem zajedničkog minimalnog standarda u propisivanju krivičnih dela i njihovih bitnih obeležja, postiže se harmonizacija međunarodnog krivičnog prava, koja je posebno značajna u ovoj oblasti kriminaliteta, imajući u vidu njegovu eksponencijalnu krivu rasta i razvoja, a koje bi trebalo da podrazumeva harmonizaciju kako na nacionalnom, tako i na međunarodnom nivou.

Ukoliko bi ovakva harmonizacija materijalnopravnih krivičnih odredbi izostala, primena drugih međunarodno pravnih instrumenata, kao što je, na primer, Palermo Konvencija ili Konvencija o pružanju međunarodne pravne pomoći u krivičnim stvarima iz 1959. godine bila bi dovedena u pitanje u smislu da bilo znatno otežano, ako ne i nemoguće, da se odredbe tih drugih konvencija primenjuju jedinstveno na teritoriji i u okviru pravnih poredaka zemalja koje su ih ratifikovale i koje osnovano žele da svoje unutrašnje pravne poretke i organe koji te poretke sprovode dovedu u takvo stanje operativnosti i saradnje koje bi garantovalo uspešno gonjenje izvršilaca krivičnih dela. Osnovni postulat pružanja međunarodne pravne pomoći u krivičnim stvarima je postojanje kažnjivosti u krivičnopravnom smislu određenog ljudskog ponašanja, koje mora biti propisano materijalnopravnim odredbama krivičnog zakonodavstva kako zemlje molilje, tako i zamoljene zemlje. U slučaju nedostatka harmonizacije materijalnopravnih propisa u ovoj oblasti, kao i u svakoj drugoj oblasti krivičnopravog

raspolaganju organima otkrivanja i gonjenja, a time i efektivnog onemogućavanja sankcionisanja takve vrste protivpravnog ponašanja. To bi, na kraju, dovelo do nemogućnosti da se društvena zajednica svake od tih zemalja zaštiti na odgovarajući način i garantuje sigurnost ljudi i njihove imovine.

Krivična dela koja su navedena „Sajber-krajm konvencijom" Saveta Evrope predstavljaju minimum regulisanja i propisivanja krivičnopravne norme u domaćim zakonodavstvima zemalja koje su je ratifikovale i koja, u svakom slučaju, ne isključuje njihovu dodatnu razradu u okviru krivičnih zakonika tih zemalja.

Komitet navedene Konvencije pod nazivom T-CY, koji je sastavljen od nacionalnih predstavnika zemalja koje su ratifikovale Konvenciju, kao i Biro navedenog Komiteta, u periodu koji je danas već duži od jedne decenije, aktivno je radio i radi na osavremenjivanju tumačenja i metoda primene osnovnih odredbi same Konvencije kroz tzv. „uputstva" („Guidelines"), koja bi trebalo da detaljnije pojasne mogućnost primene određenih odredbi Konvencije u savremenom životu, kao i u savremenom otkrivanju i gonjenju krivičnih dela iz ove oblasti.

Ipak, može se odati priznanje tvorcima teksta ovog međunarodno pravnog akta, koji su u drugoj polovini devedesetih godina XX veka uspeli da skoro u potpunosti definišu, propišu i predvide preovlađujuće oblike tzv. „sajber" kriminaliteta, te da ih utkaju u tkivo Konvencije, koja i posle skoro 20 godina od nastanka prvobitnog teksta, uz manje korekcije donošenjem dodatnog protokola i izdavanjem prethodno spomenutih uputstava, uspeva da u svetu koji se skoro dnevno menja, kao što je svet informaciono-komunikacionih tehnologija i socijalnog umrežavanja, korišćenjem tih tehnologija da odgovori na izazove koji se nalaze pred onim pripadnicima društva kojima je data ustavna i zakonska nadležnost da ga štite od štetnih društvenih pojava.

Kriminalizacija tih ponašanja u vidu protivpravnog pristupa, protivpravnog presretanja, ometanja podataka, ometanja sistema i zloupotrebe uređaja, kao i krivičnih dela kao što su računarski falsifikat, računarska prevara, zloupotreba maloletnika u pornografske svrhe (dečija pornografija), kao i krivična dela koja se odnose na povredu autorskih i drugih srodnih prava, kako u svom osnovnom obliku izvršenja, tako i kroz saučesništvo u vidu saizvršilaštva, podstrekavanja i pomaganja, uz definisanje krivičnopravne odgovornosti pravnih lica u ovoj oblasti, ukazuje na to da i pored proteka već navedenog vremenskog perioda i brze promene navedenih tehnologija, u svojoj biti izvršenje krivičnih dela, uključujući i njihove nove oblike i nove načine izvršenja u tzv. „sajber svetu", mogu biti uspešno predviđeni, definisani i sankcionisani.

Time se otvara put da primenom alata generalne i specijalne krivičnopravne prevencije, ovi oblici kriminaliteta budu, u najboljem slučaju, iskorenjeni ili svedeni na onaj nivo koji ne predstavlja ili ne bi predstavljao značajnu ili značajniju društvenu opasnost.

Činjenica je da ovom cilju teže skoro sva krivičnopravna zakonodavstva zemalja sveta današnjice, a koja predstavljaju glavni pokretački motiv postupanja službenih lica koji se nalaze u sistemu krivičnopravne zaštite i posvećeni su borbi protiv svih oblika kriminaliteta.

Treba imati u vidu da se u ovoj oblasti, pored redovnih veština kojima pripadnici ovih organa moraju da raspolažu, podrazumeva da policajci, tužioci i sudije moraju raspolagati i dodatnim znanjima i veštinama, često tehničkog i tehnološkog karaktera, kako bi bili u mogućnosti da pravovremeno, kvalitetno i uspešno odgovore izazovima ovog kriminaliteta.

4.6. Procesno pravo

Tehnološka revolucija, a posebno revolucionarni razvoj informacionih tehnologija, koja svoj poseban uspon doživljava od početka XXI veka i, u okviru toga, nezapamćeni razvoj društvenih zajednica koje su u svom nastanku i razvoju koristile usluge internet-protokola i internet-tehnologija, su međusobno povezane kroz podelu zajedničkih resursa na lokalnom i na globalnom nivou, čime neminovno dolaze u kontakt i sa kriminogenim sredinama, često bivajući otvorene ili ranjive za zloupotrebu od strane društvenih elemenata, koji nisu spremni da se pridržavaju zakonom propisanih okvira društveno prihvatljivog ponašanja.

Komunikacione mreže, koje se stalno šire na svaki mogući zamislivi način, kako teritorijalno tako i tehnološki, otvaraju, praktično svakodnevno, nova vrata za kriminalne aktivnosti, kako u pogledu tradicionalnih, tj. standardnih krivičnih dela, tako i krivičnih dela koja su specifična za upotrebu informacionih tehnologija. S tim u vezi, nije dovoljno da samo materijalno krivično pravo bude u korak sa ovakvim razvojem društvene stvarnosti i njenim zloupotrebama, nego i procesno pravo, zajedno sa istražnim tehnikama koje su propisane i neophodne za uspešno postupanje u ovoj oblasti, takođe mora biti, čak i više nego materijalno pravo, u skladu sa IKT (informaciono-komunikacionim tehnologijama), pa čak pri tome nastojati da bude ispred savremenih tehnoloških zbivanja.

Naravno, zaštitne mere koje postoje ili su predviđene kao kontrolni mehanizam za narastajuća ovlašćenja državnih institucija takođe moraju biti u korak sa razvojem tehnologije i krivičnopravnog materijalnog i procesnog okvira. Jedan od najvećih izazova u borbi protiv visokotehnološkog kriminala u mrežnom okruženju je teškoća identifikacije izvršioca krivičnog dela i procena obima štete koju izvršenje takvog krivičnog dela izaziva. Jedan od povezanih problema je osetljivost elektronskih podataka, koji mogu biti vrlo lako izmenjeni, pomereni ili izbrisani u nekoliko sekundi. Na primer, korisnik koji ima mogućnost kontrole podataka može iskoristiti računarski sistem ili računar da izbriše te podatke, a koji jesu i mogu biti predmet interesovanja krivične istrage, čime praktično pristupa uništavanju dokaznog materijala. Brzina i, ponekad, tajnost postupanja, vrlo često su od vitalnog značaja za uspeh istraga u ovoj specifičnoj oblasti kriminala. U tom smislu, Konvencija o visokotehnološkom kriminalu Saveta Evrope prilagođava tradicionalne procesne mere, kao što su pretresanje stana i prostorija novom tehničkom okruženju. S tim u vezi, mogu biti kreirane i upotrebljene nove mere i radnje, kao što su

ubrzano čuvanje podataka u cilju osiguravanja da tradicionalne mere i radnje mogu ostati i dalje upotrebljive u vrlo osetljivom tehnološkom okruženju.

S obzirom da novo tehnološko okruženje nije uvek statično, već može biti vrlo fluidno u smislu procesuiranja komunikacija i njihovog toka, druge standardne krivičnopravne procedure koje služe za prikupljanje dokaznog materijala i koje su od značaja za informaciono-komunikacionu tehnologiju, kao što su prikupljanje podataka o saobraćaju u realnom vremenu i presretanje sadržaja komunikacije, takođe mogu biti i jesu prilagođene novim okolnostima u nameri da dozvole prikupljanje elektronskih podataka koji nastaju ili su sastavni deo procesa komunikacije.

Ovom prilikom napominjemo da su neke od ovih mera navedene i u preporuci Saveta Evrope broj R(13(95 u pogledu problema krivičnoprocesnog prava koji su u vezi sa informacionim tehnologijama.

Krivično pravne materijalne i procesne odredbe se u svom opštem obliku odnose na sve tipove podataka, uključujući i tri specifična tipa računarskih podataka koji se mogu podeliti na:

1. podatke o pretplatniku („basic subscriber information“ ili „BSI“),
2. podatke o saobraćaju („traffic data“),
3. podatke o sadržini komunikacije („content data“).

Navedeni podaci mogu postojati u svoja dva zbirna pod-oblika, i to:

1. u pohranjenom obliku, i
2. u obliku korišćenja u realnom vremenu u toku komunikacije.

Konvencija predviđa definicije ovih izraza u svojim članovima 1. i 18. Primenljivost određene procedure za određeni tip ili vrstu elektronskih podataka zavisi od prirode i oblika podataka, kao i prirode procedure, što je posebno opisano u navedenim članovima Konvencije.

U toku adaptacije tradicionalnih procesnih odredbi zakona novom tehnološkom okruženju, postavilo se pitanje upotrebe odgovarajuće terminologije u odnosu na procesnopravne instrumente. Glavno pitanje odnosi se i usmereno je ka uključivanju i održavanju tradicionalnog rečnika koji je poznat u zakonicima o krivičnom postupku, kao što je „pretres stana i prostorija“, „oduzimanje predmeta“, itd., u odnosu na korišćenje novih i više tehnoloških orijentisanih računarskih termina, kao što su „pristup“ i „kopiranje“, koji su danas već standardno uključeni u tekstove međunarodnog okruženja u vezi ovih pitanja.

Čini nam se da bi jedan fleksibilniji pristup, koji bi omogućio postupajućim organima da pored standardnih koriste i nove termine, posebno u određivanju i primeni određenih procesnih radnji i tehnika, u svakom slučaju bio koristan za uspešno vođenje krivičnog postupka.

Takođe, pojam nadležnih organa, posebno u zemljama okruženja u poslednjih 10 godina, značajno je promenjen, u smislu da su ovlašćenja u istražnom postupku značajno ili u potpunosti preneta na državna tužilaštva, u kom smislu je kao sui generis ovlašćenje sudske vlasti ostalo staranje o institutima kojima se ograničavaju ljudska prava i slobode, tj. institutima čije je određivanje neophodno radi uspešnog vođenja pretkrivičnog i krivičnog postupka, kao što su tajne mere nadzora komunikacije, prikupljanje podataka o sadržaju komunikacije, itd.

Obuhvat procesnih odredbi, kada govorimo o računarskom kriminalu i „Konvenciji o visokoteheološkom kriminalu iz Budimpešte“ tj. „Sajber-krajm konvenciji“ Saveta Evrope, podrazumeva da će sve zemlje koje su ratifikovale ovu Konvenciju usvojiti takav normativni okvir koji će dalje dati ovlašćenja nadležnim državnim organima da uspešno otkrivaju i gone krivična dela koja su predviđena Konvencijom, druga krivična dela koja su izvršena putem računarskih sistema, kao i prikupljanje dokaza u elektronskoj formi radi vođenja postupka za izvršenje ovih krivičnog dela.

S druge strane, uspostavljanje i primena ovakve vrste ovlašćenja kroz procesne odredbe treba da budu pažljivo posmatrane i usmerene ka mogućnosti uslovljavanja i kontrole koje su predviđene u okviru domaćeg zakonodavstava. Drugačije rečeno, zemlje koje su ratifikovale Konvenciju su u obavezi da donesu određene procesnopravne norme radi uspostavljanja i primene ovih ovlašćenja, kako u opštim, tako i u posebnim slučajevima, a čije će propisivanje biti u skladu sa domaćim pravnim okvirom. Ove odredbe mogu uključivati i takvu vrstu zaštitnih odredbi koje su na domaćem - nacionalnom nivou predviđene u okviru Ustava, pravnog poretka, sudskog i javnotužilačkog sistema, i slično.

Bitno je naglasiti da uspostavljanje uravnoteženog sistema podrazumeva da takav pristup zahteva usklađenost potrebe i zahteva organa otkrivanja, tj. pripadnika Ministarstva unutrašnjih poslova i bezbednosnih agencija da postupaju u skladu sa odredbama Konvencije i drugih međunarodnih i pravnih akata, kojima se obezbeđuje određena zaštita ljudskih prava i sloboda.

U tom smislu, Konvencija izričito navodi i time uvažava da države koje su je ratifikovale potiču iz različitih pravnih sistema i kultura, te da nije moguće taksativno navesti kao i konkretno odrediti jasno primenljive uslove i zaštitne odredbe za svako moguće ovlašćenje ili proceduru u svakoj pojedinačnoj zemlji. S tim u vezi, ipak postoji zajednički minimum standarda koje Konvencija predviđa. Ovaj minimum standarda proističe iz obaveza svake zemlje koja ju je ratifikovala da primeni međunarodne instrumente koji su doneti u ovoj oblasti i koji uključuju

Evropsku konvenciju o zaštiti ljudskih prava i osnovnih sloboda iz 1950. godine sa dodatnim protokolima broj 7 ,6 ,4 ,1 i 12, kao i Međunarodnu konvenciju o građanskim i političkim pravima iz 1960. godine, ne isključujući, u određenim pravnim sistemima i geografskim delovima planete, primenu Američke konvencije o ljudskim pravima iz 1960. godine, kao i Afričku povelju o ljudskim pravima i slobodama naroda iz 1981. godine.

Ne ograničavajući vrste i uslove za uspostavljanje ovih mehanizama, Konvencija specifično zahteva da se takvi uslovi, koji se smatraju odgovarajućim u smislu odredaba procesnih zakonodavstava, odnose na pravosudne ili druge nezavisne organe nadzora, koji u okvirima svojih ovlašćenja mogu odobriti na određeni način krivičnopravne procesne alate u smislu vođenja krivičnih postupaka, kao i njihovo eventualno ograničavanje radi obezbeđivanja i poštovanja ljudskih prava i sloboda.

Imajući ranije navedeno u vidu u smislu procesnih odredbi, Konvencija podrazumeva takve mehanizme i alate koji nalažu hitno čuvanje pohranjenih računarskih podataka, koji su propisani članovima 16. i 17. Konvencije, i koji se odnose na podatke koje su već prikupili i čuvaju držaoci podataka, kao što su na primer internet-servis provajderi. Ove odredbe se ne odnose na prikupljanje podataka u realnom vremenu, prikupljanje podataka o budućem saobraćaju, ili pristup komunikacijama u realnom vremenu. Mere koje su opisane u ovom članu odnose se samo na podatke koji već postoje i koji su pohranjeni.

Treba naglasiti da čuvanje podataka mora da se razlikuje od pohranjivanja podataka. Iako su na prvi pogled ovi pojmovi slični, postoji bitna razlika između ovih termina u odnosu na njihovo korišćenje kada su računari u pitanju.

„Prezervacija - očuvanje podataka“ označava čuvanje podataka koji već postoje u pohranjenoj formi, koji su zaštićeni od bilo čega što može uticati na njihov kvalitet ili uslove u kojima bi eventualno bili izmenjeni ili oštećeni.

„Retencija podataka“, označava čuvanje podataka koji se trenutno proizvode - generišu u nečijem posedu od sadašnjeg momenta ka budućnosti. Retencija podataka, dalje, označava akumulaciju podataka u sadašnjosti i njihovo čuvanje za ubuduće i u budućem vremenskom periodu. Retencija podataka je, u stvari, postupak odlaganja podataka, dok je prezervacija podataka aktivnost koja označava čuvanje podataka na sigurnom i obezbeđenom mestu.

Članovi 16. i 17. Konvencije odnose se na tzv. prezervaciju podataka, a ne na retenciju. Oni ne određuju kolekciju i retenciju svih ili nekih podataka Koje je prikupio internet-servis provajderi ili drugi subjekat, tj. privredni subjekat u toku obavljanja njihovih poslova. Prezervacija - očuvanje podataka odnosi se i primenjuje na računarske podatke koji su pohranjeni sredstvima računarskog sistema, što prethodno podrazumeva da ti podaci već postoje, tj. da su bili prikupljeni i odloženi.

Konvencija u svojim narednim članovima određuje i definiše procesne instrumente kao što su:
- hitno čuvanje pohranjenih računarskih podataka (član 16.),
- hitno čuvanje i delimično pohranjivanje podataka o saobraćaju (član 17.),
- naredbu o dostavljanju podataka (član 18.),
- pretragu i zaplenu pohranjenih računarskih podataka (član 19.),
- prikupljanje podataka u realnom vremenu,
- prikupljanje podataka o saobraćaju u realnom vremenu (član 20.),
- presretanje podataka o sadržini komunikacije (član 21.).

Od navedenih mera, posebno je interesantno osvrnuti se na tzv. „naredbu o pružanju podataka“, koja predstavlja fleksibilnu meru koju bi pripadnici organa otkrivanja mogli da primene u različitim slučajevima, posebno u onim momentima kada druge vrste mera, kao što su naredbe o pretresu, zapleni, presretanju komunikacija i slično, zahtevaju ispunjavanje značajnijih i zahtevnijih pravnih i tehničkih uslova.

Primena ovog proceduralnog mehanizama je posebno korisna i može se odnositi na računarske podatke ili podatke o pretplatniku koji se nalaze u posedu ili kontroli određene osobe ili provajdera. Naravno, ova mera je primenjiva ukoliko osoba ili servis-provajder takvu vrstu podataka čuva. Treba biti svestan da u pojedinim zemljama u svetu ne postoji obaveza internet-servis-provajdera da ovakve vrste podataka čuvaju, tj. pohranjuju.

Posebno treba naglasiti, imajući u vidu posebni pravni režim pribavljanja podataka o saobraćaju, podataka o sadržini saobraćaja, da su podaci o pretplatniku definisani na takav način da se odnose na bilo koju informaciju koju servis-provajder zadržava i koja se odnosi na pretplatnika njihovih usluga. Pretplatnički podaci mogu biti čuvani u bilo kojoj formi, od elektronske do papirne.

Takođe, pojam pretplatnika uključuje široki pojam klijenata servis-provajdera, od osoba koje su na osnovu ugovornog odnosa korisnici usluga tog preduzeća, preko onih koji su povremeni pretplatnici samo za određenu priliku i u određenom ograničenom vremenskom trajanju, pa sve do onih koji usluge određenog provajdera koriste bez nadoknade.

U toku krivične istrage, pretplatnička informacija biće najverovatnije zatražena u dve situacije, tj. primera. U prvom primeru, pretplatnička informacija je potrebna radi identifikacije servisa i tehničkih mera koje je određeno lice koristilo ili ih još uvek koristi, a to lice je pretplatnik, kao što su: tip telefonskog servisa (mobilna ili fiksna linija), tip drugih pridruženih servisa tj. usluga (na primer: prosleđivanje poziva, govorna pošta, itd.), telefonski broj ili tehnička adresa (IP adresa, E-mail adresa).

U drugom primeru, kada je tehnička adresa poznata, pretplatnička informacija biće zatražena i potrebna radi ustanovljavanja identiteta osobe u pitanju.
Druge pretplatničke informacije, kao što su komercijalne informacije o naplati, tj. uslovima plaćanja koje je pretplatnik ima, takođe mogu biti od značaja za vođenje krivične istrage, posebno u slučajevima kada se istraga vodi radi utvrđivanja krivičnog dela i odgovornosti za računarsku prevaru za «klasično» krivično delo prevare, kao i druga krivična dela koja su usmerena protiv imovine lica, platnog prometa i privrede.

Takođe, podaci o pretplatniku nisu ograničeni samo na informacije koje se odnose na direktnu upotrebu komunikacionih servisa. Takođe mogu podrazumevati bilo koju informaciju, osim informacija o saobraćaju ili o sadržaju saobraćaja, na osnovu koje se može ustanoviti identitet određene osobe, poštanska ili geografska adresa, telefonski ili drugi broj ili adresa, informacije o naplati i plaćanju koje su prikupljene i zasnovane na osnovu ugovora o pretplatničkom odnosu, itd.
Navedene informacije takođe mogu obuhvatiti i podatke o lokaciji na kojoj je određena oprema instalirana (kablovski modem, na primer), i podatke koji su sadržani u ugovoru o zasnivanju pretplatničkog odnosa i instalaciji navedenog uređaja od stane ovlašćenog servisnog lica internet servis provajdera, tj. preduzeća.

Pored informacije o mestu i adresi gde je navedena oprema instalirana, ovakva vrsta informacije je takođe bitna sa stanovišta utvrđivanja činjenice da takva vrsta opreme nije lako pokretna, već da je na osnovu tehničkih pokazatelja u okviru rada navedenog preduzeća – internet-servis- provajdera, potvrđeno da je takva vrsta opreme funkcionalna na adresi na kojoj su je ovlašćena lica instalirala, shodno čemu je jasno da podaci koji se nalaze u ugovoru o zasnivanju pretplatničkog odnosa odgovaraju realnom stanju stvari.

Treba naglasiti da su ova ovlašćenja vezana sa odredbama članova 14. i 15. Konvencije o visokotehnološkom kriminalu Saveta Evrope, koje ostavljaju nacionalnim zakonodavstvima uspostavljanje sistema kontrole i zaštite ljudskih prava u ovoj oblasti.

Nacionalna zakonodavstva, ukoliko smatraju za potrebno, mogu propisati da se ovakve vrste radnji po svim elementima, ili samo u nekim za koje se može smatrati da su osetljivi sa stanovišta zaštite ličnih podataka, može tražiti kontrola pravosudnih ili drugih samostalnih i nezavisnih organa.

4.7. Međunarodna saradnja

Konvencija o visokotehnološkom kriminalu Saveta Evrope u svom trećem poglavlju, u članovima od 23. do 35, reguliše međunarodnu pravnu pomoć u krivičnim stvarima u oblasti tzv. „sajber-kriminaliteta“. Konvencija u navedenim članovima, a posebno u uvodnim, naglašava i podvlači neophodnost proširenja međunarodne saradnje na najširi i najobuhvatniji mogući način.

Praktično, Konvencija, kroz uspostavljanje principa međunarodne saradnje, omogućava uspostavljanje intenzivne i ekstenzivne međusobne saradnje država i njenih organa i pokušava da umanji svaki negativan uticaj na brz i neometan protok informacija i dokaza u međunarodnom okruženju.

Takođe, međunarodna saradnja trebalo bi da bude usmerena i obuhvata i sva krivična dela koja se odnose na računare i računarske sisteme, kao i podatke koji su generisani računarom, koji su upotrebljeni ili na drugi način iskorišćeni u toku računarske komunikacije, kao i prikupljanje dokaza u elektronskoj formi u vezi izvršenja krivičnih dela. Ovo znači da, bez obzira da li je krivično delo izvršeno upotrebom računara, računarskog sistema ili se radi o uobičajenom vršenju krivičnog koje nije izvršeno putem računara, ali uključuje elektronske dokaze, članovi Konvencije u ovoj Glavi mogu i treba da budu primenjeni.

Ipak, treba naglasiti da članovi 24 - ekstradicija, 33 - međunarodna saradnja u odnosu na prikupljanje u realnom vremenu podataka o saobraćaju i član 34 - međunarodna pomoć u odnosu na presretanje sadržaja komunikacije, dozvoljava zemljama koje su ratifikovale ovu Konvenciju da putem rezervi ili na drugi način pruže drugačiji pristup i obuhvat primene ovih mera, kada se radi o međunarodnoj saradnji.

Posebno je bitno naglasiti da međunarodna saradnja u oblasti sajber-kriminala treba da bude u skladu sa odredbama ove Glave i kroz primer, ali i kroz primenu svih relevantnih međunarodnih sporazuma u vezi sa međunarodnom saradnjom u krivičnim predmetima, drugih propisanih oblika međunarodne saradnje koji su omogućeni na osnovu reciprociteta, kao i na osnovu domaćeg zakonodavstva.

Ovo stoga što odredbe Konvencije u ovom poglavlju ne nadjačavaju odredbe međunarodnih sporazuma o međunarodnoj pomoći u krivičnim stvarima, ekstradiciji, reciprocitetu, kao i odredbe nacionalnih zakonodavstava koje regulišu međunarodnu saradnju.

Potrebno je, u ovom kontekstu, još jednom naglasiti da su računarski podaci vrlo osetljivi, te da, uz nekoliko pritisaka na računarsku tastaturu ili usled izvršenja automatskog programa, navedeni podaci mogu biti izbrisani ili na drugi način trajno uništeni, čime bi identifikacija izvršioca krivičnog dela ili upotreba možda kritičnog dela dokaznog materijala kojim bi se dokazalo postojanje krivičnog dela i krivičnopravna odgovornost njegovog počinioca, bila onemogućena. Neki oblici računarskih podataka bivaju pohranjeni samo u vrlo kratkom vremenskom periodu pre nego što budu obrisani, tj. na drugi način učinjeni trajno nedostupnim. U drugim slučajevima, značajna šteta može biti pričinjena kako ljudima, tako i imovini, ukoliko ova vrsta dokaza ne bude prikupljena vrlo brzo.

U takvim hitnim slučajevima, mora se omogućiti i izvršiti hitno slanje zahteva i odgovora. Iz tog razloga, od presudne važnosti je omogućavanje ubrzavanja procesa ostvarivanja međunarodne pravne pomoći u krivičnim stvarima, upravo u cilju izbegavanja gubitaka kritičnih informacija ili dokaza, koji bi, koji bi, bez ovakve vrste i

vrste i načina postupanja i izvršenja, bili izloženi opasnosti brisanja, tj. nepovratnog gubitka.

Činjenica je da, kroz tzv. tradicionalni način pružanja međunarodne pravne pomoći, komunikacija između nadležnih državnih organa, čak i u realnosti informatičkog ili postinformatičkog društva današnjice, i dalje dosta sporo teče, te da je u najvećem broju slučajeva razmena pismene dokumentacije ili dokumentacije kroz diplomatske kanale ili poštanski sistem vrlo spora, te da zahteva korišćenje složenih međunarodnih procedura. Ovakav način pružanja međunarodne pravne pomoći u oblasti visokotehnološkog kriminala praktično predstavlja jednu od glavnih, ako ne i glavnu prepreku uspešnom krivičnom gonjenju u ovoj oblasti kriminaliteta.

Iz tih razloga, ističe se neophodnost pružanja međunarodne pravne pomoći na način kao što je to navedeno, tj. omogućavanje da ista bude vrlo brzo postignuta kroz primenu takvih mera koje će biti predviđene ne samo kroz samu Konvenciju, već i kroz bilateralne i multilateralne sporazume o krivičnopravnoj saradnji, domaće zakonodavstvo, kao i kroz druge oblike regulisanja pravne pomoći u ovoj oblasti.

Iz tih razloga, korišćenje modernih sredstava komunikacije, kao što su elektronska pošta, faks, VOIP komunikacija, video-konferencije, upotreba direktne komunikacije i razmene podataka putem mobilnih uređaja koji koriste internet-okruženje, itd. postavlja se kao uslov bez kog se ne može postići željeni cilj.

Posebno je bitno naglasiti neophodnost praćenja razvoja informaciono-komunikacionih tehnologija i njihovo iskorišćavanje radi što brže razmene podataka i komuniciranja prilikom ostvarivanje međunarodne saradnje, posebno imajući u vidu činjenicu da će izvršioci krivičnih dela, u svakom slučaju, imati dovoljno motiva i energije da upravo najsavremenije oblike informaciono-komunikacionih tehnologija iskoriste za izvršenje krivičnih dela.

U okviru regulisanja međunarodne pravne pomoći u krivičnim stvarima, a koje se odnose na borbu protiv visokotehnološkog kriminala, posebnu ulogu zauzima postojanje tzv. „7/24 mreže“, koja predstavlja mrežu kontakt-tačaka među zemljama koje su ratifikovale Konvenciju; ove tačke se u najvećem broju slučajeva nalaze pri ministarstvima unutrašnjih poslova i javnim tužilaštvima, a ređe u ministarstvima pravde određenih zemalja. S tim u vezi, jasno je da ova mreža predstavlja brz odgovor na prethodno navedenu potrebu za efektivnom borbom protiv krivičnih dela koja su počinjena korišćenjem računarskih sistema i računara, kao i efektivno prikupljanje dokaza u elektronskoj formi.

Bitno je imati u vidu da radnje koje mi preduzimamo za tastaturom našeg računara, na primer, u toku radnog vremena, skoro momentalno imaju posledice na računarima koji se nalaze možda desetinama hiljada kilometara daleko i u različitim vremenskim zonama. Iz ovih razloga, postojanje već navedene klasične, tj. standardne saradnje i modaliteta saradnje u međunarodnoj pravnoj pomoći u krivičnim stvarima zahteva dodatne kanale komunikacije i saradnje upravo radi davanja odgovora svim ovim izazovima koje donosi informatičko i

informatičko i postinformatičko doba. Dobra iskustva grupe „G 8-“, koja je takođe za potrebe saradnje te grupe zemalja formirala sličnu „7/24 mrežu“ kontakata i saradnje, ukazala su na mogućnost uspostavljanja takvog modaliteta direktne saradnje u hitnim slučajevima na osnovu, kao i u okvirima ove Konvencije Saveta Evrope.

Članom 35. ove Konvencije svaka zemlja koja ju je ratifikovala ima obavezu da odredi kontakt-tačku, koja će biti na raspolaganju 24 časa dnevno, 7 dana u nedelji, tokom cele godine, radi omogućavanja hitnog, tj. momentalnog odgovora i pomoći u istragama, kao i procedurama međunarodne pravne pomoći. Zemlje koje su ratifikovale Konvenciju složile su se da uspostavljanje ovakve vrste povezivanja, tj. mreže, predstavlja jedan od najbitnijih elemenata po svojoj važnosti u smislu sredstava koja su na raspolaganju zemljama radi primene Konvencije i omogućavanja efektivnog odgovora organa otkrivanja, organa gonjenja i sudova na izazove koje nam donosi savremeni računarski kriminalitet.

S tim u vezi, „7/24“ kontakt-tačke moraju biti osposobljene da direktno i samostalno ili direktno uz saradnju drugih nadležnih organa zemlje članice pruže tehnički savet, čuvanje i pribavljanje podataka, pribavljanje dokaza, davanje pravnih informacija, kao i identifikaciju i lokaciju na kojoj se nalazi osumnjičeno lice.

Zemlje koje su ratifikovale Konvenciju zadržavaju slobodu da odrede gde će navedena kontakt-tačka biti uspostavljena. Najbolje rezultate, u okviru do sada uspostavljene prakse, pružaju kontakt-tačke koje su, na prvom mestu, uspostavljene u javnim državnim tužilaštvima, a nakon toga i u ministarstvima unutrašnjih poslova, a tek na kraju kontakt-tačke pri drugim agencijama ili ministarstvima pravde.

Razlog uspešnosti saradnje državnih, tj. javnih tužilaštava leži u tome što se u skoro svim zemljama koje su sada ratifikovale ovu Konvenciju primenjuju odredbe Zakonika o krivičnom postupku, koje omogućavaju državnim tužiocima vođenje tzv. „tužilačke istrage“, koja menja klasičan koncept istrage i sprovođenje istrage od strane istražnog odeljenja - istražnog sudije suda, čime se, sa jedne strane, znatno ubrzava vođenje krivične istrage, dok sa druge strane, imajući u vidu kvalitet državnih tužilaštava u smislu njihovog autonomnog ili nezavisnog položaja u okviru pravosudne grane vlasti, omogućava da tužilaštva kroz svoje radnje kontrolišu radnje i mere koje pripadnici ministarstava unutrašnjih poslova primenjuju.

Ovo posebno stoga što se u stavu 2. člana 35. Konvencije navodi da je jedan od ključnih zadataka kontakt-tačaka ove mreže upravo mogućnost uspostavljanja brzog izvršenja onih funkcija i zadataka koji su neophodni radi brzog postupanja u ovoj krivično pravnoj materiji. Na primer, ukoliko je kontakt-tačka „7/24“ određena policijska jedinica, ona mora imati mogućnost da brzo koordinira rad sa svim drugim relevantnim i nadležnim organima u okviru krivičnopravnog sistema svoje zemlje, kao što su, na primer, ovlašćeno ministarstvo za izvršavanje međunarodne pravne pomoći, javno tužilaštvo itd., radi postizanja pravovremene i pravilne reakcije na određeni međunarodni zahtev, koji može biti ispostavljen u bilo koje doba dana ili noći. Takođe, ne treba

zanemariti ni potrebu da kontakt-tačka ima takav kapacitet da na najbrži mogući način izvrši komunikaciju sa drugim članicama, tj. drugim kontakt-tačkama ove mreže na najbrži mogući način.

5. Direktiva 40/2013/EU

Direktivu 40/2013/EU doneo je Evropski parlament 20. avgusta 2013. godine, a odnosi se na napade usmerene protiv informacionih sistema. Direktiva menja Okvirnu odluku Saveta 222/2005/JHA i predstavlja sastavni deo tzv. „acquis communautaire" – zajedničkog pravnog okvira zemalja članica Evropske unije.

Cilj Direktive je da približi krivičnim zakonodavstvima zemalja članica Unije oblast napada protiv informacionih sistema uspostavljanjem minimalnih pravila koja se odnose na definiciju krivičnih dela i odgovarajućih krivičnopravnih sankcija, da unapredi saradnju između nadležnih organa koji uključuju pripadnike policije, drugih specijalizovanih agencija za sprovođenje zakona članica Unije i nadležnih specijalizovanih agencija i tela same Evropske unije, kao što su EUROJUST, EUROPOL i njegov Evropski centar za računarski kriminal (EC 3), kao i da omogući uključivanje u rad Evropske agencije za mrežnu i informatičku sigurnost (ENISA).

Informacioni sistemi u okviru ove Direktive identifikovani su kao ključan element političke, društvene i ekonomske interakcije u samoj Uniji. Društva su trenutno veoma zavisna od navedenih sistema, a ta zavisnost će ubuduće sve više rasti. Neometana upotreba, kao i njihova sigurnost u okviru zemalja članica Unije, od vitalnog interesa je za razvoj, kako internih tržišta tako i moderne, inovativne i kompetitivne tržišne ekonomije. Ovakve vrste napada predstavljaju pretnju postizanju sigurnijeg informatičkog društva kao cilja, te predstavljaju pretnju i oblasti sloboda, sigurnosti i pravde. Iz tih razloga, zahtevaju odgovor na nivou Evropske unije kroz unapređenje saradnje i koordinacije na međunarodnom nivou.

Činjenica je da postoji veliki broj objekata u fizičkom ili softverskom obliku koji predstavljaju delove kritične infrastrukture, te bi prekidanje rada ili uništenje ovakve vrste infrastrukture imalo za posledicu nanošenje značajne štete, i žiteljima i njihovoj imovini. Postalo je jasno da postoji potreba da se kritična infrastruktura definiše kao sredstvo, sistem ili deo sredstava iz sistema, koji su esencijalni za održavanje vitalnih društvenih funkcija, kao što su zdravlje, sigurnost, ekonomska ili društvena dobrobit naroda. Sistemi kao što su elektrane, transportne mreže ili mreže komunikacija u službi vlada država ključno je zaštititi, pošto bi njihovo narušavanje ili uništenje dovelo do, sasvim izvesno, i katastrofalnih posledica.

Postoje dokazi koji ukazuju na tendenciju rastuće opasnosti i ponavljanja napada u velikom obimu i snazi koji su usmereni protiv informatičkih sistema, a koji su od kritičnog značaja za zemlje članice Unije. Ova tendencija je propraćena i razvojem sofisticiranih metoda, kao što su proizvodnja i korišćenja tzv. „bot-netova",

", koji uključuju nekoliko nivoa izvršenja krivičnog dela, gde svaki od tih nivoa može predstavljati značajan rizik za javni interes.

Ova Direktiva, između ostalog, uvodi krivične sankcije za novo krivično delo u vidu pravljenja i korišćenja tzv. „bot-netova", kao čin uspostavljanja udaljene kontrole nad značajnim brojem računara putem inficiranja istih kroz instalaciju malicioznog softvera, a kroz precizno usmerene „sajber"- napade. Jednom kada se kreira, takva mreža konstituiše „bot-net", koji može biti aktiviran bez znanja i pristanka vlasnika, tj. korisnika računara radi otpočinjanja napada u širokom obimu i zahvatu, koji obično ima takav kapacitet, tj. mogućnost i snagu da izazove znatnu štetu na način kao što je to opisano u Direktivi.

Ovakve vrste velikih i širokih napada mogu izazvati značajnu ekonomsku štetu, kako kroz prekidanje rada informacionih sistema i komunikacija, tako i kroz gubitak ili izmenu komercijalno bitnih poverljivih informacija i podataka. Posebna pažnja treba da bude usmerena ka podizanju svesti malih i srednjih preduzeća u cilju identifikacije ovakve vrste opasnosti, kao i ranjivosti tih preduzeća u ovom smislu, a kroz njihovu se veću zavisnost od informacionih sistema. Bitno je naglasiti i da ova Direktiva propisuje visinu krivičnih sankcija, tj. barem za ona krivična dela koja se ne smatraju manje društveno opasnim.

Države članice Unije mogu propisati šta predstavlja manje društveno opasna dela u skladu sa njihovim nacionalnim zakonodavstvima i praksom. Na primer, krivično delo u tom smislu može biti nanošenje štete integritetu računara, računarskih sistema i podataka u takvoj meri i na takav način koji ne prelazi određeni prag krivičnopravne odgovornosti koja zahteva reakciju organa otkrivanja i gonjenja u okviru krivičnog postupka.

S druge strane, Direktiva, posebno u oblasti napada protiv informacionih sistema, zahteva efektivno, proporcionalno i dovoljno odvraćajuće krivičnopravne sankcije i njihovu visinu, kao i unapređenje saradnje među pravosudnim i drugim nadležnim organima, a a što sve ne mogu postići zemlje članice ponaosob, već bi trebalo da bude postignuto na nivou same Evropske Unije; iz tih razloga, Unija može ostvariti takve vrste mera koje su u skladu sa principom supsidijariteta, koji je propisan članom 5. Ugovora o Evropskoj uniji.

Direktiva 40/2013/EU u članu 2. daje značenje pojmova i izraza:

- „Pravno lice" predstavlja subjekat koji ima status pravnog lica prema primenjivom pravu, ali ne obuhvata države, tj. državne ili javne organe, institucije ili tela koja postupaju u ime države, kao ni javne međunarodne organizacije.

- „Bespravan“ označava postupak iz ove Direktive, uključujući pristup, ometanje ili presretanje, bez dozvole vlasnika ili drugog nosioca određenog prava na sistemu ili njegovom delu, ili koji domaće zakonodavstvo ne dopušta.

U svom tekstu, Direktiva daje elemente bića krivičnih dela, kao što su neovlašćeni pristup informacionom sistemu, neovlašćeno ometanje sistema, neovlašćeno ometanje podataka, korišćenje sredstava za izvršenje ovih krivičnih dela.

Posebno je potrebno naglasiti da u članu 9, koji se odnosi na vrstu i visinu sankcija, Direktiva obavezuje zemlje članice Evropske unije da u okviru svojih domaćih zakonodavstava uvedu krivične sankcije koje su efektivne, proporcionalne i dovoljno odvraćajuće u odnosu na izvršioce krivičnih dela.

S tim u vezi, Direktiva predviđa obavezu da za navedena krivična dela bude zaprećena maksimalna kazna zatvora koja ne može biti kraća od 2 godine, i to za krivična dela koja se ne smatraju manje društveno opasnim.

Takođe, za krivična dela neovlašćenog ometanja sistema i neovlašćenog ometanja podataka, kada su učinjena sa umišljajem, moraju biti zaprećena maksimalnom kaznom zatvora koja ne može biti kraća od 3 godine, kada je došlo do značajnijeg oštećenja informacionog sistema i njihovog broja kroz korišćenje alata na koje se odnosi član 7. Direktive, tj. uređaja i programa koji su dizajnirani ili adaptirani prevashodno u tu svrhu.

Takođe, za krivična dela iz članova 4. i 5. Direktiva predviđa da treba biti zaprećena, tj. propisana najviša kazna od najmanje 5 godina zatvora u slučajevima:

- kada je ova krivična dela izvršila kriminalna organizacija, kako je definisana Okvirnom odlukom 841/2008/JHA, bez obzira na kaznu koja je propisana za samu organizaciju;
- ukoliko je izvršenje krivičnog dela načinilo ozbiljnu štetu, ili
- ukoliko je krivično delo izvršeno protiv informacionog sistema kritične infrastrukture.

U članu 17. Direktiva obavezuje Evropsku komisiju da do 4. septembra 2017. godine podnese izveštaj Evropskom parlamentu i Savetu, u okviru koji će sadržavati procenu primene ove Direktive u zemljama članicama u smislu preduzimanja mera na primeni Direktive i, zavisno od situacije, upućivanja zakonskih predloga u proceduru. Isto tako, Komisija je dužna da uzme u obzir tehnička i zakonodavna kretanja u oblasti sajber-kriminala, naročito imajući u vidu predmet ove Direktive.

6. Normativni i institucionalni okvir u Srbiji

6.1. Zakonodavni okvir u Srbiji (*)

Zakon o potvrđivanju konvencije o „cyber" kriminalu (2009) predvideo je uvođenje adekvatnih instrumenata kada je reč o procesnim odredbama, kako bi se stvorila osnova za istraživanje i procesuiranje ovih krivičnih dela, ustanovljavanje brzih i efikasnih institucija i procedura međunarodne saradnje. Takođe, predviđeno je osnivanje kontakt-tačke ili tački „7/24 mreže", koja bi služila kao podrška policijskim i drugim organima zemalja koje su ratifikovale Konvenciju, kao kontakt za sva obaveštenja i početna tačka za sve zahteve koji se tiču procesuiranja i istraživanja krivičnih dela visokotehnološkog kriminala.

Zakon o potvrđivanju Protokola uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema (2009) predviđa inkriminisanje akata rasističke i ksenofobične prirode počinjenih putem računarskih sistema. Njegova osnovna svrha je da se inkriminišu ponašanja koja nisu obuhvaćena Konvencijom, a koja se tiču širenja mržnje, netolerancije i netrpeljivosti prema rasnim, nacionalnim, verskim i drugim grupama i zajednicama korišćenjem računara kao sredstva komunikacije i širenja propagande.

Zakon o potvrđivanju Fakultativnog protokola uz Konvenciju o pravima deteta o prodaji dece, dečjoj prostituciji i dečjoj pornografiji (2002) predviđa, pored ostalog, obavezu ustanovljavanja mera zaštite prava deteta u krivičnom postupku, mere za obezbeđenje odgovarajuće obuke, posebno pravne i psihološke, za lica koja rade sa žrtvama nezakonitih radnji zabranjenih prema ovom zakonu, i propisuje obavezu ustanovljavanja mera kako bi se zaštitili bezbednost i integritet lica i/ili organizacija uključenih u sprečavanje i/ili zaštitu i rehabilitaciju žrtava takvih nezakonitih radnji.

Zakon o potvrđivanju Konvencije Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja (2010) reguliše sprečavanje i borbu protiv seksualnog iskorišćavanja i seksualnog zlostavljanja dece, kao i zaštitu prava dece-žrtava seksualnog iskorišćavanja i seksualnog zlostavljanja, te unapređenje nacionalne i međunarodne saradnje u borbi protiv seksualnog iskorišćavanja i seksualnog zlostavljanja dece.

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala predstavlja specifičnost Republike Srbije i primenjuje se radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela protiv bezbednosti računarskih podataka, intelektualne svojine, imovine, privrede i pravnog saobraćaja, kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj primeraka autorskih dela prelazi 2.000 ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara; krivična dela protiv sloboda i prava čoveka

* Zakonodavni okvir bliže će biti razmatran u tekstovima koji slede.

i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, koja se zbog načina izvršenja ili upotrebljenih sredstava mogu smatrati krivičnim delima visokotehnološkog kriminala.

Krivični zakonik Republike Srbije propisuje krivična dela protiv bezbednosti računarskih podataka čije je krivično gonjenje u isključivoj nadležnosti Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala, kao i ostala krivična dela iz nadležnosti ovog tužilaštva, a koja mogu biti učinjena na štetu maloletnih lica. Takođe, definiše značenje izraza od važnosti za visokotehnološki kriminal.

Zakonik o krivičnom postupku utvrđuje pravila čiji je cilj da niko nevin ne bude osuđen, da se učiniocu krivičnog dela izrekne krivična sankcija pod uslovima koje propisuje krivični zakon, na osnovu zakonito i pravično sprovedenog postupka. Bitno je napomenuti da Zakonik propisuje i niz posebnih dokaznih radnji koje se mogu primeniti u krivičnim postupcima protiv učinilaca krivičnih dela iz stvarne nadležnosti Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala. Takođe, definiše značenje izraza od važnosti za visokotehnološki kriminal.

Zakon o elektronskim komunikacijama uređuje uslove i način za obavljanje delatnosti u oblasti elektronskih komunikacija, nadležnosti državnih organa u oblasti elektronskih komunikacija, zaštitu prava korisnika i pretplatnika, bezbednost i integritet elektronskih komunikacionih mreža i usluga, tajnost elektronskih komunikacija, zakonito presretanje i zadržavanje podataka, nadzor nad primenom ovog zakona, mere za postupanje suprotno odredbama ovog zakona, kao i druga pitanja od značaja za funkcionisanje i razvoj elektronskih komunikacija u Republici Srbiji.

Zakon o odgovornosti pravnih lica za krivična dela uređuju uslove odgovornosti pravnih lica za krivična dela, krivične sankcije koje se mogu izreći pravnim licima i pravila postupka u kojem se odlučuje o odgovornosti pravnih lica, izricanju krivičnih sankcija, donošenju odluke o rehabilitaciji, prestanku mere bezbednosti ili pravne posledice osude i izvršenju sudskih odluka.

Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima uređuje postupak pružanja međunarodne pravne pomoći u krivičnim stvarima u slučajevima kada ne postoji potvrđeni međunarodni ugovor, ili kada određena pitanja njime nisu uređena.

Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine uređuje posebna ovlašćenja organa državne uprave i organizacija koje vrše javna ovlašćenja radi efikasne zaštite prava intelektualne svojine u skladu sa propisima kojima se uređuje pravo intelektualne svojine.

6.2. Podzakonski akti

Pravilnik o uslovima za pružanje internet-usluga i ostalih usluga prenosa podataka i sadržaju odobrenja, koji je u okviru svojih nadležnosti usvojila Republička agencija za telekomunikacije, propisuje osnovne tehničke i druge uslove za pružanje internet-usluga i ostalih usluga prenosa podataka, kao i način izdavanja i sadržaj odobrenja za obavljanje ove delatnosti.

7. Institucionalni okvir

Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala iz 2005. godine osnovano je **Posebno tužilaštvo za borbu protiv visokotehnološkog kriminala**. Ovo tužilaštvo nadležno je za krivično gonjenje učinilaca krivičnih dela visokotehnološkog kriminala i nadležno je da postupa na celoj teritoriji Republike Srbije.

Shodno odredbama navedenog zakona, za postupanje u predmetima visokotehnološkog kriminala nadležan je **Viši sud u Beogradu** za teritoriju Republike Srbije, a za odlučivanje u drugom stepenu nadležan je Apelacioni sud u Beogradu.

Takođe, odredbom Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, u okviru Ministarstva unutrašnjih poslova, Službe za borbu protiv organizovanog kriminala, obrazovano je **Odeljenje za borbu protiv visokotehnološkog kriminala,** koja postupa po nalozima Posebnog tužioca za visokotehnološki kriminal.

Značajnu ulogu u ovoj oblasti ima i **Ministarstvo spoljne i unutrašnje trgovine i telekomunikacija**, tako što doprinosi usklađivanju domaćih propisa u oblasti elektronskih komunikacija sa odgovarajućim propisima Evropske unije; preduzima mere za podsticanje istraživanja i razvoja u oblasti elektronskih komunikacija, u saradnji sa ministarstvom nadležnim za poslove razvoja i unapređenja naučnoistraživačke delatnosti;

Republička agencija za elektronske komunikacije (RATEL), osnovana Zakonom o elektronskim komunikacijama, predstavlja samostalnu organizaciju sa svojstvom pravnog lica, koja vrši javna ovlašćenja u cilju efikasnog sprovođenja utvrđene politike u oblasti elektronskih komunikacija, zaštite interesa korisnika elektronskih komunikacija i nadležna je za saradnju sa nadležnim regulatornim i stručnim telima država članica Evropske unije i drugih država radi usaglašavanja prakse primene propisa iz oblasti elektronskih komunikacija i podsticanja konkurencije elektronskih komunikacionih mreža i usluga, unapređivanja njihovog kapaciteta,

odnosno kvaliteta, doprinosa razvoju tržišta elektronskih komunikacija i zaštite interesa korisnika elektronskih komunikacija

Takođe, učestvuje u radu međunarodnih organizacija i institucija u oblasti elektronskih komunikacija u svojstvu nacionalnog regulatornog tela u oblasti elektronskih komunikacija.

Republička radiodifuzna agencija (RRA) osnovana je Zakonom o radiodifuziji, kojim se uređuju uslovi i način obavljanja radio-difuzne delatnosti u skladu sa međunarodnim konvencijama i standardima, kojim se dalje utvrđuju uslovi i postupak za izdavanje dozvola za emitovanje i uređuju druga pitanja od značaja za oblast radiodifuzije.

8. Savremeni trendovi

Pored svih specifičnosti koje računarski kriminal sadrži zbog svoje uske povezanosti sa tehnološkom sadržaocem, još jedan aspekt ga dodatno čini raznovrsnijim i složenijim u odnosu na standarde oblike kriminogenog ponašanja. Naime, za razliku od „klasičnih“ krivičinih dela, kod kojih način izvršenja ostaje, u najvećem broju slučajeva, isti kroz duži vremenski period, ili se vrlo teško menja, računarski kriminal u vrlo kratkom vremenskom periodu, praktično iz godine u godinu, može doživeti vrlo drastične promene ne samo načina izvršenja pojedinih dela, već i potpunu izmenu same supstance koja čini krivična dela sadašnjice ili bliske budućnosti.

Prilikom kratkog osvrta na početke računarskog kriminaliteta u Republici Srbiji, konstatovali smo da je prisutan više od 40 godina i da je, u decenijama koje su usledile, skoro dekadno doživljavao određene izmene, kako u motivaciji, tako i načinu izvršenja. Čini se da se zakonitosti „Murovog zakona“ („broj tranzistora u integrisanom računarskom kolu svake dve godine biva dupliran“) skoro mogu primeniti, u određenom smislu, i na svet računarskih krivičnih dela. Naime, za razliku od ranijeg perioda, u poslednjih nekoliko godina trendovi izvršenja krivičnih dela značajno češće se menjaju kako u svojim osnovnim, tako i u svojim pratećim oblicima, sledeći ponajviše put kojim svetska tehnologija i ekonomija idu.

Imajući navedeno u vidu, čini se da su brzina razvoja računarskih i komunikacionih tehnologija i ekonomskih kretanja direktno proporcionalna razvoju, trendu i obimu izvršenja krivičnih dela računarskog, tj. „cyber“ kriminala.

Trendovi izvršenja krivičnih dela u poslednjih nekoliko godina na svetskom i domaćem nivou mogu se podeliti u sedam glavnih pravaca:

1. računarski kriminal na mobilnim platformama,
2. intenzivno korišćenje bankarskih „malware"-a i „trojanaca",
3. „haktivizam" i zloupotreba društvenih mreža,
4. savremene povrede prava intelektualne svojine,
5. porast ciljanih napada („APT – Advanced Persistent Threat";
6. pojava i zloupotreba kripto- valuta (Bitcoin, Ethereum, Ripple);
7. pojava i zloupotreba interneta stvari („IoT", „Internet of Things").

8.1. Računarski kriminal na mobilnim platformama

Omasovljenje upotrebe mobilnih računarskih platformi ima svoju uzlaznu putanju još od pojave prvih mobilnih računara tokom sedamdesetih i osamdesetih godina prošlog veka u vidu tzv. „laptop", „notebook", „handheld", „palmtop" i drugih varijanti manjih računarskih uređaja koji su mogli biti lako transportovani, vrlo često i u džepovima odeće. Prava eksplozija prisustva i korišćenja ovakvih uređaja nastaje pojavom prvog „smartphone"-a u vidu Apple Inc. iPhone mobilnog telefonskog uređaja, koji u isto vreme ima i značajne računarske kapacitete. Svet današnjice se praktično ne može zamisliti bez prisustva „pametnih" mobilnih telefona, koji su, u stvari, mali računarski uređaji koji se prevashodno koriste za računarsku, a manje prvobitnu namenu, tj. obavljanje telefonskih razgovora.

Ovakav trend, naravno, nije ostao nezapažen u kriminogenim sredinama, pa su tako zabeleženi značajni prodori izvršenja i raznorodnih krivičnih dela putem korišćenja ovih mobilnih uređaja na različite načine. Posebno treba naglasiti postojanje raznih vrsta malicioznog softvera (virusa, trojanaca, vormova, itd.), koji se mogu instalirati na operativnim sistemima modernih mobilnih telefona, i koji imaju različite funkcije: od prostog kopiranja brojnih baza podataka koje oštećeni poseduju na svojim uređajima (lista telefonskih kontakata, elektronska pošta, SMS, fotografije, video zapisi, poruke na društvenim mrežama, itd.), praćenja kretanja korisnika uređaja u realnom vremenu i posmatranja putem zloupotrebe kamere i mikrofona okruženja u kome se aparat, tj. korisnik nalaze, do uticaja na novčane transakcije koje oštećeni putem tzv. „mobilnih aplikacije" čine pomoću svog uređaja.

8.2. Intenzivno korišćenje bankarskih „malware“-a i „trojanaca“;

Računari i mobilni računarski uređaji postali su sastavni deo poslovanja pravnih i fizičkih lica današnjice. Skoro je nemoguće zamisliti bavljenje ili obavljanje mnogih poslova bez upotrebe računara. Ovo je posebno vidljivo kada govorimo o oblasti u kojoj su računaru „domaći“, tj. u oblasti računanja matematičkih izraza, a koji su dalje sastavni deo poslovanja finansijskih institucija u javnom i privatnom sektoru. Naravno, imajući u vidu značajan potencijal za sticanje protivpravne dobiti, ovo polje korišćenja računara postalo je jedno od omiljenih i za kriminalnu zloupotrebu.

Zeus, Citadel, SpyEye, WannaCry i sl., samo su neki od naziva različitih „malware“-a koji su nastali poslednjih godina radi instaliranja, bez znanja korisnika računara, na njihove uređaje u cilju pribavljanja i zloupotrebe finansijskih podataka protivpravnim preuzimanjem kontrole nad bankarskim računima oštećenih i novčanim transakcijama u korist izvršilaca krivičnih dela. Poslednji primeri tzv. „BEC – Business E-mail Compromise“ slučajeva u kojima su stotine hiljada, pa i milioni evra, preusmereni na prevarne račune pod kontrolom kriminalaca radi ostvarivanja enormnih kriminalnih profita, ukazuju na dalji pravac razvoja ekonomskih krivičnih dela i sve veću upotrebu informacionih tehnologija radi njihovog izvršenja.

8.3. „Haktivizam“ i zloupotreba računarskih mreža

Prema slobodnim izvorima “haktivizam”(*) predstavlja subverzivnu upotreba računara i računarskih mreža za promovisanje političke agende ili socijalnih promena. Sa korenima u kulturi hakera i hakerskoj etici, njegovi ciljevi često su povezani sa slobodom govora, ljudskim pravima ili pokretima koji promovišu slobodan protok informacija. Termin je ušao u upotrebu 1994. godine. Primetno je da postoje razlike u bližem određivanju ove vrste aktivizma na internetu. Dok neke definicije podrazumevaju akte sajber-terorizma (“Anonymous”), druge pokušavaju da daju opravdanje upotrebi neovlašćenog pristupa računarima da bi se izvršile društvene promene. Ipak, «haktivizam» u najvećem broju slučajeva predstavlja radnje usmerene na zlonamerne i destruktivne radnje pojedinaca koje, u stvari, podrivaju bezbednost interneta kao tehničke, ekonomske i društvene platforme.

Zloupotrebe računarskih mreža u proteklih nekoliko godina dobile su svoje novo težište na takozvanim „društvenim mrežama“, tj. stalno aktivnim globalnim računarskim programima koji omogućavaju direktnu komunikaciju korisnika putem razmene poruka, foto i video-materijala, glasa, itd. Porast zloupotrebe ovih mreža sa ciljem zastrašivanja, iznuđivanja željenog ponašanja, kao i zloupotrebe u pornografske svrhe poprima zabrinjavajuće razmere u našoj zemlji, o čemu će biti detaljnije reči u tekstu ovog priručnika.

* https://en.wikipedia.org/wiki/Hacktivism

8.4. Savremene povrede prava intelektualne svojine

Povrede prava intelektualne svojine, u krivičnopravnom smislu, spadaju u grupu krivičnih dela koja su dobro poznata javnim tužiocima, zamenicima javnih tužilaca i sudijama. Može se slobodno konstatovati da je upravo izvršenje ovih krivičnih dela tokom devedesetih godina prošlog, i početkom ovog veka, posebno kroz zloupotrebu računara i računarskih tehnologija za masovno kopiranje i nelegalnu prodaju autorskih sadržaja, kao što su filmovi, muzika i računarskih programi, i dovelo do početka ozbiljnijeg posvećivanja pažnje računarskom kriminalitetu.
Ipak, prema procenama Američke privredne komore(*) u Republici Srbiji, do 2015. godine zabeležen je pad neovlašćene upotrebe autorskih prava u oblasti računarskih programa na %67. Naravno, taj procenat nikako nije zadovoljavajući, imajući u vidu da u zemljama Evropske unije iznosi oko %29, i obavezuje na dalje delovanje državnih organa.
Posebnu pažnju treba skrenuti na prodaju, putem interneta, falsifikovanih lekova i medicinskih preparata. Trend kupovine ovih proizvoda putem računarskih mreža je u uzlaznoj liniji, ali su zabeleženi značajni slučajevi prodaje nelegalnih kopija medikamenata putem internet-oglašavanja i dostavljanja na kućnu adresu. U nekim slučajevima, došlo do ugrožavanja života lica koja su konzumirala ove preparate usled delovanja na organizam supstanci od kojih su bili napravljeni. Nažalost, u svetu su zabeleženi i smrtni slučajevi usled ovakvog pribavljanja i konzumacije.

8.5. Porast ciljanih napada – Advanced Persistent Threat („APT“)

Ciljani napadi predstavljaju novi oblik izvršenja krivičnih dela u čijoj osnovi se nalazi takozvani „socijalni“ tj. društveni inženjering. Glavne odlike izvršenja ovih krivičnih dela su da njihovi izvršioci na svom raspolaganju imaju široki spektar programskih alata i zlonamernih programa, putem kojih se infiltriraju i preuzimaju kontrolu nad ciljanim računarom i mrežom, ili vrše prismotru tih sistema radi pribavljanja podataka koji nisu javni. Takođe, ciljani napadi se mogu okarakterisati i kao uporni iz razloga što se jednom ostvaren uvid i kontrola nad računarskim procesima mete – žrtve ne napušta, već koristi do momenta otkrivanja. Ponekad se koristi i dodatni atribut ovih napada u smislu pretnje koju stvaraju, imajući u vidu postojanje specifičnog cilja, obuke, motivisanosti, organizovanosti i postojanja izvora finansiranja.
Trenutno najprisutniji načini izvršenja ovakve organizovane kriminalne akcije mogu se videti u ranije spomenutim predmetima „BEC“ prevara, gde cilj predstavlja presretanje i kontrola poslovnih komunikacija između dva i/ili

* https://www.amcham.rs

Trenutno najprisutniji načini izvršenja ovakve organizovane kriminalne akcije mogu se videti u ranije spomenutim predmetima „BEC“ prevara, gde cilj predstavlja presretanje i kontrola poslovnih komunikacija između dva i/ili više poslovnih entiteta radi preusmeravanja procesa plaćanja na prevarne račune. U tom kontekstu, privreda Republike Srbije u proteklih nekoliko godina doživela je štetu u stotinama miliona dinara.

8.6. Pojava i zloupotreba kripto-valuta (Bitcoin, Ethereum, Ripple, itd);

Kripto-valute predstavljaju računarsko programsko digitalno sredstvo dizajnirano radi upotrebe kao sredstvo plaćanja ili razmene dobara i usluga, gde se kriptografija koristi za osiguranje transakcija i kontrole stvaranja dodatnih jedinica valute. Kripto-valute su klasifikovane kao podskup digitalnih i alternativnih valuta. “Bitcoin” predstavlja prvu poznatu kripto-valutu, koja je nastala 2009 godine. Bitcoin i njegovi derivati koriste decentralizovanu kontrolu nasuprot centralizovanim elektronskim novčanim i bankarskim sistemima. Naime, kripto-valute ne predstavljaju novac koji izdaje centralna bankarska institucija određene zemlje, već računarski podatak koji se stvara korišćenjem određenih programa koji se koriste na internetu i koji se čuva u isključivo elektronskom obliku prolazeći kroz niz različitih provera korisnika interneta koji učestvuju u tim transakcija, s obzirom da ove vrste valuta ne postoje u “pravom”, tj. štampanom ili kovanom obliku.

Kripto-valute se koriste na različite načine i danas je moguće elektronskim putem kupiti veliki broj dobara i usluga na internetu ovim “virtuelnim novcem”. Ipak, bitno je naglasiti da i pored jake promocije ovih valuta od strane “boraca za slobode i privatnost interneta”, kriminalci i kriminalne grupe od samog njihovog nastanka intenzivno koriste ovakav vid plaćanja imajući u vidu poteškoće sa kojim se državni organi suočavaju prilikom praćenja ovih transakcija i zaplene kripto-valuta.

Posebno treba spomenuti da na manje pristupačnim delovima interneta, kao što su “Deep” ili “Dark Web”, korišćenje ovih valuta predstavlja pravilo prilikom kupoprodaje narkotika, vatrenog oružja, trgovine ljudima i dečijom pornografijom, pa čak i prilikom naručivanja ubistava.
Interesantan je podatak da u Republici Srbiji, pored značajne zajednice tzv. “Bitcoin miner-a”, kao i upotrebe ove kripto-valute za razmenu dobara i usluga, u skladu sa svetskim trendovima postoji i nekoliko tzv. “Bitcoin ATM”, tj. automata za razmenu ove valute za dinare ili njenu kupovinu prodajom dinara.

8.7. Pojava i zloupotreba interneta stvari („IoT“, „Internet of Things“)

Internet stvari predstavlja međusobno umrežavanje fizičkih objekata, vozila (što se odnosi i na „povezane” i „pametne uređaje”), zgrada i drugih stvari sa ugrađenom elektronikom, programima, senzorima, koji predmetima omogućavaju da razmenjuju podatke sa proizvođačem, operaterom i/ili drugim povezanim uređajima.. Global Standards Initiative on Internet of Things (IoT-GSI) definisala je IoT kao „globalnu infrastrukturu informatičkog društva koja omogućava napredne usluge (fizičkim i virtualnim) umrežavanjem stvari, pri tom se zasnivajući na postojećim i interoperabilnim informacionim i komunikacionim tehnologijama u razvoju”. U tu svrhu, termin „stvar” predstavlja „predmet fizičkog sveta (fizičkih stvari) informacija, ili reč (virtualne stvari), koji je moguće identifikovati i koji može da bude integrisan u komunikacionim mrežama”.

“IoT” omogućava da objekti budu opaženi i kontrolisani daljinski putem postojeće mrežne infrastrukture, čime se stvara prilika za direktniju integraciju fizičkog sveta i računarskih sistema, što rezultuje povećanjem efikasnosti, tačnosti i ekonomske koristi, uz smanjenje ljudske intervencije. Svaku stvar je moguće jedinstveno identifikovati kroz ugrađen računarski sistem i svaka stvar je interoperabilna u okviru postojeće internet-infrastrukture. Stručnjaci procenjuju da će “IoT” do 2020. godine imati između 26 i 30 milijardi predmeta.

U kontekstu ovog priručnika, ova oblast korišćenja računara i računarskih mreža zaista predstavlja budućnost kriminala koja je na pomolu. Načini zloupotrebe mogu biti značajni i primeri koji su već sada zabeleženi u vidu, na primer, daljinske kontrole motornih vozila od strane „hakera“, aktiviranja i kontrole kućnih uređaja koji su povezani na internet, i to onih čijom se zloupotrebom može nadgledati, pa i uticati na događaje koji se odvijaju u određenom prostoru, u ovom slučaju privatnom, ukazuju da posebna pažnja mora biti posvećena ovoj nastupajućoj opasnosti, kao i novim oblicima izvršenja krivičnih dela koji će predstavljati direktan proizvod ovog razvoja tehnologije.

Prvo reagovanje na elektronske dokaze

1. Uvod

U okviru projekta "Spojeni i sigurni – u susret virtuelnoj sredini koja je sigurna za decu" stvorila se potreba za dodatnim usavršavanjem, te je izvršena edukacija nosilaca pravosudnih funkcija u cilju upoznavanja sa prvim reagovanjem na elektronske dokaze(*), koja je pomogla pripadnicima policije i tužilaštva da se upoznaju sa mogućnostima efikasnog sprečavanja i otkrivanja visokotehnološkog kriminala kao novog izazova, umnogome različitog od onih koji su predmet konvencionalnih krivičnih istraga.

Savremena tendencija prikupljanja elektronskih dokaznih radnji prilikom postupanja policijskih službenika, kako u tradicionalnim krivičnim delima, tako i u krivičnim delima visokotehnološkog kriminala tokom privremenog oduzimanja predmeta inicirala je donošenje ''Obavezne instrukcije o prikupljanju i obezbeđivanju elektronskih dokaza'', kojom se utvrđuje metodologija za prikupljanje elektronskih dokaza tj. njihovo otkrivanje, obezbeđivanje, prikupljanje i evidentiranje u cilju jedinstvenog postupanja policijskih službenika Ministarstva unutrašnjih poslova Republike Srbije sa elektronskim dokazima. Navedena instrukcija predstavlja standard za pravilno rukovanje elektronskim dokazima sa ciljem sprečavanja njihovog oštećenja, gubitka, modifikacije, transporta i osiguranja autentičnosti elektronskih dokaza neophodnih da se obezbedi proglašenje osumnjičenog krivim.

2. Strategija za prikupljanje digitalnih dokaza

U ovo doba tehnološke revolucije, skoro da je nemoguće zamisliti scenario gde ne bi bilo moguće da dokaz ili obaveštajni podatak nisu snimljeni u nekom elektronskom tj. digitalnom obliku. Imajući to na umu, policijski službenici koji zajedno sa tužilaštvom istražuju krivična dela trebalo bi uvek da uzmu u obzir strategiju za prikupljanje elektronskih dokaza od početka svih svojih upita. Najčešći uređaji koji mogu sadržavati elektronske dokaze su: sistemi video nadzora, računarski sistemi, tablet-uređaji, uređaji za skladištenje podataka (hard-diskovi i solid state diskovi SDD, memorijske kartice, USB uređaji za pohranu podataka, optički kompakt diskovi, trake za pohranu podataka, i dr.),

* Elektronski dokaz je bilo koja informacija generisana, obrađena, uskladištena ili prenesena u digitalnom obliku na koju se sud može osloniti kao merodavnu, tj. svaka binarna informacija, sastavljena od digitalnih 1 i 0, uskladištena ili prenesena u digitalnoj formi, kao i druge moguće kopije originalne digitalne informacije koje imaju dokaznu vrednost i na koje se sud može osloniti u kontekstu forenzičke akvizicije, analize i prezentacije, što je saglasno sa čl.112. st. 17. i st. 26. Krivičnog zakonika Republike Srbije („Sl. glasnik RS", br. 2005/88 ,2005/85 - ispr., 2005/107 - ispr., 2014/108 ,2013/104 ,2012/121 ,2009/111 ,2009/72 i 2016/94).

digitalni fotoaparati i video-kamere, digitalni audio-snimači, digitalni video-rekorderi sa memorijskim modulima, igračke konzole, MP3 i MP4 plejeri, GPS uređaji, ruteri, pametni podataka tj. naloga elektronske pošte, podatka koji se odnose na kriptografsku zaštitu, davaoce internet usluga i korišćenja računarskih mreža, skladištenja elektronskih podataka na drugom lokalitetu, i skrivenih uređaja za pohranjivanje podataka.

2.1. Sistemi video-nadzora

Sistemi video nadzora sada preovladavaju na većini javnih mesta. Za sva mesta izvršenja krivičnog dela, uključujući njihove pristupne i odstupne putanje, trebalo bi proveriti da li postoje bezbednosne kamere. Većina sistema video nadzora sačuvaće snimke samo ograničen vremenski period. Da bi se izbegao gubitak dokaza, policijski službenici moraju da preduzmu korake kako bi obezbedili dokaze sa sistema video-nadzora što je moguće pre.

2.2. Podaci iz otvorenog internet-izvora

Informacije koje su važne za istragu mogu biti objavljene na internetu. Ovi podaci se mogu izgubiti ukoliko policijski službenik ne deluje brzo kako bi ih sačuvao. Razlog gubitka ne mora biti eventualno uklanjanje elektronskih dokaza tj. podataka od strane izvršioca ili nekog drugog lica: mogu nestati zbog vremenskog ograničenja trajanja određenog internet-domena ili drugom kriminalnom aktivnošću trećih lica, npr. ubacivanjem malicioznih programa tzv. *ransomvera*(*) koji šifruju podatke na serverima, računarima i drugim uređajima.

2.3. Onlajn korisnički nalozi za skladištenje podataka

Danas je postalo uobičajeno da ljudi skladište svoje elektronske podatke onlajn (*free file hosting sites, cloud computing* (**)), što im daje mogućnost da im pristupe sa bilo kog računara ili drugog uređaja. Često se kopije ovih podataka ne čuvaju na lokalnim računarima. Elektronska pošta, tekstualni dokumenti i fajlovi sa multimedijalnim sadržajima (slike, muzika i video snimci) su tipični primeri. Pristupanje ovim podacima policijskim službenicima često može predstavljati izazov u smislu pribavljanja elektronskih dokaza koji se ne nalaze na fizičkoj lokaciji na kojoj se obavlja računarsko pretraživanje elektronskih podataka.

* Ransomware (u pojedinim slučajevima taj tip malvera označava se i kao kripto-virus, kripto-trojanci ili kripto-crv) obuhvaća klasu malvarea koja ograničava pristup računarskim sistemima koje inficira, te zahteva plaćanje otkupnine (ucene) kreatorima malicioznih programa kako bi ograničenje bilo uklonjeno. Izvor: http://www.nod32.com.hr/ThreatCenter/ThreatTest/tabid/2556/Default.aspx#ransomware

** Tako, na primer, Evropska unija u svom strateškom dokumentu „ Oslobađanje potencijala klaud-kompjutinga u Evropi“ navodi da: „Klaud-kompjuting (Cloud Computing), u pojednostavljenom smislu, može se shvatiti kao čuvanje, obrađivanje i korišćenje podataka koji se nalaze na udaljenim računarima i kojima se može pristupiti preko interneta“. Izvor: http://pravoikt.org/racunarstvo-u-oblacima-cloud-computing-sta-je-i-sto-nas-treba-da-bude-briga/

2.4. Elektronska evidencija i komunikacioni podaci (zadržani podaci)

Internet, telekomunikaciona industrija i druge onlajn organizacije proizvode tokom poslovanja raznu elektronsku evidenciju koja se beleži kroz zadržane podatke, kao što su internet protokol adrese, podaci o saobraćaju, podaci o lokaciji, i dr. Ova evidencija može da bude od neprocenjive važnosti za policijskog službenika i kao dokaz i u smislu obaveštajnih podataka. U nekim slučajevima to će biti jedine informacije koje povezuju osumnjičenog sa krivičnim delom. Ovakve evidencije u skladu sa čl.128. Zakona o elektronskim komunikacijama („Sl. glasnik RS“, br. 2013/60 ,2010/44 - odluka US i 2014/62) čuvaju se 12 meseci od dana obavljene komunikacije, a čl.129. navedenog zakona definisane su vrste zadržanih podataka. Stoga, potrebno je da policijski službenici reaguju brzo da ne bi izgubili dokaze.

2.5. Podaci sa uređaja krajnjeg korisnika

„Uređaj krajnjeg korisnika” je opšti naziv za svaki korisnički proizvod koji se koristi za obradu ili skladištenje elektronskih podataka. Kao što je navedeno, dostupno je mnogo različitih vrsta uređaja krajnjeg korisnika, kao što su: računari, mobilni telefoni, video-kamere, muzički plejeri, Sat-Nav, GPS, optički diskovi, memorijski stikovi, i dr. Svi ovi uređaji mogu da pruže vitalne dokaze, ali se mora poštovati stroga procedura kada se njima rukuje.

Strategija za prikupljanje digitalnih dokaza trebalo bi da uzme u obzir četiri faze:

2.5.1. Obezbeđivanje nestalih dokaza

Što se tiče elektronskih dokaza, prvo što bi policijski službenici morali da imaju na umu je da sačuvaju nestalne dokaze:

- moguće je nasnimiti nešto preko snimaka sistema video nadzora;
- moguće je da podatke objavljene na internetu ukloni njihov autor ili administrator;
- moguće je da evidencija komunikacije bude pročišćena ili preko nje nešto nasnimljeno;
- podaci na uređajima krajnjeg korisnika mogu biti slučajno ili namerno izmenjeni, obrisani ili preko njih nešto nasnimljeno;
- očuvanje se može obezbediti oduzimanjem uređaja koji sadrži prvobitne podatke, uzimanjem kopije tih podataka ili zahtevajući od trećeg lica da ih sačuva za kasniju potrebu.

Policijski službenik mora da bude upoznat sa opštim principima oduzimanja elektronskih dokaza (uvrštenih u ovaj priručnik) kako bi se obezbedilo da ono što preduzme ne ugrozi dokaznu verodostojnost podataka.

2.5.2. Elektronsko traganje

Postoje dva aspekta elektronskog traganja:
- utvrđivanje porekla svake elektronske informacije,
- traganje za osumnjičenima preko njihovih elektronskih otisaka.

Lokardov osnovni princip forenzike: "Svaki kontakt ostavlja trag" istinit je kada su u pitanju računari i internet. Zapravo, u svakom trenutku, kreiranje, modifikovanje ili brisanje elektronskih podataka moći će se dovesti u vezu sa određenim računarom i korisničkim nalogom.

U većini slučajeva, ovo će značiti identifikovanje autora ili kreatora elektronskih podataka preko internet-protokola tj. IP adrese računara koji je korišćen. Za ovo su potrebni i tačan datum i vreme (uključujući vremenske zone) da je informacija zabeležena. Ova informacija može biti dostavljena pružaocima usluga korišćenja internet-mreža (internet-servis provajderima - ISP), koji će utvrditi ime osobe koja je koristila taj internet-nalog. Tradicionalne policijske veštine će i dalje biti neophodne kako bi se osumnjičeni doveo u vezu sa identifikovanim računarom ili internet nalogom.

2.5.3. Pretres i zaplena

Kada se identifikuje osumnjičeni, verovatno će biti potrebno da se pretrese i oduzme elektronski dokaz koji je kod njega. Ovaj priručnik pruža sveobuhvatan vodič za nacionalnu najbolju praksu prilikom pretresanja i oduzimanja elektronskih podatka. Priručnik ističe ključne stvari koje bi tužilaštvo i policijski službenici trebalo da imaju na umu prilikom svakog procesa pretresanja i oduzimanja.

2.5.4. Računarsko-digitalno veštačenje

Kada se oduzmu „uređaji krajnjeg korisnika", potrebno je da idu na digitalno forenzičko veštačenje kako bi se izvukli svi elektronski dokazi u obliku koji je prihvatljiv za sud. Biće potrebno da elektronski dokazi prikupljeni tokom istrage budu protumačeni i predstavljeni tako da oni koji nisu poznavaoci tehnike ili nisu prethodno bili upoznati sa slučajem mogu jednostavno da shvate povezanost tih dokaza sa slučajem.

Ovo je postupak za koji su potrebni specijalističke veštine i znanja.

3. Opšti principi

Ovaj Vodič između ostalog, pruža najbolju praksu u radu sa elektronskim dokazima. Postoje četiri opšta principa kojih policijski službenici moraju da se pridržavaju kako bi se očuvala verodostojnost dokaza:

Prvi princip
Policijski službenik nijednom radnjom ili postupkom ne sme da izmeni datum na računaru ili uređaju za skladištenje podataka, koji bi kasnije mogao da posluži kao dokaz pred sudom. Stoga, potrebno je planirati pretres elektronskih dokaza, prikupiti informacije o osumnjičenom, lokacijama i proceniti ljudske kapacitete i potrebnu opremu.

Drugi princip
U slučaju da policijski službenik smatra da je neophodno da pristupi prvobitnom datumu na računaru ili uređaju za skladištenje podataka, Mora biti kompetentan, znati kako da dođe do dokaza, objasni značaj dokaza i šta namerava postići tom radnjom.

Treći princip
Svi postupci primenjeni na elektronske dokaze izuzete sa računara ili drugog uređaja moraju biti zabeleženi u obliku evidencije o preduzetim radnjama/postupcima/koracima ili nekom drugom obliku. Neophodno je da primenjene postupke ponovi nezavisno stručno lice i dobije iste rezultate.

Četvrti princip
Policijski službenik zadužen za istragu (nadležan za taj predmet) dužan je da postupa u skladu sa zakonom i ovim principima.

4. Obezbeđivanje dokaza sa sistema video-nadzora

U oblasti bezbednosti i praćenja, sistemi video-nadzora su malo standardizovani, tako da se mnoštvo različite opreme razlikuje po kvalitetu slike i koristi različite forme zapisa i njihovog skladištenja.

Kada utvrdi položaj sistema video-nadzora, policijski službenik treba da se poveže sa operaterom sistema i zatraži od njega da sarađuje u obezbeđivanju odgovarajućih snimaka.

Tipično za stare analogne sisteme je da snimaju na VHS ili SVHS video kasete, što policijskom službeniku daje mogućnost da privremeno oduzme kasete na određeni vremenski period.

Noviji digitalni sistemi obično snimaju na interni hard-disk, preko kog će, nakon određenog vremenskog perioda, automatski biti nasnimljen novi snimak. Ovaj vremenski period zavisiće od veličine hard-diska i konfiguracije sistema video-nadzora. Policijski službenik treba da traži od operatera na sistemu video-nadzora da nabavi kopiju traženih snimaka. Većina sistema će imati opciju za kopiranje podataka na eksterni uređaj (DVD, CD, USB).

U slučajevima kada je dokaz obezbeđen na samom uređaju sistema video-nadzora i ukoliko ga nije moguće kopirati na eksterni uređaj ili optički kompakt-disk, policijski službenik treba, u skladu sa Zakonikom o krivičnom postupku, da privremeno oduzme takav uređaj.

Nakon što se obezbede podaci sa sistema video nadzora, potrebno je da budu predočeni na uobičajen način, a potom predati policijskoj jedinici za obradu video-materijala. Oni će pohraniti originalni primerak i pripremiti dokazne kopije podataka u obliku koji je pogodan za potrebe suda.

5. Evidencije i podaci pružalaca komunikacionih usluga

5.1. Dobijanje podataka o komunikaciji

Sve organizacije ili poslovni subjekti koji pružaju internet-uslugu koja omogućava bilo kakav oblik komunikacije treba smatrati „telekomunikacionim operaterima”. Zahtevi za dobijanje podataka od ovih subjekata moraju biti u skladu sa Zakonikom o krivičnom postupku Republike Srbije i Zakonom o elektronskim komunikacijama.

„Podaci o komunikaciji" ili zadržani podaci znače:
1. svi podaci koji utvrđuju identitet nekog lica, sprave ili lokacije sa koje se komunikacija obavlja, već je obavljena ili bi mogla da bude obavljena,
2. sve informacije koje se odnose na lica koja koriste neku telekomunikacionu ili poštansku uslugu,
3. sve informacije o licu kojem se pruža ili je već pružena telekomunikaciona ili poštanska usluga.

Zahtevi za „podacima o komunikaciji" od „poštanskog ili telekomunikacionog operatera" moraju se uputiti na osnovu obrazloženog pisanog službenog dokumenta sa zakonskim osnovom telekomunikacionom operateru, tj. pružaocu internet usluga.

5.2. Dobijanje sadržaja komunikacije

Sadržaj komunikacije je isključen iz zadržanih podataka o komunikaciji koji se mogu dobiti po osnovu odredbi Zakonika o krivičnom postupku. Za dobijanje ovih informacija, potrebno je da policijski službenik dostavi zahtev nadležnom tužilaštvu radi inicijative za posebne dokazne radnje i dobijanje naredbe nadležnog suda u smislu posebnih dokaznih radnji definisanih u čl.162. Zakonika o krivičnom postupku.

5.3. Dobijanje podataka od drugih onlajn usluga u Republici Srbiji

Postoji mnogo „onlajn usluga", kao što su veliki i mali veb sajtovi koji nisu „telekomunikacioni operateri". Policijski službenici mogu da zahtevaju podatke od ovih organizacija po osnovu Zakonika o krivičnom postupku i Zakona o elektronskim komunikacijama.

5.4. Dobijanje podataka iz inostranstva

Postoji mnogo onlajn usluga koje pružaju organizacije koje se nalaze van Republike Srbije i međunarodne organizacije koje svoje podatke drže van Republike Srbije. U tom slučaju je možda neophodna pomoć strane policijske službe. Ovi upiti su često spor postupak. Da bi se sprečio gubitak podataka dok traje postupak međunarodnih upita, preporučuje se da se vlasniku podataka (internet-servis-provajderu i dr.) izda „zahtev za očuvanje podataka", kojim se obaveštava o traženim informacijama. Ovo omogućuje da se podaci očuvaju dok se čeka dobijanje odgovarajućeg pravnog dokumenta tj. međunarodne zamolnice za pružanje pravne

pravne pomoći. Zahtevi za očuvanje podataka upućuju preko kontakt-tačke 7/24 pri Odeljenju za borbu protiv visokotehnološkog kriminala, ili Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala.

Takođe, veliki pružaoci internet usluga, poput servisa Facebook, Google, Yahoo, i dr. ostvaruju neposrednu komunikaciju sa nadležnim institucijama zaduženim za vođenje pretkrivičnog postupka. Primera radi, kompanija Facebook autorizovanim institucijama za sprovođenje zakona, u skladu sa svojom poslovnom politikom i primenjivim zakonom, na obrazloženi zahtev nadležnog tužilaštva dostavlja zadržane podatke o svojim korisnicima (internet-protokol i elektronske adrese, i dr.).

Više informacija o saradnji u krivičnim istragama sa kompanijom Facebook možete naći na internet-stranici društvene mreže *fejsbuk(*)*, koja daje detaljna pravna uputstva, poput informacija za policijske službe, zahteva na osnovu sudskih rešenja u SAD, podatka o nalogu, koje otkrivaju isključivo u skladu sa svojim uslovima korišćenja usluge i važećim zakonom, uključujući savezni Zakon o sačuvanoj komunikaciji (Stored Communications Act, „SCA"), 18. tom Kodeksa SAD (U.S.C.), odeljci 2712–2701., zahteva na osnovu međunarodnih sudskih rešenja, čuvanja naloga, zahteva u hitnim slučajevima, pitanja vezana za bezbednost dece, zadržavanja i dostupnosti podataka, obliku zahteva, pristanku korisnika naloga (ako pripadnik policijske službe traži informacije o fejsbuk-korisniku koji je pristao na to da taj pripadnik policije pristupi podacima o nalogu korisnika ili da ih dobije, korisniku treba preporučiti da sam preuzme te informacije sa naloga), obaveštavanje korisnika naloga čija se provera traži (politika kompanije Facebook nalaže da korisnike usluga obaveste o zahtevima za pristup njihovim informacijama pre nego što te informacije otkriju, osim kada im zakon to zabranjuje ili u izuzetnim okolnostima, kao što su slučajevi eksploatacije dece, hitni slučajevi ili slučajevi u kojima bi obaveštenje bilo kontraproduktivno.), veštačenja, nadoknade troškova i podnošenja zahteva sa adresom.

Svi zahtevi nadležnog tužilaštva moraju da sadrže detaljne informacije o traženim podacima, kao i sledeće stavke:

- naziv organa koji ga je izdao (navesti nadležno tužilaštvo), broj značke/identifikacionog dokumenta zaduženog policijskog službenika, e-adresu sa domena policijske službe i direktan broj telefona za kontakt,
- e-adresu, identifikacioni broj korisnika (http://www.facebook.com/profile.php?id=1000000XXXXXXXX) ili njegovo korisničko ime (http://www.facebook.com/username) sa fejsbuk-profila.

* https://www.facebook.com/safety/groups/law/guidelines

6. Podaci iz otvorenih internet-izvora

Informacija iz otvorenog izvora definiše se kao: „Svaka informacija koja nije označena kao poverljiva, u bilo kom sredstvu informisanja, koja je opštedostupna javnosti, čak i u slučaju da je distribucija ograničena ili moguća samo uz plaćanje".
Na internetu postoji značajan broj informacija iz otvorenog izvora koje se mogu upotrebiti kao dokaz ili obaveštajni podatak u prilog slučaju koji se obrađuje, kao npr. identifikacioni podaci o licu, koje možemo uvezati sa nekim elektronskim nalogom ili fotografijom, kućnom adresom, telefonskim brojem, imovinom, geo-podacima tj. lokacijom, poslovanjem i finansijskim podacima, povezanost osoba po različitim osnovama, interesovanja, i mnogo drugih podataka na osnovu kojih je moguće izvršiti kvalitetnu analizu i profilisanje lica.

7. Onlajn korisnički nalozi i onlajn skladištenje podataka

Kako se tehnologija razvija postaje uobičajeno da ljudi rutinski skladište svoje elektronske podatke onlajn. To im omogućuje da svojim fajlovima pristupe sa bilo kog računara koji ima pristup internetu, uključujući mobilne uređaje, kao što su laptop računari, tableti ''pametni'' telefoni i dr. Ovakav pristup obradi, skladištenju i ponovnom pronalaženju podataka često se naziva „računarstvo u oblacima". U mnogim slučajevima kopije ovih fajlova neće se čuvati na ličnom računaru neke osobe, već će ti onlajn podaci verovatno biti čuvani u šifrovanom obliku na serverima izvan teritorije Republike Srbije. Najčešće vrste fajlova koji se u današnje vreme skladište onlajn su elektronske poruke, razna dokumenta u različitim formatima i multimedijalni fajlovi (fotografije, muzika i video-zapisi). Pristup ovim podacima često može biti izazov za policijske službenike.

Oštećeni i svedoci

Kada su elektronski dokazi dostupni oštećenom licu ili svedoku preko onlajn naloga, potrebno je zahtevati od njih zahtevati da dostave kopiju tih podataka, koji se mogu predočiti na uobičajen način. Ukoliko je moguće, te podatke treba kopirati na optički kompakt disk (CD/DVD) kako bi se sačuvao njihov prvobitni oblik. Ukoliko to nije moguće, policijski službenik mora da razmotri odgovarajuće alternativno rešenje. Moguće opcije mogle bi biti da sačini štampanu kopiju, prenese podatke na USB uređaj ili ih pošalje elektronskom poštom.

Osumnjičeni

Kada se obavlja razgovor sa osumnjičenima, važno je pitati ih da li imaju pristup bilo kom onlajn nalogu

gde se mogu pohraniti elektronski podaci. Kada se utvrdi da osumnjičeni ima nalog, potrebno ga je upitati da li želi dobrovoljno da pristane da policijski službenik pristupi tim nalozima i kopira sve podatke koje smatra bitnim za slučaj koji se istražuje i privremeno preuzme takav nalog u smislu odredbi čl.147. st. 3 u vezi sa st.1 Zakonika o krivičnom postupku, uz uredno izdatu potvrdu o privremeno oduzetim predmetima, u kojoj je neophodno konstatovati da je lice dobrovoljno predalo svoja korisnička imena i šifre za svoje elektronske naloge policijskim službenicima.

8. Uređaji krajnjeg korisnika (oštećeni - svedoci)

Kada se obavlja razgovor sa oštećenim licem ili svedokom, važno je utvrditi da li poseduje ili kontroliše bilo kakav uređaj koji može da sadrži elektronske dokaze. Osetljivost elektronskih podataka je takva da lako mogu biti oštećeni ili uništeni. Stoga je potrebno preduzeti mere da se sačuva njihova dokazna verodostojnost.

Ukoliko je moguće, policijski službenik od oštećenog lica ili svedoka traži da sarađuje i pristane da obezbedi uređaj kako bi se veštačenjem moglo doći do bilo kakvih dokaza.

Vodič pruža detaljne informacije o oduzimanju, rukovanju i ispitivanju elektronskih uređaja i uređaja povezanim sa njima. U odeljku Vodiča „Pretresanje i oduzimanje“ navedene su ključne stvari koje treba zapamtiti.

U slučaju da ne može da se dobije pristanak, policijski službenik mora da razmotri da li je odgovarajući korak da privremeno oduzme uređaj po osnovu čl.147. st.3. u vezi st.1. Zakonika o krivičnom postupku.

Kada se po osnovu zakona nalazi u nekim prostorijama, policijski službenik može da oduzme svaki predmet za koji veruje da postoji osnovana sumnja da je dokaz krivičnog dela i da je oduzimanje neophodno kako bi se sprečilo da uređaj bude sakriven, izgubljen, izmenjen, oštećen ili uništen.

Kada policijski službenik ima ovlašćenje da oduzme bilo koji materijal u elektronskom obliku, on može da zahteva da taj materijal sačini u obliku koji se može poneti, da je jasan i čitak.

8.1. Profesionalni svedoci

U radu sa profesionalnim svedocima koji drže elektronske dokaze kao deo evidencije koju prikupljaju u poslovanju ili pružanju usluga kroz određene internet-prezentacije, kao što su internet- servis-provajderi, pružaoci usluga mobilne telefonije i administratori internet prezentacija, policijski službenik postupa po sledećim odeljcima ovog priručnika:

- Evidencija i podaci provajdera komunikacionih usluga,
- Specijalne procedure na osnovu najbolje prakse koje ne utiču na izmenu elektronskih dokaza.

9. Elektronsko traganje

Postoje dva aspekta elektronskog traganja:

- utvrđivanje pravog identiteta neke osobe putem onlajn identifikatora,
- utvrđivanje autora određene elektronske informacije na osnovu internet-protokol-adrese

9.1. Onlajn-identifikator

Skoro svaki pružalac usluga preko interneta koji dozvoljava interakciju korisnika (više od samog pregledanja objavljenih sadržaja) zahteva da se kreira „korisnički nalog". Ovi nalozi služe da se obezbedi izvestan stepen odgovornosti i revizorske funkcionalnosti pružaocu usluga. Stepen verifikacije identiteta koji se odnose na onlajn naloge u velikoj meri se razlikuje među provajderima. U nekim slučajevima, traži se veoma malo ličnih podataka da bi se otvorio nalog i ništa od navedenih podataka se ne proverava. U tim slučajevima, navedeni podaci ne mogu se sa sigurnošću smatrati tačnim. Sa druge strane, postoje nalozi u vezi sa kojima se primenjuju znatne bezbednosne mere kako bi se potvrdio tačan identitet lica koje otvara nalog ili mu pristupa. Kada je lični identitet sadržan u onlajn nalogu, dužnost je policijskog službenika da utvrdi njegovo poreklo pre nego što postupi po toj informaciji.

9.2. Internet protokol (IP) adresa

Računari povezani sa internetom između sebe komuniciraju putem internet-protokola (IP). Svaki računar povezan sa internetom mora da ima jedinstvenu IP-adresu preko koje se može identifikovati. IP-adresa računara se može smatrati „brojem telefona" za telefonsku mrežu ili „poštanskom šifrom" za poštanske usluge. To je jedinstven identifikator koji omogućuje da se pošalju informacije. Očita razlika između analogija telefona i poštanske usluge sa IP-adresiranjem je u tome što su im jedinstveni identifikatori dodeljeni za stalno dok IP-adrese često dodeljuje internet-servis-provajder (ISP) svojim klijentima (pretplatnicima) u vidu kratkoročnog zakupa i te adrese nazivamo dinamičkim. Iz tog razloga policijski službenik obavezno mora da utvrdi tačan datum i vreme (uključujući vremensku zonu) za koje je zainteresovan u vezi sa datom IP-adresom. To dozvoljava da internet-servis-provajder proveri svoju evidenciju i utvrdi kojem pretplatniku je dodeljena konkretna IP-adresa u konkretno vreme, kako bi se identifikovao autor određene elektronske informacije. Međutim, ISP čuva ovu evidenciju samo tokom ograničenog vremenskog perioda. U većini slučajeva je to period od 12 meseci.

Policijski službenik mora da deluje brzo da bi se sprečio gubitak podataka koji su od ključnog značaja za ulaženje u trag osumnjičenom.
Primer IP adrese: 176.221.75.99 (IP-adresa Republičkog javnog tužilaštva tj. www.rjt.gov.rs)

Postoje određene IP-adrese koje su rezervisane za privatne mreže. Ovo omogućuje međusobnu komunikaciju računara u okviru neke mreže, ali ne direktno sa internetom. Ukoliko računari sa privatne mreže imaju pristup internetu, to se odvija preko određenog računara poznatog kao gateway (kapija).
Raspon privatne (interne) IP adrese:

- 10.xxx.xxx.xxx [xxx = vrednost između 0 i 255]
- 192.168.xxx.xxx [xxx = vrednost između 0 i 255]
- 172.yy.xxx.xxx [yy = raspon između 16 i 31][xxx = raspon između 0 i 255]

Ukoliko policijski službenik tokom istraga dobije privatnu IP-adresu, iz te informacije neće biti moguće da identifikuje određenu privatnu mrežu ili računar. Važno je da prvo identifikuje „internet-kapiju“ (gateway), što potom vodi identifikaciji privatne mreže.

9.3. Utvrđivanje onlajn identifikatora

Bez obzira da li pokušavate da identifikujete osobu iza nekog „onlajn identiteta“ ili pripisujete internet-sadržaj određenoj osobi, metodologija će biti ista. Policijski službenik mora da traži od internet-servis-provajdera ili onih koji poseduju podatke tj. evidencije o korisničkim pristupima. Uz verifikovane naloge, to može da bude dovoljno informacija za delovanje. U drugim slučajevima, može biti neophodno da se zahteva istorijat logovanja određenog naloga ili traži IP-adresa koja je povezana sa određenom informacijom ili transakcijom (ne treba zaboraviti vreme i datum). Napredak u internet-upitima da bi se dobile najkvalitetnije informacije koje je moguće verifikovati je veština koja se razvija isključivo praksom. Policijski službenici i tužioci podstiču se da u svom radu upućuju upite koji se tiču interneta jer će to neizostavno proširiti njihove istražne veštine. Internet-upiti o korisnicima opsega IP-adresa koji se nalaze kod jednog od 5 svetskih regionalnih internet-registara „Whois“ baza podataka *(African Network Information Centre, American Registry for Internet Numbers, Asia-Pacific Network Information Centre, Latin America and Caribbean Network Information Centre, RIPE Network Coordination Centre)(*)* najčešće se vrše preko sledećih onlajn internet-servisa: https://centralops.net, http://www.infosniper.net i dr.

Nakon što se utvrdi IP-adresa, trebalo bi da bude moguće da se poveže sa nalogom pretplatnika preko odgovarajućeg internet-servis-provajdera.

* Izvor: https://en.wikiversity.org/wiki/Whois/IP_address

Zapamtite da sve zahteve koje se tiču IP-adresa i drugih upita upućenih operaterima telekomunikacija i internet-servis-provajderima podležu Zakoniku o krivičnom postupku i Zakonu o elektronskim komunikacijama.

10. Savet o pretresanju

10.1. Pre pretresa

Potrudite se da prikupite što više informacija o vrsti, mestu i konekciji svakog računarskog sistema. Ukoliko planirate da izvršite pretres poslovne prostorije gde postoje korporativne mreže, potrebno je da se za savet obratite Posebnom tužilaštvu za borbu protiv visokotehnološkog kriminala ili Odeljenju za borbu protiv visokotehnološkog kriminala.

10.2. Brifing

Veoma je važno da svi službenici koji prisustvuju mestu pretresanja budu adekvatno informisani. U ovoj fazi, daje se savet o tome kako da se bezbedno pribavi svaki dokaz sa računara. Daju se stroga upozorenja kako bi neobučeni službenici bili sprečeni da pristupaju računarima i nosačima memorija. Timovima za pretresanje savetuje se da se za savet obrate Posebnom tužilaštvu za borbu protiv visokotehnološkog kriminala pre nego što oduzmu bilo koji računar koji je deo korporativne mreže.

10.3. Priprema za pretres

Proverite da li oprema za pretresanje mesta izvršenja krivičnog dela sadrži odgovarajući materijal za oduzimanje računara, uređaja za pohranjivanje elektronskih podataka i svaki drugi dokaz koji ima veze s tim.
Šta poneti:

- foto-aparat i/ili kameru za snimanje lica mesta i informacija na ekranu,
- rukavice za jednokratnu upotrebu (za sve službenike koji vrše pretres),
- alat (baterijsku lampu, makaze, šrafciger, klešta i rezače žica),
- nalepnice za dokazni materijal,
- kese za zaštitu od neovlašćenih izmena dokaznog materijala (raznih veličina),
- providne plastične kese za dokazni materijal (raznih veličina) i pečate za kese,
- papirne kese za dokazni materijal (raznih veličina) i selotejp,
- flomastere u boji za obeležavanje šifri i naziva predmeta koji su uzeti,
- kutije na sklapanje.

10.4. Pretresanje mesta izvršenja krivičnog dela

Pri dolasku na mesto izvršenja krivičnog dela ili tokom pretresanja prostorija gde postoji mogućnost da se nalazi elektronski dokaz na računaru, policijski službenik preuzima kontrolu nad tim mestom i vodi računa da se lica odmaknu od računara ili drugih uređaja na kojima bi mogli da utiču na dokaz.

Nakon što se obezbedi, prostorija se snima kamerom ili fotografiše pre početka pretresa. Naročito treba obratiti pažnju na radno mesto u i oko računarskih sistema, te utvrditi da li ima DVD/CD medija u uređaju.

Ukoliko su računari isključeni, nemojte da ih uključujete. Ukoliko su uključeni, nemojte da padate u iskušenje da vršite pretragu na njima tražeći dokaze. Za pretragu računara potrebna je posebna veština. Pristupanje računaru bez primene odgovarajuće procedure veštačenja izmeniće podatke i kompromitovati dokaze.

Što se tiče laptopova, imajte na umu da se neki mogu automatski uključiti samim podizanjem poklopca. Uključivanjem računara promeniće se datum u operativnom sistemu što može da kompromituje verodostojnost dokaza na njemu.

Uvek se pridržavajte saveta o oduzimanju računara navedenih u '"Obaveznoj instrukciji o prikupljanju i obezbeđivanju elektronskih dokaza" od 2013 .02 .26. godine broj: 12-13/1000-01. (UKP br. 13/1633 4/03 od 01.03.2013.).

Setite se da potražite lozinke koje su često zabeležene u dnevnicima ili beleškama oko računara.

Potražite priručnike sa uputstvima za softver ili oduzete uređaje. To može biti korisno veštaku kada sprovodi analizu.

Potražite sve povezane uređaje za skladištenje elektronskih podataka. Mnogi uređaji imaju opcije za odvojeno skladištenje podataka. Dokaz koji tražite možda je već prenet na taj odvojeni deo i više nije dostupan na uređaju. Uređaj za skladištenje može fizički da bude veoma mali, a da može da pohrani veliku količinu podataka, pa je neophodna temeljna pretraga.

Sve oduzete predmete treba pažljivo zapakovati i priložiti na uobičajen način. Predmeti se prilažu pojedinačno, osim u slučaju veće količine sličnih predmeta pronađenih na istom mestu. Na primer, svi kompakt-diskovi pronađeni na radnom stolu mogu se priložiti zajedno, dok svi hard-diskovi mogu da se prilože kao sledeći dokaz. Međutim, ove dve vrste predmeta ne treba izmešati u jedan dokazni predmet.

Sve dokazne predmete čuvajte dalje od magneta i radio-odašiljača.

Sve dokazne materijale treba evidentirati kao spisak dokaznih materijala u potvrdama o privremeno

oduzetim predmetima i zapisnicima i zalepiti na njih nalepnice na kojima je navedeno mesto oduzimanja i mesto za skladištenje.

Kako oduzeti računar (kada je isključen)

- Ne uključujete računar.
- Imajte na umu da se laptopi mogu uključiti samim podizanjem poklopca.
- Ne dozvolite osumnjičenima da pristupe uređaju.
- Fotografišite računar i radni sto / mesto gde se nalazi.
- Fotografišite kablove koji idu do/od računara.
- Isključite kabl za struju iz zadnjeg dela računara, a ne iz zida.
- Nacrtajte dijagram i označite kablove za kasnije raspoznavanje povezanih uređaja.
- Posebno pogledajte da li postoji bilo kakva internet-konekcija.
- Isključite sve kablove i uređaje iz računara.
- Pažljivo spakujte i označite predmete koji se oduzimaju kao dokazni materijal.
- Oduzmite sve uređaje za skladištenje elektronskih podataka koji se nalaze na tom mestu.
- Oduzmite sve priručnike za upotrebu tih uređaja.
- Oduzmite sve beleške u blizini računara.
- Dokumentujte sve što ste radili.

Laptop

Imajte na umu da se laptopi mogu uključiti samim podizanjem poklopca.
Da biste obezbedili da se laptop, slučajno ne uključi preporučuje se da izvadite bateriju.

Kako oduzeti računar (kada je uključen)

- Obezbedite oblast gde se nalazi kompjuterska oprema.
- Udaljite ljude od računara i napajanja za struju.
- Ne dozvolite da osumnjičeni prilaze uređajima.
- Ne koristite računar, niti pretražujte po njemu tražeći dokaze.
- Evidentirajte ono što je na ekranu (fotografija i beleške).
- Ne koristite tastaturu.
- Ako je aktivan skrinsejver, pokret miša trebalo bi da ga skloni, koristite miš da prelazite preko otvorenih prozora sa task-bara.
- Ukoliko neka aplikacija briše podatke – odmah isključite računar tako što ćete izvući kabl za struju iz zadnjeg dela računara. Pojedinim vrstama podatka moglo bi biti nemoguće ponovo pristupiti nakon što bi se isključio računar. Ukoliko sumnjate da neka od otvorenih aplikacija možda sadrži dokaze, pre nego što nastavite, posavetujte se sa Odeljenjem za VTK ili Službom za specijalne istražne metode radi eventualnog kreiranja forenzičke kopije RAM(*) memorije.
- Procenite da li bi bilo dobro da korisniku postavite određena pitanja o aplikacijama.
- Vodite evidenciju o svim preduzetim radnjama, postupcima i koracima.
- Pustite da svi štampači završe štampanje.
- Fotografišite računar i radni sto / mesto gde se nalazi.
- Izvadite kabl za napajanje strujom iz zadnjeg dela računara (ne iz zida) bez isključivanja bilo kog programa, ili isključite računar po uobičajenom postupku.
- Fotografišite kablove koji vode do/od računara.
- Nacrtajte dijagram i označite kablove za kasnije raspoznavanje povezanih uređaja.
- Posebno pogledajte da li postoji bilo kakva internet-konekcija.
- Isključite sve kablove i uređaje iz računara.
- Pažljivo spakujte i označite predmete koji se oduzimaju kao dokazni materijal.
- Oduzmite sve uređaje za skladištenje elektronskih podataka koji se nalaze na tom mestu.
- Oduzmite sve priručnike za upotrebu softvera i oduzetih uređaja.

* Osobina RAM memorije je da se svakom njenom bajtu može slobodno pristupiti nezavisno od prethodne memorijske lokacije, s tim da se u nju podaci mogu i upisivati (write) i očitavati (read) iz nje. Svakim upisom podatka u neku lokaciju, njen prethodni sadržaj se automatski gubi. Druga važna osobina RAM memorije je da podatke koji se u njoj nalaze zadržava (čuva) samo dok postoji napon napajanja na njoj. Čim nestane napona napajanja, kompletan sadržaj memorije se gubi i prilikom ponovnog dolaska napona napajanja (pri sledećem uključenju računara) ona je potpuno prazna.

- Oduzmite sve beleške u blizini računara.
- Pustite da se oprema ohladi pre premeštanja.
- Dokumentujte sve korake preduzete u postupku oduzimanja.

Laptopi

Skidanje kabla sa laptopa verovatno ga neće isključiti jer će se prebaciti na baterijsko napajanje. Da biste ga isključili, pritisnite i držite ''on/off'' dugme 5 do 10 sekundi (dok se ne isključi). Potom izvadite bateriju.

Ukoliko su otvorene neke aplikacije (kao što su šifrovane), možda bi bilo bolje da laptop ostane uključen na baterijskom punjenju i da ga prenesete direktno u Upravu kriminalističke policije, Službu za specijalne istražne metode, ukoliko je to moguće. Time ćete verovatno smanjiti rizik od gubitka tih podataka kada se računar isključi.

Kućne mreže – šta imati na umu

Danas se domaći broadband pristup internetu može ostvariti od kuće na jedan od sledeća dva načina:

- ADSL Broadband (npr. BT telefonska linija), (*)
- optički kabl (npr. SBB SOLUTIONS kablovski internet),

Obično internet-servis-provajder isporučuje broadband internet uslugu preko modema koji je fizički povezan sa telefonskom linijom korisnika. Modem je jednostavan elektronski uređaj koji konvertuje digitalne podatke sa računara tako da mogu biti preneti preko telefonske mreže. Modem može biti konektovan direktno na računar ili na ruter. Ruter je elektronski uređaj koji omogućuje da više računara bude povezano kako bi razmenjivali podatke i sredstva (kao što su štampači i internet-konekcije).

Ruteri daju jednaku mogućnost računarima da budu povezani fizički (Ethernet Cable) ili bežično (WiFi). U praksi nije neuobičajeno da „modem" i „ruter" budu kombinovani u jednom uređaju koji je povezan kablom i bežičnim putem za pristup broadband internetu. Modem / ruter pruža pristup internetu jednom ili više računara. Oni mogu biti povezani kablovima (Ethernet Cables) ili bežično. Treba imati na umu da, pored desktop-računara i laptopa, i drugi portabl-uređaji mogu da pruže pristup internetu, poput pametnih telefona, PDA-uređaja, igračkih konzola, tablet-računara, TV-a koji u sebi sadrže memorijske jedinice, i dr.

* Širokopojasni pristup internetu koji omogućuje velike brzine prenosa podataka korišćenjem telefonske infrastrukture, dok BT telefonska linija podrazumeva više telefonskih linija kroz jedan priključak.

Kućne mreže – šta uzeti u obzir pri pretresanju i privremenom oduzimanju predmeta

- Obezbedite oblast gde se nalazi računarska oprema.
- Udaljite ljude od svih računara i napajanja za struju.
- Ne dozvolite da osumnjičeni prilaze uređajima.
- Utvrdite gde je modem / ruter i isključite ga iz telefona i napajanja
- Utvrdite gde su uređaji krajnjeg korisnika (računari, telefoni, personalni digitalni asistent -PDA, itd.)
- Obradite svaki uređaj (odredite prioritete u oduzimanju): da li je uređaj uključen? (dajte mu prednost u odnosu na isključene), da li se podaci brišu? (izvucite kabl za struju da ga isključite).
- Ne koristite računare, niti da pokušavajte da vršite pretrage na njima tražeći dokaze.
- Sistematski se pozabavite svakim računarom kao što je gore navedeno.

Oduzimanje modema i rutera

Od prirode vaše istrage zavisiće da li bi trebalo da oduzmete internet modem / ruter. Ovi uređaji se ne koriste za skladištenje ličnih fajlova, ali mogu da sadrže fajlove o logovanju i informacije o konfiguracijama koji mogu da pomognu pri identifikaciji uređaja koji su preko njih konektovali na internet. Neki od ovih uređaja će izgubiti ove informacije ako se isključe. Ukoliko mislite da informacije sa modema / rutera mogu da budu od koristi za vaše istrage, dodatno se posavetujete sa Odeljenjem za borbu protiv VTK, (biće vam potrebni detalji i model modema / rutera).

Alternativne metode pristupa internetu

Trebalo bi da imate na umu činjenicu da, pored konvencionalnih internet usluga koje se pružaju preko kućnog fiksnog telefona, postoje i alternativne metode pristupa internetu, preko uređaja kao što su: Broadband Dongle, MiFi (Mobile Internet Hub), WiFi hotspot-ova, deljenje mreže preko pametnih telefona, tablet-računara i sl. Takođe je moguće da se neko konektuje preko nebezbednog bežičnog rutera nekog u komšiluku (sa ili bez njegovog znanja), ili u nekom restoranu, hotelu, internet-kafeu, i sl.

Mrežni serveri i poslovne mreže

Kada se susretnete sa poslovnom mrežom i serverom složene infrastrukture, pre nego što bilo šta preduzmete, obavezno se obratite za dalju pomoć nekome iz Službe za specijalne istražne metode.

Utvrdite ko je mrežni ili sistem administrator kako bi pripadnici Službe za specijalne istražne metode mogli sa njim da razgovaraju o mogućim načinima obezbeđivanja dokaza.

Imajte na umu da bi to lice moglo da bude osumnjičeni u određenim slučajevima.

Obezbedite to mesto i nemojte da dozvolite da bilo ko koristi bilo koji od računarskih sistema dok se ne dobiju odgovarajuće smernice.

UPOZORENJE

Izvlačenje utikača može da:

- ozbiljno ošteti sistem,
- izazove gubitak ključnih dokaza,
- omete zakonito poslovanje,
- otvori mogućnost za preduzimanje zakonite radnje, ukoliko je neophodno privremeno oduzeti server nakon završetka računarskog pretraživanja podataka na osnovu naredbe nadležnog sudije za prethodni postupak, imajući u vidu činjenicu prekid funkcionisanja rada servera, npr. ukoliko se na serveru nalaze isključivo nedozvoljeni i štetni sadržaji, kao i drugi nezakoniti podaci.

Mobilni telefoni i ostali digitalni uređaji krajnjeg korisnika

Mobilni telefoni mogu da uskladište dokazne podatke direktno na internu-memoriju, SIM karticu ili dodatnu memorijsku karticu. U daljem tekstu, detaljno navodimo kako pravilno oduzeti i sačuvati ove uređaje i sa njima povezane dodatne delove.

- Ako je uređaj isključen, ne uključujte ga.
- Ako je uređaj uključen:

- fotografišite ili zabeležite sve što je na ekranu,
- uporedite datum i vreme na ekranu sa stvarnim datumom i vremenom.

- U redovnom postupku oduzimanja, isključite telefon.
- U vanrednom slučaju, ostavite uređaj da radi.
- Ni u kom slučaju ne pretražujte uređaj u potrazi za dokazima.
- Telefon stavite u torbu sa efektom Faradejevog kaveza, ukoliko je posedujete. (*)
- Pitajte vlasnika da li želi da dobrovoljno preda PIN ili lozinke.
- Oduzmite sve kablove (uključujuće one za napajanje strujom) i držite ih sa uređajem.
- Oduzmite sve uređaje za skladištenje (memorijske kartice).
- Dokumentujte sve korake koje ste preduzeli pri oduzimanju uređaja i komponenata.

Ovi uređaji imaju bezbednosnu osobinu daljinskog brisanja podataka za slučaj krađe uređaja. Da biste sprečili aktiviranje ove osobine, izvadite SIM karticu i stavite uređaj u torbu sa efektom Faradejevog kaveza.

Obaveštenje

Isključivanje mobilnog telefona moglo bi naknadno aktivirati traženje lozinke ili PIN koda, čime se odlaže ili sprečava kasniji pristup dokazima ukoliko ne znamo tu informaciju ili je ne možemo lako dobiti. Međutim, ukoliko bi mobilni telefon ostao uključen, postoji rizik da podaci mogu biti izmenjeni ili preko njih nasnimljeni novi od dolazećih poziva i tekstualnih poruka. Policijski službenici moraće sami da procene šta je najbolje uraditi u datoj situaciji.

Pored računara i mobilnih telefona, postoje mnogi drugi digitalni ili elektronski uređaji krajnjih korisnika koji imaju mogućnost da pruže dokazne podatke. Neki od uobičajenih primera su: personalni digitalni asistenti (PDA), digitalne kamere, MP3 muzički plejeri, globalni sistemi za određivanje položaja (GPS) i sistemi za satelitsku navigaciju (Sat-Nav) i dr. Ovi uređaji mogu da skladište podatke pomoću interne memorije ili dodatnih delova. U daljem tekstu, navodimo uputstva za oduzimanje portabl-uređaja krajnjeg korisnika i sa njima povezanih dodatnih delova.

- Ako je uređaj isključen, ne uključujte ga.
- Ako je uređaj uključen:
- fotografišite ili zabeležite sve što je na ekranu, a PDA ne isključujte (pogledati savet za PDA). Ostale uređaje isključite.
- pokupite sve kablove (uključujući one za napajanje strujom i kućišta uređaja).

* Faradejev kavez ili Faradejev štit predstavlja prostor ograničen nekim provodljivim materijalom ili mrežom napravljenom od takvog materijala. Takav prostor ima osobinu da blokira spoljašnje statičko električno polje.

- Oduzmite sve dodatne uređaje za skladištenje (memorijske kartice).
- Pitajte vlasnika da li želi dobrovoljno da vam kaže lozinke.
- Dokumentujte sve korake koje ste preduzeli pri oduzimanju uređaja i komponenata.

Savet za PDA

Isključivanje personalnog digitalnog asistenta (PDA) moglo bi da aktivira traženje lozinke, što sprečava ili odlaže pristup dokazima. Većina ovih uređaja ima internu bateriju koja je od ključnog značaja za čuvanje ličnih podataka korisnika (poznate kao „nestalna memorija“). Važno je da ova baterija uvek bude napunjena, inače dokazi mogu biti izgubljeni. Ukoliko je to moguće, stavite ovaj uređaj na punjenje dok vršite pretres i ponovo kada se vratite u policijsku stanicu. Čim je to moguće, odnesite uređaj u Službu za specijalne istražne metode gde može biti pohranjen i pregledan na odgovarajući način.

Računarsko veštačenje

Policijski službenici ni u kom slučaju ne smeju da uključuju ili pretražuju sadržaj bilo kojih računara, mobilnih telefona, ostalih elektronskih uređaja krajnjeg korisnika ili sa njima povezanih uređaja kada postoji mogućnost da imaju dokaznu vrednost. Računarska trijaža je proces koji koristi tehnologiju automatske pretrage kako bi se otkrio specifičan dokaz na računarima ili uređajima za skladištenje podataka. Tehnički je pogodnija da potvrdi postojanje dokaza na uređaju nego da dokaže da nema dokaza. Stoga, trijažu nikako ne treba smatrati zamenom za temeljno veštačenje računara. Međutim, to je koristan postupak za utvrđivanje da li je oduzet pravi uređaj, ili da se odredi prioritet u ispitivanju oduzetih predmeta.

- Savet o tome da li je neki slučaj pogodan za trijažu potražite od Službe za specijalne istražne metode.
- Ispitivanje računara, mobilnih telefona i drugih digitalnih uređaja krajnjeg korisnika zahteva veštine specijaliste za digitalno forenzičko veštačenje.
- Zaposleni u Službi za specijalne istražne metode su prošli opsežnu obuku kod akreditovanih organizacija i poseduju potrebno znanje i iskustvo za obavljanje temeljnog veštačenja, a svoja otkrića predstavljaju u formatu pogodnom za sudske postupke
- U svim slučajevima u kojima su, zajedno sa računarima, radi ispitivanja oduzeti i mobilni telefoni, njih će obraditi Služba za specijalne istražne metode. Zahtevi za ovim ispitivanjima podnose se u skladu sa postupkom dodele zadatka Službi za specijalne istražne metode
- U slučajevima kada su oduzeti samo mobilni telefoni, policijski službenik se za savet i uputstva mora obratiti Službi za specijalne istražne metode

• Svi zahtevi za digitalnim forenzičkim veštačenjem moraju se dostavljati preko Službe za specijalne istražne metode, koja će odrediti prioritete.

Visokotehnološki kriminal kao krivično delo u domaćem zakonodavstvu sa posebnim osvrtom na tzv. *cyberbullying i grooming*

1. Uvod

U svetlu globalnog trenda virtuelnog druženja i života u sajber-prostoru, neminovno je da se suočimo sa viktimizacijom mladih na društvenim mrežama. Tome nesumnjivo doprinosi nedovoljna kompjuterska informaciona pismenost roditelja, ali mnogo više nedovoljna svest mladih o rizicima koje plasiranje ličnih informacija i postavljanje fotografija sa sobom nosi. Današnji svakodnevni život, naročito mladih, postao je gotovo nezamisliv bez upotrebe informacionih tehnologija. Mladi ljudi su od najranijih dana upućeni na tehnologiju. Sa njima ih, najpre, upoznaju roditelji dajući im svoje mobilne telefone ili tablet-računare da se zanimaju dok su oni zauzeti poslom ili su u kafiću, u poseti kod prijatelja.

Deca se tako zabavljaju, upoznaju svet, igraju igrice koje nisu uvek edukativne, uče da komuniciraju, a da ne moraju da izgovore nijednu reč. Vremenom, deca smatraju postojanje interneta prosto pitanjem života i bez njega ne bi mogli da funkcionišu. Pri svemu tome, roditelji neminovno počnu da kaskaju sa umešnošću upotrebe najnovije tehnologije, čiji razvoj je nezaustavljiv i oni nemaju vremena, interesovanja i volje da sve to isprate. To, dalje, dovodi do nemogućnosti roditelja da već u nekim ranim uzrastima ostvare adekvatan nadzor nad aktivnostima dece na internetu, pa i neznanja da sami prepoznaju opasnosti koje vrebaju.

Sposobnost roditelja da kontrolišu decu na internetu zavisi od više faktora, od kojih su neki stepen otvorenosti i bliskosti sa decom, obrazovanje roditelja, posvećenost deci i dr. S jedne strane, roditelji su svesni da je internet neiscrpan izvor informacija i zabave, te da bi samim isključivanjem dece iz svih tih aktivnosti mogli ugroziti socijalizaciju dece, ali istovremeno svesni i da pojačan nadzor može dovesti do sukoba sa decom. Kod činjenice da ne manjkaju odrasli koji internet koriste na različite zlonamerne načine, te da deca takođe brzo nauče kako da ga zloupotrebe, današnje društvo se suočava sa ozbiljnim problemom - nebezbednošću dece na internetu, naročito na društvenim mrežama. Organizacija za evropsku bezbednost i saradnju sistematizovala je rizike kojima su izložena deca kao korisnici interneta. Svi rizici su podeljeni na rizike usled izlaganja neprimerenim sadržajima (content risk) i na rizike usled nebezbednih kontakata sa drugim korisnicima (contact risk).

Neprimereni sadržaji se mogu podeliti na one čije je cirkulisanje zakonom zabranjeno, na sadržaj neprimeren uzrastu dece i na sadržaje koje popularišu negativne obrasce ponašanja. Tako je, u najvećem broju država, ilegalno promovisanje rasizma i bestijalnosti i rasturanje materijala koji sadrže elemente dečije pornografije (nelegalni sadržaji). Scene nasilja i pornografski sadržaji spadaju u materijale neprimerene uzrastu, dok bi davanje saveta za samopovređivanje i samoubistvo ili propagiranje poremećaja u ishrani, poput anoreksije, mogli okarakterisati kao uticaj na usvajanje negativnih obrazaca ponašanja.

Nebezbedne kontakte na internetu eksperti OEBS-a dele na: 1) kontakte putem kojih se stvaraju preduslovi kako bi se kasnije ostvario kontakt, pri kojem bi dete moglo biti viktimizovano (građenje odnosa u kojima dete stiče poverenje u lice sa kojima kontaktira – grooming, da bi se potom ostvarila seksualna eksploatacija deteta), 2) kontakte usled kojih su deca izložena agresivnom ponašanju drugih korisnika (vređanje i podsmevanje obično od strane drugih vršnjaka, ili cyberbullying) 3) kontakte putem kojih, zbog nepromišljenosti, dete doprinosi nastanku štetne posledice (kockanje na internetu, učestvovanje u pirateriji koje može usloviti kasniju odgovornost isl.). (*)

2. Krivični zakonik i pojmovna određenja

Kada govorimo o visokotehnološkom kriminalu u kontekstu zaštite maloletnih lica u Srbiji, treba najpre poći od člana 112. Krivičnog zakonika. Saglasno ovoj odredbi i to tačkama 9 ,8 i 10, detetom se smatra lice koje nije navršilo četrnaest godina, maloletnikom lice koje je navršilo četrnaest godina, a nije navršilo osamnaest godina. dok se maloletnim licem smatra lice koje nije navršilo osamnaest godina. Dalje, u tačkama (20-17) daje se značenje izraza računarski podatak, računarska mreža, računarski program i računarski virus, dok se tačkama 33. i 34. definiše računar i računarski sistem. U Vodiču, s obzirom na ograničen prostor, osvrnućemo se samo na neka krivična dela visokotehnološkog kriminala u domaćem zakonodavstvu i neke primere iz sudske prakse.

Pod ovim krivičnim delima najčešće se podrazumevaju krivična dela protiv bezbednosti računarskih podataka i to:

- član 298. Oštećenje računarskih podataka i programa,
- član 299. Računarska sabotaža,
- član 300. Pravljenje i unošenje računarskih virusa,
- član 301. Računarska prevara,

* OEBS

- član 303. Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži,
- član 304. Neovlašćeno korišćenje računara ili računarske mreže,
- član 304a. Pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka.

Međutim brojna su i druga krivična dela koja se smatraju visokotehnološkim kriminalom. S tim u vezi, važno je ukazati na Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, kojim se institucionalizuje navedena borba, ali istovremeno definiše visokotehnološki kriminal koji, u smislu tog zakona, predstavlja vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku.

Navedeni zakon primenjuje se ne samo na krivična dela protiv bezbednosti računarskih podataka, već i kod onih kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku pod određenim uslovima: krivična dela protiv intelektualne svojine, imovine, privrede i pravnog saobraćaja i, konačno, na ona koja se zbog načina izvršenja ili upotrebljenih sredstava mogu smatrati krivičnim delima visokotehnološkog kriminala, u skladu sa navedenom definicijom: krivična dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije.

Ilustracije radi, ukazaćemo samo na neka:

- Krivična dela protiv intelektualne svojine (neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava, neovlašćeno uklanjanje ili menjanje elektronske informacije o autorskom i srodnim pravima),
- Krivična dela protiv imovine (iznuda, ucena),
- Krivična dela protiv privrede (član 223: falsifikovanje novca (odredbe važeće DO 1. marta 2018. godine); član 241: falsifikovanje novca (odredbe važeće OD 1. marta 2018. godine), (član 225: falsifikovanje i zloupotreba platnih kartica (odredbe važeće DO 1. marta 2018. godine); član 243: falsifikovanje i zloupotreba platnih kartica (odredbe važeće OD 1. marta 2018. godine)),
- Krivična dela protiv pravnog saobraćaja (falsifikovanje isprave),
- Krivična dela protiv sloboda i prava čoveka i građanina ((član 138: ugrožavanje sigurnosti, član 138a: proganjanje (odredbe važeće od 1. juna 2017. godine), neovlašćeno prisluškivanje i snimanje, neovlašćeno fotografisanje, neovlašćeno objavljivanje i prikazivanje tuđeg spisa, portreta i snimka, neovlašćeno prikupljanje ličnih podataka)

prikupljanje ličnih podataka) (Saglasno članu 153. stav 1. KZ krivično gonjenje za pojedina od navedenih dela preduzima se po predlogu, o čemu uvek treba voditi računa),

• Krivična dela protiv polne slobode (član 182a: polno uznemiravanje (odredba važeća od 1. juna 2017. godine), posredovanje u vršenju prostitucije, član 185. (izmenjen od 1. juna 2017. godine): prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju, navođenje deteta na prisustvovanje polnim radnjama (član 185a, odredbe važeće od 1. juna 2017. godine), iskorišćavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu (silovanje, obljuba nad nemoćnim licem, obljuba sa detetom, obljuba zloupotrebom položaja, nedozvoljene polne radnje, podvođenje i omogućavanje vršenja polnog odnosa, posredovanje u vršenju prostitucije, iskorišćavanje maloletnika za proizvodnju slika, audio-vizuelnih ili drugih predmeta pornografske sadržine ili za pornografsku predstavu, navođenje deteta na prisustvovanje polnim radnjama),

• Krivična dela protiv javnog reda i mira (izazivanje panike i nereda)
• Krivična dela protiv ustavnog uređenja i bezbednosti Republike Srbije (izazivanje nacionalne, rasne i verske mržnje i netrpeljivosti)

U Vodiču će se, nadalje, najviše pažnje pokloniti pojedinim krivičnim delima iz glave XIV (protiv sloboda i prava čoveka i građanina) i glave XVIII (krivična dela protiv polne slobode) Krivičnog zakonika. Ovde treba pomenuti da, počev od 1. juna 2017. godine, Krivični zakonik poznaje nova krivična dela od kojih će se, saglasno temi Vodiča, pažnja posvetiti proganjanju i polnom uznemiravanju.

Proganjanje - Član 138a
(1) Ko u toku određenog vremenskog perioda:
1) drugo lice neovlašćeno prati ili preduzima druge radnje u cilju fizičkog približavanja tom licu protivno njegovoj volji;
2) protivno volji drugog lica nastoji da sa njim uspostavi kontakt neposredno, preko trećeg lica ili putem sredstava komunikacije;
3) zloupotrebljava podatke o ličnosti drugog lica ili njemu bliskog lica radi nuđenja robe ili usluga;
4) preti napadom na život, telo ili slobodu drugog lica ili njemu bliskog lica;
5) preduzima druge slične radnje na način koji može osetno da ugrozi lični život lica prema kome se radnje preduzimaju, kazniće se novčanom kaznom ili zatvorom do tri godine

(2) Ako je delom iz stava 1. ovog člana izazvana opasnost po život, zdravlje ili telo lica prema kome je delo izvršeno ili njemu bliskog lica, učinilac će se kazniti zatvorom od tri meseca do pet godina.
(3) Ako je usled dela iz stava 1. ovog člana nastupila smrt drugog lica ili njemu bliskog lica, učinilac će se kazniti zatvorom od jedne do deset godina.

Imajući u vidu da do sada nije bilo predviđeno u Krivičnom zakoniku, sudske prakse, razumljivo, nema. Međutim, izvesno je da će se pojaviti nedoumice u primeni ove odredbe. Ne prvi put će ih upravo sudska praksa otkloniti i dati odgovor na pitanja kao što su: šta podrazumeva određeni vremenski period; koje je to optimalno vreme praćenja drugog lica da bi se moglo raditi o ovom delu; šta precizno obuhvata radnja nastojanja da se uspostavi kontakt; gde je granica između stava 3. ovog dela i osnovnog oblika krivičnog dela ugrožavanja sigurnosti (osim pretnje napadom na slobodu), tim pre što je moguće ugroziti sigurnost jednokratnim preduzimanjem radnje navedene u stavu 3. ovog člana; koje su to druge slične radnje i dr. U pogledu stava 1. tačke 4, možda treba obratiti pažnju na vrstu pretnje i učestalost ponovljenih pretnji. Pa tako, na primer, da li komunikacija sadrži pretnju („naći ću te“), fizičku pretnju („prebiću te“) ili ozbiljnu pretnju za tešku telesnu povredu ili za smrt u smislu “slomiću ti nogu”, ili “ubiću te” i slično. Treba praviti razliku da li se ona ponavlja na isti ili različite načine (ponavljanje E-mail-ova ili poruka, u “chat” sobama, na najposećenijim društvenim mrežama i sl.), koliko je učestala i da li izvršilac poziva i treća lica da se uključe u tu komunikaciju i dr.

3. Krivična dela protiv polne slobode

3.1. Krivično delo prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju (čl. 185. KZ RS)

Ovo delo vrši ono lice koje 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. Kvalifikovani oblici obuhvataju ona lica koja iskoriste maloletnika za proizvodnju slika, audio-vizuelnih ili drugih predmeta pornografske sadržine ili za pornografsku predstavu i najteži oblik, ukoliko je delo izvršeno prema detetu. Sledeći oblik vrši lice koje pribavlja za sebe ili drugog, poseduje, prodaje, prikazuje, javno izlaže ili elektronski ili na drugi način čini dostupnim navedene materijale nastale iskorišćavanjem maloletnog lica. Zakonom o izmenama i dopunama Krivičnog zakonika(*) iz novembra 2016. godine, koje su posledica usaglašavanja krivičnog zakonodavstva sa potvrđenim međunarodnim ugovorima - Konvencijom o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja(**) , član 185. je izmenjen tako što je posle stava 4. dodat

* „Službeni glasnik RS“, br. 2016/94 od 24. novembra 2016
** „Službeni glasnik RS - Međunarodni ugovori”, broj 10/1

stav 5, koji sankcioniše svesno pristupanje pomoću sredstava informacionih tehnologija slikama, audio-vizuelnim ili drugim predmetima pornografske sadržine nastalim iskorišćavanjem maloletnog lica. Radnja izvršenja novog oblika krivičnog dela zasniva se na obavezi predviđenoj u članu 20. stav 1. tačka Đ navedene Konvencije. Ono što je još značajnije je da stav 6. navodi da se predmetima pornografske sadržine nastalih iskorišćavanjem maloletnog lica smatra svaki materijal koji vizuelno prikazuje maloletno lice koje se bavi stvarnim ili simuliranim seksualno eksplicitnim ponašanjem, kao i svako prikazivanje polnih organa deteta u seksualne svrhe, čime je Krivični zakonik dao definiciju dečije pornografije koja je preuzeta iz pomenute konvencije.

S obzirom da se u široj javnosti pojavilo nerazumevanje razloga za neophodnost kriminalizacije posedovanja dečje pornografije, što se očekuje i u pogledu proširivanja inkriminacije i na pristupanje, treba reći da se njen stepen razlikuje u nacionalnim sistemima krivičnog prava. Razlog je opravdan i nalazi se u činjenici da izvršioci na taj način podstiču sve veću i veću potražnju, što dalje dovodi do stalne proizvodnje ovih materijala. Zbog tog odnosa između posedovanja i seksualnog zlostavljanja dece, efikasan način da se smanji proizvodnja dečje pornografije je da se ustanove sankcije za zakonom određeno ponašanje svakog učesnika u lancu, od proizvodnje do posedovanja. Interesantno je da Konvencija o visokotehnološkom kriminalu ne samo da ne pominje svesno pristupanje predmetima pornografske sadržine nastalim iskorišćavanjem maloletnog lica, već omogućava stranama ugovornicama da isključe kriminalizaciju pukog posedovanja. S druge strane, vidi se da su pravni interesi zastupljeni u navedenoj Konvenciji širi od direktne zaštite dece od seksualnog zlostavljanja. Dok se stav 2(a) direktno fokusira na zaštitu od zlostavljanja, dotle stavovi 2 (b) i 2 (c) pokrivaju čak i slike koje su proizvedene bez kršenja prava deteta, na primer, slike koje su u potpunosti kreirane pomoću 3D softvera za modeliranje. Razlog za kriminalizaciju radnji u vezi sa fiktivnom dečjom pornografijom je činjenica da ove slike mogu - bez obaveznog stvaranja štete za realno stvarno „dete“ - da iniciraju dalju potražnju za dečijom pornografijom, a time njenu proizvodnju. Sudska praksa je do sada pokazala da dokazivanje posedovanja nije donosilo problema, međutim, dokazivanje svesnog pristupanja inkriminisanim materijalima sigurno će dati priliku odbrani da ističe slučajni klik bez ikakvog ili makar bez nesumnjivog znanja šta će videti na monitoru, sa kakvim navodima se sudovi već susreću i povodom samog posedovanja.

Praksa, dalje, ukazuje da su izvršioci krivičnih dela vezanih za seksualnu zloupotrebu maloletnih lica u pornografske svrhe na internetu svih uzrasta, nivoa obrazovanja, porodičnog statusa. U praksi se, tako, susretalo sa automehaničarom (43 godine), magistrom istorije (40 godina, zaposlen u ministarstvu), novinarom (60 godina, sa završenim FPN), sa ocem petoro dece, hemijskim tehničarom (63 godine), inženjerom informatike (24 godine), fotografom (54 godine, sa završenim Poljoprivrednim fakultetom), ocem troje dece (43 godine) i dr. Stoga, nije moguće govoriti o iskristalisanom profilu izvršioca.

Dalje, u odnosu na krivična dela iz ove glave KZ, treba ukazati da je navedenim izmenama član 185a. promenjen na taj način što je, osim pooštrene sankcije, sužena primena tako da se sada odnosi samo na dete, a ne više na maloletno lice.

U pogledu novog krivičnog dela uvedenog od 2017 .6 .1. godine, polno uznemiravanje iz člana 182a. KZ za potrebe vodiča će se predstaviti stav 2, kojim je predviđeno kao kažnjivo polno uznemiravanje učinjeno prema maloletnom licu sa zaprećenom kaznom zatvora od tri meseca do tri godine, koje se goni po službenoj dužnosti, za razliku od osnovnog oblika, koje se preduzima se po predlogu.

U pogledu ovog krivičnog dela, dobro je što je zakonodavac razrešio dilemu koja je mogla da se pojavi u primeni i što je definisao, u stavu 3, pojam polnog uznemiravanja kao svako verbalno, neverbalno ili fizičko ponašanje koje ima za cilj ili predstavlja povredu dostojanstva lica u sferi polnog života, a koje izaziva strah ili stvara neprijateljsko, ponižavajuće ili uvredljivo okruženje. Ipak, čini se da će i ovde biti problema u dokazivanju da je određeno ponašanje izvršioca imalo nedvosmisleno za cilj povredu dostojanstva lica, i to isključivo u sferi polnog života. Posebno će biti poteškoća kako u ispitivanju oštećenih na ovu okolnost, a da se time sekundarno ne viktimizuju, tako i u definisanju ponašanja koje, na primer, stvara uvredljivo okruženje.

4. Grooming

Polazeći od međunarodnih instrumenata, ovde treba istaći da je odnedavni, ali sve više zabrinjavajući fenomen dece koja budu seksualno povređena na sastancima sa odraslima sa kojima su se prvobitno susretali u sajber-prostoru, posebno u internet chat-u ili igricama, doveo do usvajanja Konvenciju za zaštitu dece od seksualnog iskorišćavanja i seksualnog zlostavljanja(*) tzv. "Lanzarote" konvenciju iz 2007. godine, koju je potpisala i ratifikovala Republika Srbija.

U članu 6. Lanzarote konvencije naglašeno je da uspešna borba iziskuje upoznavanje dece sa rizicima, i to na osnovnoškolskom i srednjoškolskom nivou u okviru šireg seksualnog obrazovanja, te da opasnostima povezanim sa upotrebom informacionih tehnologija treba posvetiti posebnu pažnju(**). Dalje, član 23. obavezuje države da u svoje krivično zakonodavstvo uvedu odredbu koja bi inkriminisala uspostavljanje elektronskih kontakata koji imaju za cilj povezivanje odraslih i maloletnih lica u cilju kasnije seksualne eksploatacije maloletnika.

* Konvencija za zaštitu dece od seksualnog iskorišćavanja i seksualnog zlostavljanja

** Treba reći da se Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija iz juna 2016. godine bavi upravo tim pitanjima. Ona uređuje preventivne mere za bezbednost i zaštitu dece pri korišćenju informaciono-komunikacionih tehnologija, odnosno na internetu, i postupanje u slučaju narušavanja ili ugrožavanja bezbednosti dece na internetu, predviđa preduzimanje preventivnih mera za bezbednost i zaštitu dece na internetu, kao aktivnosti od javnog interesa, putem: 1) informisanja i edukacije dece, roditelja i nastavnika; 2) uspostavljanja jedinstvenog mesta za pružanje saveta i prijem prijava u vezi bezbednosti dece na internetu. Cilj Uredbe je da se podigne nivo svesti i znanja o prednostima i rizicima korišćenja interneta i načinima bezbednog korišćenja internet, ali i da se unapredi digitalna pismenost dece, odnosno učenika, roditelja, odnosno staratelja i nastavnika.

Prema definiciji Svetske zdravstvene organizacije iz 1999. godine, seksualna zloupotreba deteta je uključivanje deteta u seksualnu aktivnost koju ono ne shvata u potpunosti, sa kojom nije saglasno ili za koju nije razvojno doraslo i nije u stanju da se sa njom saglasi, ili onu kojom se krše zakoni ili socijalni tabui društva. Zakonodavstvo svake države utvrđuje uzrast kada se neka maloletna osoba može saglasiti sa seksualnim kontaktom, i on se najčešće kreće u rasponu između 14 i 18 godina.
Prema Krivičnom zakoniku, taj uzrast je navršenih 14 godina. Kako dete mlađe od 14 godina još uvek nije dovoljno zrelo – ni kognitivno, ni emocionalno, ni socijalno - bilo kako iskazana saglasnost neće se smatrati validnom.

Shodno navedenom članu 23. Lanzarote konvencije, u Krivičnom zakoniku je članom 185b propisano krivično delo - iskorišćavanje računarske mreže ili komunikacija drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu. Ovo krivično delo u osnovnom obliku vrši onaj ko u nameri izvršenja krivičnog dela iz čl. 178. stav 179 ,4. stav 180 ,3. st. 1. i 181 ,2. st. 2. i 182 ,3. stav ,1 183. stav 184 ,2. stav 185 ,3. stav 2. i 185a ovog zakonika, koristeći računarsku mrežu ili komunikaciju drugim tehničkim sredstvima, dogovori sa maloletnikom sastanak i pojavi se na dogovorenom mestu radi sastanka. Kvalifikovani oblik postoji ako se delo iz stava 1. izvrši prema detetu. Kod grooming-a, kako je predviđeno u našem krivičnom zakonodavstvu, mora biti prisutna ne samo veza sa taksativno navedenim krivičnim delima u stavu 1. već je važno istaći da je bitan elemenat činjenica dolaska počinioca na mesto sastanka. S obzirom na zaprećenu kaznu, pokušaj je kažnjiv. Ovde treba ukazati da je Odbor za primenu Lanzarote Konvencije usvojio mišljenje o odredbi 23, kojim poziva države ugovornice da razmisle o proširenju kriminalizacije i na slučajeve kada seksualno zlostavljanje nije rezultat neposrednog sastanka, već i na ona ponašanja koja se završavaju na internetu, postignutim dogovorom za sastanak.

Uobičajeni način izvršenja je da izvršilac nastoji, najpre, da dođe do „prijateljskog“ zbližavanja porukama koje će kod deteta učvrstiti ubeđenje da komunicira sa osobom koja ima razumevanja za detetova razmišljanja, deli interesovanja za iste društvene mreže i online igre i sl. Poseban aspekt te problematike se vezuje upravo za delovanje u virtuelnom svetu, naročito u vidu nesposobnosti dece da shvate značaj prosleđivanja različitih informacija, različitim putevima na internetu, pa tako se navodi gde rade tata ili mama, kako se roditelji zovu, koliko godina imaju, kavo im je radno vreme, kada su i koliko odsutni od kuće, što može biti od koristi izvršiocu.

Potom se izvršilac okreće nenametljivom uvođenju deteta u razgovore o intimnim stvarima, postepenom izlaganju detetu seksualno eksplicitnih materijala. Zatim se neagresivno predlaže „screen-to-screen“ ćaskanje

ili komuniciranje preko veb-kamere, što obično vodi dalje u dobrovoljno slanje sopstvenih kompromitujućih fotografija deteta. Konačno, izvršilac dogovara mesto i vreme sastanka. Izvršioci se, pri svemu tome, lažno predstavljaju ili upotrebljavaju podatke drugih maloletnih lica kao i njihove fotografije da bi se lažno predstavili žrtvama kao vršnjaci. Dešava se da se lažni identitet upotrebi više puta za vršenje istih ili različitih kriminalnih radnji.

Onlajn podvođenje maloletnika je veoma frustrirajuće za mnoge optužene jer ne zahteva završni «akt» sa maloletnim licem, a naime da je izvršeno neko od pobrojanih krivičnih dela. Tipičan optuženi će tvrditi: „Ja je nisam pipnuo, zašto sam optužen?“ Sa stanovišta odbrane, okrivljeni je, u suštini, optužen za jednostavan čin komunikacije na određeni način sa maloletnim licem.

Za traženje na internetu ili online podvođenje maloletnika, način kontakta mora uključivati neku vrstu komunikacije elektronskim putem. Dokle god je metod elektronski i razgovor istovremeno uključuje zahtev za susret sa detetom kako bi se izvršilo neko od navedenih dela, optuženi može biti optužen za grooming.

Kada se sagledaju iskazi oštećenih lica, može se videti da su pretežno ženskog pola, a što se tiče posledica, različito se izjašnjavaju. Neke žrtve navode da su imale noćne more, da se plaše da upoznaju nove ljude, da ne smeju više noću da se kreću same, zatvorile su profile, i nakon dosta vremena još uvek osećaju sramotu jer je npr. cela škola videla golišave slike, ili da i dalje ima osećaj stida pred ocem. Pojedine žrtve su rekle da je to neprijatno iskustvo dovelo do raskola u porodici, do međusobnog okrivljavanja kako između roditelja, tako i između roditelja i dece, što je za njih bila još dodatna frustracija.

U situaciji ne baš bogate domaće sudske prakse ukazaćemo na neka iskustva država koje se odavno, u velikom broju i već duže vreme suočavaju sa ovim krivičnim delom. Između ostalog, postavilo se i pitanje da li je optužba neodrživa ukoliko je optuženi imao komunikaciju sa pripadnikom policije koji se samo predstavljao kao dete? U nekim slučajevima, okrivljeni su se branili da su ih policajci agresivno ciljali da ih ubede da počine krivično delo koje oni inače nisu imali predispoziciju da počine. Nameštaljka, klopka, podstrekivanje, provocirano krivično delo - sve je ovo bila teza odbrana. Mnoge države u SAD su baš zato promenile svoje zakone kako bi omogućile osudu zasnovanu na verovanju okrivljenog da razgovora sa maloletnim licem. Još jedan odbrambeni ugao je pokušaj da se dokaže da optuženi nije znao da je osoba sa druge strane maloletna. Većina država ima zakone po kojima država nije dužna da dokaže da je optuženi znao koliko je dete bilo staro, već samo da je znao da je u pitanju maloletno lice.

Optuženi se brane i pozivanjem da su mu prekršena prava na slobodu govora, ali takva odbrana nije uspešna. Primer sledećeg navoda odbrane je da je razgovor bio samo onlajn fantazija ili dokazivanje da okrivljeni nikada nije ni nameravao da zaista susretne maloletnika. Imajući u vidu da je izvršenje ovog krivičnog dela po našem zakonodavstvu neophodno da se izvršilac pojavi na mestu sastanka, slučajno zaticanje na istom mestu bi bilo teško prihvatljivo.

Poslednjih godina uočena je pojava „sekstinga“ (kovanica od reči sex i texting) veoma zastupljena među tinejdžerima, koja podrazumeva razmenu tekstualnih poruka eksplicitnog sadržaja i fotografija na kojima se vide nagi delova tela i/ili seksualni čin. Poruke i fotografije se, pre svega, razmenjuju između vršnjaka, s tim što jedanput poslata poruka lako stiže do onih kojima nije bila namenjena. Visok procenat adolescenata praktikuje danas seksting, a sve više se sada govori o posledicama koje takvo ponašanje može da izazove u tinejdžerskim godinama. Greška mladog čoveka može dovesti do odbacivanja ili ismevanja od strane vršnjaka, ali i posledica koju seksting može imati i na društveni ugled, pa čak i kasniju mogućnost zaposlenja. Izlaganje fotografija i ličnih podataka može da rezultira negativnim posledicama i onda kada nije reč o fotografijama koje prikazuju nagost. Fotografije mogu biti smeštene u negativan kontekst, propraćene negativnim komentarima, što može pogubno uticati na samopouzdanje deteta.

Ovde će se prikazati zanimljiv primer iz američke države Ilinoj, gde osoba vrši krivično delo dečije pornografije ako snimi ili fotografiše lice za koje zna je mlađe od 18 godina i koje je angažovano u bilo kom seksualnom aktu ili u pozi koja uključuje nepristojno prikazivanje nage osobe ili genitalija, stidne oblasti, zadnjice ili ženskih grudi. Ne postoji izuzetak za slikanje sebe. Traženje ili mamljenje osobe, za koju bi trebalo da zna da je mlađa od 18 godina, da se pojavi na takvoj slici ili video-zapisu sankcioniše se kao dečja pornografija, ali i prosleđivanje seksting-poruka drugima ili širenje takvih slika drugima. Delo vrši i osoba koja, znajući sadržaj ili prirodu, poseduje fotografiju ili film koji prikazuje nekoga za koga treba da zna da je maloletno. Posedovanje se smatra voljnim, kad osoba „svesno nabavi ili dobije“ nezakoniti materijal „sa dovoljno vremena da okonča posedovanje“.

Sledeći primer stavlja prethodno navedena dela u perspektivu: šesnaestogodišnja devojka koja snima seksualnu sliku sebe polugole i pošalje je kao telefonsku poruku svom dečku izvršila je najmanje tri krivična dela: stvaranje, širenje i posedovanje dečje pornografije. Ako joj je njen dečko tražio da mu pošalje takvu poruku, on će odgovarati za najmanje dva krivična dela: navođenje i dobrovoljno posedovanje seksting-poruke. Tako, jedna ne baš mudra mladalačka nesmotrenost može rezultirati u pet krivičnih dela i par tinejdžera je spremno za upisivanje u registar „seksualnih prestupnika“. (*)

* https://www.isba.org/ibj/04/2010/sextingitsnojokeitsacrime

5. Cyberbullying

Bullying- vršnjačko nasilje je neželjeno, agresivno ponašanje među decom školskog uzrasta koje uključuje stvarnu ili percipiranu neravnotežu moći. Cyberbullying je takvo ponašanje koje se javlja na internetu upotrebom pretećeg ili zlog jezika u nameri uznemiravanja ili emocionalnog povređivanja jedne osobe ili grupe ljudi, slanjem tekstualnih poruka, elektronske pošte, u online igricama, sobama za četovanje, na diskusionim grupama ili veb-stranicama i dr.

Ponašanje se ponavlja ili ima potencijal da se ponovi tokom vremena. Deca koja su maltretirana, ali i ona koja maltretiraju druge, mogu imati ozbiljne, trajne probleme. Potreba da se drugi maltretira obično potiče iz nasilnog ponašanja negde drugde u životu dece, koja u školi ili na drugim mestima ponavljaju ona ponašanja koja su iskusila, videla ili naučila kod kuće.

Jedan od početnih koraka za izvršenje krivičnog dela je i krađa identiteta. Informacije od značaja za izvršioce krivičnih dela koji se bave krađom identiteta širom sveta obuhvataju imena i prezimena, adrese, zdravstvene podatke i sve drugo što kasnije mogu da zloupotrebe. Za krađu identiteta vrlo često se upotrebljavaju računarski virusi koji obavljaju funkcije, kao što su snimanja otkucaja karaktera na tastaturi (keylogger), snimanje procesa na monitorima računara (screen logger), redirekcije internet-saobraćaja, ubacivanje „trojanaca“ u sistem, krađa ličnih i drugih podataka korisnika i njemu bliskih lica. Do ličnih podataka može se doći i bez korišćenja računara krađom podataka iz lične pošte, krađom elektronskih uređaja - mobilnih telefona, tableta ili pronalaženjem zaboravljenih ili izgubljenih predmeta u kojima se nalaze lični podaci, kao što su novčanici, notesi i telefonski imenici. U okviru cyberbullying-a govori se i o krađi ili pogađanju lozinke deteta, pa se zatim ta lozinka menja ili se blokira, zaključava, tako da dete više ne može da pristupi svom nalogu. Posle krađe obično sledi zloupotreba identiteta, koja podrazumeva upotrebu ličnih podataka nekog lica koji su prethodno pribavljeni bez njegovog znanja i odobrenja za izvršenje krivičnih dela pod njegovim identitetom.

Kada se govori o nasilju preko interneta, ono, između ostalog, podrazumeva:
- slanje uznemirujuće poruke mejlom ili na četu,
- slanje poruka neprimerenog sadržaja,
- slanje neželjene pošte, spemova i virusa putem elektronske pošte ili na bilo koji drugi način na internet mreži,

- slanje fotografija koje vređaju dostojanstvo, integritet, slobodu i bezbednost,
- krađa ili promena lozinke za mejl ili nadimak na četu,
- objavljivanje privatnih podataka ili neistine na četu, blogu ili internet-stranici,
- postavljanje internetske ankete o žrtvi,
- podsticanje govora mržnje i mržnje uopšte na internetu,
- podsticanje komunikacije uvreda i nipodaštavanja,
- prosleđivanje tuđih fotografija i traženje komentara ili bilo kakvog sadržaja o drugome sa zahtevom za komentarisanje,
- povređivanje privatnosti upadanjem u tuđi kompjuter i čitanjem tuđih sadržaja komunikacije na internetu,
- lažno predstavljanje i upotrebu lažnog identiteta,
- proizvodnju i distribuciju dečje pornografije(*).

Osim navedenih, primeri online nasilja podrazumevaju i slanje pretnji, provokativnih uvreda ili rasne ili etničke uvrede, seksualno pogrdno obraćanje, deljenje primljenih E-mail-ova bez dozvole onog koji ga je napisao, zastrašivanje i pretnje ili stvarno nasilje, ili drugi oblici diskriminacije usmereni na lica koja su (ili za koja izvršilac smatra da su) pripadnici LGBT populacije, zatrpavanje E-mail inbox-a nasilnim porukama, deljenje slika snimljenih u neprijatnim situacijama, bez dozvole lica na fotografiji, ubeđivanje drugih da isključe nekog iz zajednice (online ili offline), postavljanje ili širenje lažnih informacija o osobi sa ciljem da se povredi ta osoba ili njena/njegova reputacija, slanje u više navrata neprijatnih, zlih poruka, ruganje, spletkarenje.

Ovde treba ukazati da je Protokolom postupanja u ustanovi u odgovoru na nasilje, zlostavljanje i zanemarivanje(**) navedeno da nasilje i zlostavljanje mogu da se jave kao fizičko, psihičko (emocionalno) i socijalno. Osim navedenih oblika, nasilje i zlostavljanje prepoznaju se i kroz: zloupotrebu, seksualno nasilje, eksploataciju deteta i učenika, elektronsko nasilje i dr. Elektronsko nasilje i zlostavljanje su zloupotreba informacionih tehnologija koja može da ima za posledicu povredu druge ličnosti i ugrožavanje dostojanstva i ostvaruje se slanjem poruka elektronskom poštom, SMS-om, MMS-om, putem veb-sajta, četovanjem, uključivanjem u forume, socijalne mreže i sl.

Oblici psihičkog nasilja i zlostavljanja su, naročito: omalovažavanje, ogovaranje, vređanje, ruganje, nazivanje pogrdnim imenima, psovanje, etiketiranje, imitiranje, „prozivanje“, ucenjivanje, pretnje, nepravedno kažnjavanje, zabrana komuniciranja, isključivanje, manipulisanje, zastrašivanje.

* http://internetbezbednost.weebly.com/10801085109010771088108510771090109 1-10851072-10531072108910801113 1077.html

** „Službeni glasnik RS“ br. 2010/30

Oblici socijalnog nasilja i zlostavljanja su, naročito: dobacivanje, podsmevanje, isključivanje iz grupe ili zajedničkih aktivnosti, favorizovanje na osnovu različitosti, širenje glasina, spletkarenje, uskraćivanje pažnje od strane grupe (ignorisanje), neuključivanje, neprihvatanje, manipulisanje, iskorišćavanje, pretnje, izolacija, maltretiranje grupe prema pojedincu ili grupi, organizovanje zatvorenih grupa (klanova), što za posledicu ima povređivanje drugih. Oblici seksualnog nasilja i zlostavljanja su, naročito, neumesno, sa seksualnom porukom: lascivni komentari, širenje priča, etiketiranje, pokazivanje pornografskog materijala, pokazivanje intimnih delova tela, svlačenje.

Oblici nasilja i zlostavljanja zloupotrebom informacionih tehnologija i drugih komunikacionih programa su, naročito: uznemiravajuće pozivanje, slanje uznemiravajućih poruka SMS-om, MMS-om, oglašavanje, snimanje i slanje video zapisa, zloupotreba blogova, foruma i četovanja, snimanje kamerom pojedinaca protiv njihove volje, snimanje nasilnih scena kamerom, distribuiranje snimaka i slika, dečija pornografija. Sve navedeno, iako se tiče prosvete, a imajući u vidu da se govori o vršnjačkom nasilju, može biti od koristi kako tužiocima, tako i sudijama u predmetima po kojima će postupati radi pravilne ocene da li se u konkretnom slučaju može nesumnjivo (u)tvrditi da se radi o protivpravnom ponašanju.

"Cyberbullying" se uglavnom posmatra kao situacija kada jedno dete odabere kao cilj drugo dete, koristeći interaktivnu tehnologiju. Vršnjačko nasilje može da traje mnogo duže nego što traje školovanje i prati žrtve svuda gde god koriste svoje mobilne telefone ili gde se loguju na internet, može se događati 24 sata dnevno, 7 dana u nedelji, u bilo koje doba dana ili noći, može doći do deteta čak i kada je samo. Poruke i slike mogu se objaviti anonimno i brzo se distribuirati širokoj publici. Može biti veoma teško, a ponekad i nemoguće pratiti izvor, dok je brisanje neprimerenih ili uznemiravajućih poruka, tekstova i slika gotovo nemoguće nakon objavljivanja ili slanja.

Postoje dva načina cyberbullying-a, a to su: direktni napadi, tj. poruke koje su poslate detetu direktno, ili one koje su poslate preko drugih, koji u tome treba da im pomognu, bez obzira da li su oni toga svesni ili ne. To je „cyberbullying pomoću „proxy"-ja, koji često obuhvati i odrasle koji su uključeni u to i samim tim je opasniji za više lica.

Direktni napadi se izvršavaju putem tekstualne poruke, ponekad i hiljade tekstualnih poruka na mobilni telefon, kada deca šalju poruke mržnje ili preteće poruke drugoj deci, a da ponekad nisu da svesni da, iako nisu

izrečene u stvarnom životu, takve poruke su veoma podobne da povrede i umeju da budu veoma ozbiljne. Ovi napadi mogu biti i na blogovima ili na veb-sajtovima. Naime, danas su deca toliko tehnološki opismenjena da znaju da kreiraju internet stranicu, specifično dizajniranu kako bi se neko vređao. Dalje, deca vrlo često fotografišu druge u svlačionicama ili ukoliko su u mogućnosti u kupatilu, toaletima i onda postavljaju te slike ili ih šalju drugima putem mobilnih telefona. Direktni napadi čine deca koja šalju viruse ili spyware i koji na taj način prosto špijuniraju njihovu žrtvu. „Trojanci" takođe omogućuju cyberbullying i to na taj način da kontrolišu sa daljine računar žrtve ili koriste svoja umeća kako bi se izbrisao hard-disk žrtve.

Internet polling predstavlja neku vrstu ankete kojima se postavljaju pitanja i pozivaju drugi da glasaju ko je od ponuđenih vršnjaka najdeblji, najružniji, itd. Takođe, mogu da se postave pitanja tipa: ko jeste zgodan ili zgodna a ko nije, ili who›s hot, who›s not, ili ko je najveća „drolja" ili „najveća daska" u određenom razredu. Pitanja su, uglavnom, veoma uvredljiva, a najstrašnije je to što ih kreiraju deca ili tinejdžeri. Što se tiče gaming-a, ogroman broj dece igra interaktivno igrice bilo na Sony playstation, Xbox live ili računaru. Igra se često online i pruža se mogućnost međusobne komunikacije putem četovanja ili live internet-veze sa bilo kim ko istovremeno igra. Tada ponekad deca verbalno -maltretiraju drugu decu, koriste pretnje ili neki ružan rečnik, a ponekad čak idu i korak dalje, isključujući ih iz igara, ili šire nekakve lažne vesti o njima.

Cyberbullyng pomoću proxy-ja je jedan od najozbiljnijih i najopasnijih vrsta, jer vrlo često uključuje odrasle osobe. To se najčešće čini tako što se maltretiranje, u stvari, sprovodi preko nekoga ko obavlja „prljav posao", vrlo često bez svoje volje i bez znanja da se to čini uopšte. Warning ili notify words su primeri ovakvog cyberbullying-a putem proxy-ja. Deca, naime kliknu na dugme za upozorenje ili za obaveštenje na njihovom ekranu, četu ili na i-mejl stranici i na taj način upozoravaju internet-provajdera da je žrtva učinila nešto što krši njihova pravila. Pružaoci usluga su upoznati sa ovom vrstom zloupotrebe, često proveravaju da bi videli da li je upozorenje zaista opravdano. Ali, sve što izvršilac treba da učini je da dovoljno razljuti žrtvu toliko da ona sada zaista pošalje nekakav ružan komentar ili komentar pun mržnje. Tačnije, da uzvrati takvim komentarom, što je dovoljno, pa u takvoj situaciji, pošto je provajder već jedanput upozoren (lažno), ponovo se upozorava na isti način tako se predstavlja kao da je žrtva ta koja je sve započela. U tom slučaju, Internet Service Provider je, u stvari, jedan nedužni saučesnik u ovom cyberbullying procesu. Ponekad su ti neželjeni saučesnici i roditelji same žrtve. Ukoliko izvršilac može da učini da izgleda kao da žrtva radi nešto pogrešno, loše i o tome obavesti žrtvine roditelje, velika je verovatnoća da će roditelji žrtvu kazniti. Vrlo često će se desiti da izvršioci zlonamerno registruju žrtvu za E-mailing ili za instant-poruke na pornografskim stranicama.

Tada se desi da žrtva primi stotine i-mejlova od takvog sajta. Osim ovoga, može biti i mnogo ozbiljnije, a to je u situacijama kada izvršioci postavljaju informacije o žrtvi u chat room-ove zlostavljača dece i čak reklamirajući žrtvu za seks. Onda oni prosto samo sede i čekaju da članovi te hate grupe ili grupe za zlostavljače dece napadaju ili kontaktiraju žrtvu bilo online, a ponekad čak i offline. Zamena ličnosti, odnosno predstavljajući se kao žrtva, izvršilac može da načini značajnu štetu. Oni mogu da postave provokativnu poruku u chat room neke hate grupe i na taj način pozivaju na napad prema žrtvi, vrlo često ostavljaju ime, adresu, pa i telefonski broj žrtve, što dalje prouzrokuje da hate grupa ima vrlo lak posao. Drugo, izvršioci često šalju poruku nekome predstavljajući se da su oni, u stvari, žrtve, govoreći neke preteće stvari ili govor mržnje. Takođe, oni mogu da izmene poruku koja dolazi od žrtve, tako da zamene uloge u tekstu, predstavljajući da je žrtva, u stvari, rekla ružne stvari o nekom drugom.

Cyberbullying je situacija kada su u celu priču uključeni samo maloletnici i to sa obe strane, bilo kao izvršilac bilo kao žrtva, ili makar treba da bude inicirano od strane maloletnika prema drugom maloletniku. Kod vršnjačkog nasilja, izvršioci uvek pokušavaju da uključe što više drugih u celu ovu priču. Odrasli se mogu uključiti u ovu priču najčešće kada se upravo na ove sajtove za zlostavljače dece ili za seksualne „predatore“ zainteresuju za te postove, naročito ukoliko je postavljen navod da je žrtva zainteresovana navodno za seks što može da vodi u grooming . U stvarnosti se vrlo često dešava i da u jednom trenutku onaj ko je žrtva postane izvršilac i obratno. Posledice mogu da budu od onih koje nisu tako ugrožavajuće, do ubistva počinjena ili do samoubistava počinjenih nakon što je neko bio uključen u cyberbullying.

Kada je reč o motivima izvršioca, vrlo često se radi o nekom besu, osveti ili prosto frustraciji. Nekada to čine radi svoje „zabave“ ili zato što im je dosadno, ili imaju previše vremena i previše gadget -a, odnosno previše tehnoloških „igrački“ koje su im dostupne. Mnogi to čine prosto radi sticanja pažnje ili prosto reakcije drugih. Dešava se i da se to učini slučajno, ili se pošalje poruka pogrešnom primaocu, ili se ne razmišlja pre nego što se bilo šta od svega navedenog do sada učini. Oni koji su željni neke nadmoći ili moći nad drugima, to čine da bi mučili druge ili zbog svog ega.

Međutim, treba imati u vidu da je moguće i pogrešno razumevanje. Otkucana reč prosto ne može da iskaže kakav ton bi pratio izgovorenu reč i svakako se značajno razlikuje od informacije koju bi dobili kada bi čuli glas osobe koja se obraća ili videli govor tela. Treba, dakle, razmišljati i o objektivnom kriterijumu dobijenih informacija prilikom procene ili ocene, a ne da se one baziraju samo na tome kako su se te reči učinile žrtvi, vodeći svakako računa o uzrastu, s obzirom da ta ocena može biti pogrešna i ponekad se teško može izbeći da

se reči protumače izvan konteksta. Te reči, ukoliko nisu praćene nekim emotikonom ili akronimom kao „jk“, u smislu just kidding, mogu biti pogrešno shvaćene. Sve to onda dalje može da rezultira u povređenim osećanjima, u ljutnji i besu, u frustraciji ili osećaju straha, ili prosto osećaju da neko preti.

Pregled sudske prakse

Rešenjem Veća za maloletnike, prema maloletnom licu je izrečena mera upozorenja sudskog ukora i to zbog krivičnog dela ugrožavanja sigurnosti iz člana 138. stav 1. Naime, maloletna je ugrozila sigurnost oštećenog maloletnog lica na taj način što je sa svog mobilnog telefona na njegov uputila poruku sadržine: „Iseli se iz našeg grada, bilo bi ti bolje, . . . crno ti se piše“. Branila se tako što je rekla da je bila sa drugaricom u piceriji kada joj je ona ispričala da je oštećeni pričao za nju da je trudna i da je kurva. Zatražila je njegov broj telefona i sa svog mu poslala poruku sa navedenom sadržinom. Oštećeni je u svom iskazu naveo da se uplašio za svoju ličnu bezbednost, jer su reči „crno ti se piše“ bile napisane velikim slovima, a poruku je primio sa nepoznatog broja. Sud je, u toku dokaznog postupka, izvršio uvid u kriminalističko-tehničku dokumentaciju, utvrdio tekst poruke, datum slanja i broj sa kojeg je poslata a potom je izvršen uvid i u listing odlaznih poruka sa mobilnog telefona maloletne. Sud je zaključio da se u radnjama maloletne stiču svi zakonski elementi krivičnog dela iz člana 138. stav 1, nalazeći da poruka sa navedenom sadržinom predstavlja ozbiljnu pretnju s obzirom da je objektivno podobna da kod onoga kome se preti, odnosno oštećenog, izazove osećaj straha ili nesigurnosti, što je oštećeni potvrdio.

Drugi primer za isto krivično delo je presuda kojom je okrivljeni oglašen krivim što je ugrozio sigurnost oštećenog pretnjom da će napasti na život i telo tog lica na taj način što je internet-mreži fejsbuk sa svog korisničkog profila poslao oštećenom preteće poruke, između ostalog i sadržine: „Mrtav si, majmune, odrobijaću te“, a potom je na svom korisničkom profilu postavio sliku na kojoj se nalazio oštećeni sa zaokruženom glavom na kojoj je bio postavljen tekst: „Poslednji pozdrav“.

Primer za krivično delo iz člana 138. stav 2. je presuda kojom je okrivljena oglašena krivom što je sa svog kućnog računara ugrozila sigurnost više lica - dve oštećene, pretnjom da će napasti na njihov život i telo tako što je na internet-prezentaciji društvene mreže fejsbuk sa korisničkog profila, koji je kreirala pod lažnim imenom, na korisnički profil maloletne oštećene uputila pretnje: „Slušaj mala, poruči mami da se smiri da joj ne bi jebali mamu, . . ., reci joj da se smiri da ne bi mi tebe maltretirali . . . ovo je poslednja opomena, doći ću i razvaliću je od batina“.

Pred Višim sudom u Beogradu doneta je presuda kojom je prihvaćen sporazum o priznanju krivičnog dela iskorišćavanja računarske mreže ili komunikacija drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu iz člana 185b. stav 1. KZ u vezi sa članom 184. stav 2. u vezi sa članom 30. KZ i to koje je okrivljenom stavljeno na teret.

Okrivljeni je oglašen krivim što je u stanju uračunljivosti, svestan svog dela da je zabranjeno, pri čemu je hteo njegovo izvršenje, u nameri da izvrši krivično delo posredovanja u vršenju prostitucije iz člana 184, stav 2, u vezi sa stavom 1, koristeći računarsku mrežu, sa umišljajem pokušao da dogovori sastanak sa maloletnom oštećenom starom 13 godina na taj način što je sa svog mobilnog telefona elektronskim putem, koristeći svoj fejsbuk-profil stupio u kontakt sa oštećenom, kojoj je najpre poslao zahtev za prijateljstvo da bi, nakon što ga je oštećena prihvatila i saopštila mu da ima 14 godina, počeo da joj šalje poruke seksualne sadržine, kao i poruke kojima je navodi i podstiče na prostituciju: „Ćao, mačkice, ajde da ti dam 500 evra mesečno za povremeno viđanje u tajnosti“, “Važi, mačkice moja . . . ako budeš dobra u krevetu onda i više ćeš da dobiješ, jesi već vodila ljubav sa nekim“, i slično, zatim je tražio broj telefona oštećene, nakon čega je oštećena prekinula komunikaciju sa njim. Osuđen je na kaznu zatvora u trajanju od 1 godine, koja će se izvršiti u kućnim uslovima uz elektronski nadzor, i izrečena je novčana kazna u iznosu od 50.000,00 dinara, kao i mera bezbednosti oduzimanja predmeta, računara, mobilnih telefona.

Prema okrivljenom je, na osnovu člana 89a KZ izrečena, mera bezbednosti zabrane približavanja i komunikacije sa oštećenom i to na udaljenosti manjoj od 200 metara, stanu u kome oštećena živi i osnovnoj školi koju pohađa maloletna oštećena, a zatim je na osnovu člana 7, stav 1, tačka 2, i 3, Zakona o posebnim merama za sprečavanje vršenja krivičnih dela protiv polne slobode prema maloletnicima, (tzv. Marijin zakon) prema okrivljenom izrečena mera zabrane posećivanja mesta na kojima se okupljaju maloletna lica (vrtići, škole i slično) i obavezno posećivanje profesionalnih savetovališta i ustanova.

Određeno je da će se mere sprovoditi posle izdržane kazne zatvora, najduže 20 godina posle izvršene kazne zatvora, s tim što će sud po službenoj dužnosti po isteku svake 4 godine od početka primene ovih mera odlučiti o potrebi njihovog daljeg sprovođenja.

Primer za 185b KZ je još jedan prihvaćen sporazum o priznanju krivičnog dela, kojim je okrivljeni oglašen krivim što je, u nameri da izvrši obljubu nad detetom koristeći računarsku mrežu, sa umišljajem pokušao da dogovori sastanak sa oštećenim detetom, starim 11 godina, na taj način što je sa svog mobilnog telefona, elektronskim putem preko interneta na društvenoj mreži fejsbuk, na kome se lažno predstavljao kao dvanaestogodišnji dečak, stupio u kontakt sa oštećenim dečakom, predstavljajući se kao dečak koji ga zna sa fudbala, da bi nakon toga počeo da mu šalje poruke seksualne sadržine, na primer: „Kad bi te uhvatio, oborio bi te u krevet, onda bi ti noge raširio i onda znaš“, „Znaš gde bi te jebao, stavio bi ti moju kitu i jako te udarao, da l' da budem jako grub ili malo prema tebi, 'oćeš da ti kažem kako bi te rasturio, znaš šta volim da radim dečacima posle utakmice“, da bi mu poslao poruke u kojima navodi da želi da dođe na trening određenog datuma upozna se sa maloletnim oštećenim, te da će doći u svlačionicu nakon treninga, nakon čega je oštećeni prekinuo komunikaciju sa njim.

Osuđen je na kaznu zatvora u trajanju od 1 godine, i to u prostorijama u kojima stanuje, izrečena mera bezbednosti oduzimanja mobilnog telefona i SIM kartica, a primenjena je odredba člana 89a KZ - izrečena mera bezbednosti zabrana približavanja i komunikacije sa oštećenim i to na udaljenosti od 200 metara, zabranjen je pristup u prostor oko mesta stanovanja oko škole koju maloletni pohađa i 200 metara od škole fudbala te sportske sale, zabranjeno mu je uznemiravanje oštećenog, odnosno dalja komunikacija sa oštećenim, i ta mera prema izreci presude može trajati najduže 3 godine. Primenjena je i odredba člana 7, stav 1, tačka 2, i 3, Zakona o posebnim merama za sprečavanje vršenja krivičnih dela protiv polne slobode prema maloletnicima, i to: zabrana posećivanja mesta na kojima se okupljaju maloletna lica i obavezno posećivanje profesionalnih savetovališta i ustanova.

Primer je i presuda kojom je okrivljeni oglašen krivim zbog izvršenja krivičnog dela iz člana 185, stav 2, u vezi sa stavom 1. u vezi sa članom 180. stav 1. i zbog izvršenja krivičnog dela iz člana 185. stav 4. KZ i to zato što je u nameri da izvrši obljubu sa detetom, koristeći računarsku mrežu i komunikaciju drugim tehničkim sredstvom – mobilnim telefonom, sa umišljajem dogovorio sastanak sa maloletnom oštećenom, starom dvanaest godina, i pojavio se na dogovorenom mestu radi sastanka, tako što je elektronskim putem, preko interneta, na društvenoj mreži fejsbuk, koristeći svoj korisnički profil, stupio u kontakt sa oštećenom, uputio joj poruku: „Lep pozdrav za tebe, hvala ti za dodavanje ... vrlo si lepa i posebna ... voleo bih da se više upoznamo ... ako si malo više znatiželjna, imam neke jako lepe priče za tebe, intrigantne ...posebne ... vrlo si slatka ... ženstvena i vrlo seksi“, nakon čega je maloletna oštećena prijavila poruku svojoj majci, koja je promenila lozinku navedenog profila, nastavila da komunicira sa okrivljenim, predstavljajući se kao dete, da bi nakon toga okrivljeni u porukama koje

su poslate preko ove mreže počeo da joj upućuje poruke eksplicitnog sadržaja, sa seksualnom konotacijom poput: „Jako bih voleo da te diram i još nešto ... pa normalno da želim da uđem u tebe ili da te jebem ... kako hoćeš ... recimo da svojom rukom stavljam u tebe ... i da te gledam i slušam kako svršavaš ... uzimam samo najbolje i najmlađe ... mnogo volim da jebem tri curice u krug ... najmlađa dvanaest ... one dve starije za godinu ... dobiju poklon, ali ja odlučujem o tome, ako ti se bude posrećilo možda ga i ti primiš .... jako želim da ti ga trpam i u guzu, da ti svršavam u usta, po sisama ... kolike su ti ...“, sve vreme u ubeđenju da komunicira sa detetom, nakon čega je dogovorio da se sa detetom sastane u Beogradu, pri čemu se pojavio na zakazanom sastanku kako bi se upoznao sa detetom, u nameri da izvrši krivično delo obljuba sa detetom iz člana 180. stav 1. KZ, nakon čega je lišen slobode, kao i što je posedovao 606 slika pornografske sadržine, nastalih iskorišćavanjem maloletnih lica. a što je pronađeno prilikom pretresa stana u kojem stanuje. Prema okrivljenom je izrečena mera bezbednosti oduzimanja predmeta – laptopa, dve fleš memorije, jedan mobilni telefon i primenjena odredba člana 7. u vezi sa članom 9. i 10. Zakona o posebnim merama za sprečavanje vršenja krivičnih dela protiv polne slobode prema maloletnicima, i to: zabrana posećivanja mesta na kojima se okupljaju maloletna lica, kao što su školske zgrade, školska dvorišta, vrtići, igrališta, dečije manifestacije i sl., kao i obavezno posećivanje profesionalnih savetovališta i ustanova prema programu koji će mu biti određen od strane organizacione jedinice Uprave za izvršenje krivičnih sankcija, nadležne za tretman i alternativne sankcije. Navedene mere će se sprovoditi prema okrivljenom nakon izdržane kazne zatvora.

Apelacioni sud u Beogradu je odbio kao neosnovanu žalbu branioca okrivljenog i potvrdio navedenu presudu. U obrazloženju odluke se navodi da je postojanje komunikacije, između dva profila na društvenoj mreži fejsbuk, deteta i okrivljenog, telefonskim putem preko SMS poruka i poziva te sadržine poruka, nije sporio ni okrivljeni, a potvrđena je pismenim dokazima u spisima, i to: zapisnikom o pretresanju stana i drugih prostorija, potvrdi o privremeno oduzetim predmetima, izveštajem o prikupljanju podataka iz mobilnih telefona, veštačenjem CD medija (pregled uređaja), kao i izveštaja MUP Direkcije policije UKP. Optuženi se branio da nije zainteresovan za decu i devojčice mlađeg uzrasta, kao ni za dečiju pornografiju, ali i da nije komunicirao sa detetom, već da je sve vreme znao da se dopisuje sa majkom. Međutim takva odbrana osnovano od strane prvostepenog suda nije prihvaćena kao verodostojna. Nesumnjivo je utvrđeno da je okrivljeni i ranijem tokom 2014 ,2013. i 2016. godine, koristeći računarsku mrežu, kontaktirao sa maloletnim devojčicama drugih korisničkih profila, gde je sadržina tih poruka takođe bila seksualne konotacije, što je prvostepeni sud nesumnjivo utvrdio iz veštačenja CD medija. Na laptop-računaru koji je od okrivljenog oduzet, kao i na dve USB fleš memorije, pronađeno je i oduzeto ukupno 606 fotografija sa dečijom pornografijom, a posedovanje takvog materijala okrivljeni nije sporio, a potvrdili su ga i pisani dokazi u spisima. Da je okrivljeni sve vreme komunikacije tokom

koje je dogovorio sastanak sa maloletnom oštećenom bio uveren da ih šalje detetu, da je to i hteo upravo u nameri da izvrši obljubu sa detetom, prvostepeni sud je nesumnjivo utvrdio kako iz sadržine poslatih poruka, koje se u većini odnose na seksualne odnose sa decom, tako i ocenom ostalih pisanih dokaza u spisima, ali i iskaza majke maloletne svedoka, koji je u svemu saglasan sa materijalnim dokazima. Dalje je sud utvrdio da je okrivljeni došao na dogovoreni sastanak, da je menjao mesto gde će se naći insistirajući da to bude na autobuskoj stanici, da će on stajati u bočnoj ulici i biti u parkiranom vozilu sa uključenim migavcima, da maloletna dođe do kola, a u telefonskom razgovoru je i ponovio da joj je poneo mobilni telefon koji joj je prethodno obećao.

Primer za krivično delo prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju iz člana 185, stav 3, u vezi sa stavom 1. i 2. i stav 4. KZ i krivično delo iskorišćavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu iz člana 185b stav 2. u vezi sa stavom 1. KZ u vezi sa članom 180. stav 1. KZ u vezi sa članom 30. KZ je i postupak u kojem je okrivljenom stavljeno na teret da je učinio dostupnim slike i audio-vizuelni materijal pornografske sadržine detetu starom 8 godina, i u više navrata iskoristio dete za proizvodnju slika pornografske sadržine na taj način što je preko interneta, putem društvene mreže fejsbuk, preko svog korisničkog profila, stupio u kontakt sa oštećenom i u više navrata slao slike svog polnog organa u erekciji i prilikom ejakulacije i video-snimak na kom se samozadovoljava, te od oštećene zahtevao da mu šalje svoje slike na kojima je ona naga i, pri tom, davao uputstva na koji način i koje delove da slika, što je ona učinila i poslala mu ukupno 8 slika, te je na elektronski način učinio dostupnim navedene slike pornografske sadržine nastale iskorišćavanjem maloletnog lica tako što je preko fejsbuka poslao tri fotografije na kojoj je maloletna oštećena naga korisnicima drugih profila. Osim toga, okrivljenom je dalje stavljeno na teret da je u periodu od nedelju dana, u nameri da izvrši obljubu sa detetom, koristeći računarsku mrežu fejsbuk, sa umišljajem pokušao da dogovori sastanak sa oštećenom na taj način što je uputio više poruka sledeće sadržine: „A znaš da mi je veliki, ja mislim da ti ne bi ceo mogao stati, hoćemo probati jednom to, mislim da vidimo da li bi ti mogao stati, pa jedino da ti dođeš kod mene, jer bi htela da jednu noć spavamo zajedno“, ali sa umišljajem započeto delo nije dovršio jer je oštećena prekinula kontakt sa njim. Od predloženih dokaza: zapisnik o pretresanju stana i drugih prostorija potvrda o privremeno oduzetim predmetima izveštaji službe za specijalne istražne metode o veštačenju hard-diska oduzetog od okrivljenog, deo komunikacije izdvojen u foto-dokumentaciji, komunikacija između okrivljenog i korisnika profila na koje je slao fotografije, predloženo je da se izvrši uvid u sadržaj medija koji je dostavljen uz izveštaj veštačenja elektronske opreme oduzete od okrivljenog, i to slike, kao i video-klip koji se nalaze u označenom folderu, kao i sadržaj CD medija dostavljenog spisima.

Sledeći primer krivičnog dela iz člana 185. stav 3. u vezi sa stavom 2, u sticaju sa krivičnim delom prinude iz člana 135. stav 1. je i osuđujuća presuda kojom je okrivljeni oglašen krivim da je iskoristio dete staro 13 godina za proizvodnju slika i video-klipova pornografske sadržine i ozbiljnom pretnjom da će fotografije oštećene, na kojima se nalazi bez odeće, i video-snimak na kojem je prikazana oštećena bez gornjeg dela odeće, postaviti na internet, prinudio oštećenu da nešto učini na taj način što je koristeći društvenu mrežu fejsbuk kreirao više lažnih profila, zatim od maloletne zahtevao da se fotografiše i svlači pred veb-kamerom koja je instalirana na njenom računaru, da prikazuje svoje gole grudi, svoj polni organ – vaginu, pri čemu je sve to snimao i čuvao na svom računaru. Navedeni materijal je koristio da bi pretio oštećenoj detetu da će fotografije objaviti javno i dostaviti njenim prijateljima i na taj način je prinudio da mu i dalje dostavlja svoje nage fotografije i svlači se pred veb-kamerom, te kada je maloletna htela da prekine kontakt, pretnje je ostvario postavivši navedene slike na "zid" fejsbuk-naloga oštećene i potom ih poslao njenim prijateljima iz osnovne škole. Za navedena krivična dela utvrđene su mu pojedinačne kazne, i to: uz primenu ublažavanja, najpre za 185. stav 3. u vezi sa stavom 2, kazna zatvora u trajanju od 10 meseci, a za krivično delo prinuda iz člana 135. stav 1. kazna zatvora od 3 meseca, te je osuđen na jedinstvenu kaznu zatvora u trajanju od 1 godine, koja se ima izvršiti u prostorijama u kojima osuđeni stanuje. Izrečena je i mera bezbednosti oduzimanja telefona, kućišta desktop-računara i SIM kartica.

Primer za krivično delo prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju iz člana 185. stav 2. u vezi sa članom 33. KZ je i primer presude kojom su okrivljeni oglašeni krivim što su iskoristili maloletnog oštećenog za proizvodnju audio-vizuelnog predmeta pornografske sadržine i pornografsku predstavu tako što su ga nagovorili da ima seksualni odnos sa kobilom, za koje vreme je jedan okrivljeni držao kobilu za uzde sprečavajući je da se udalji sa lica mesta, a drugi okrivljeni držao rep kako bi omogućio maloletnom oštećenom da ima polni odnos sa kobilom, podstičući ga na isti, a za to vreme je treći okrivljeni snimio polni odnos telefonom i snimak postavio na Youtube. Za navedeno krivično delo izrečenu su im uslovne osude.

Sledeći primer je primer ukinute presude za krivično delo iz člana 185b KZ, kojom je okrivljeni, student, neosuđivan, oglašen krivim što je, u nameri da izvrši nedozvoljenu polnu radnju nad maloletnikom, koristeći računarsku mrežu i komunikaciju, putem mobilnog telefona dogovorio sastanak sa oštećenom maloletnom i pojavio se na dogovorenom mestu radi sastanka, preko interneta, elektronskim putem, na društvenoj mreži fejsbuk, koristeći lažni profil, lažno se predstavljao kao devojka koja se bavi manekenstvom, stupio u kontakt sa oštećenom koja je imala četrnaest godina, uputio joj poruku da je lepa i zgodna, pitanje „da li bi želela da se bavi foto-modelingom", da će uvek imati šta poželi, make-up, garderobu, upitao koje je godište, oštećena je sve ovo prijavila svom ocu, koji je, zajedno s njom, nastavio da komunicira sa okrivljenim, da bi nakon toga okrivljeni u porukama počeo da upućuje pitanja: „kakav donji veš nosi, da li nosi haltere i štikle, da li pije i sl.",

poslao joj je poruku u kojoj je naveo da ukoliko želi na lakši način da postane foto-model može da ode kod njegovog šefa, da mu „izdrka“ ili „popuši“, a ako to ne želi da uradi njemu, može imati seksualni ili oralni odnos sa njegovim sinom, nakon čega je tražio broj mobilnog telefona, pa pošto mu ga je ona poslala, oštećenoj je poslao poruku da će broj telefona proslediti šefovom sinu, koji će s njom komunicirati putem mobilnog telefona, potom je kontaktirao, dogovorio se da se sa njom sastane u restoranu, pojavio se na sastanku, rekao joj da ga sačeka da uđe u muški toalet, da će je pozvati odakle i da ga oralno zadovolji, da bi nakon ulaska u toalet pozvao telefonom oštećenu i rekao joj: „Ajde, gde si više, čekam te“. Prvostepenom presudom je oglašen krivim i osuđen na kaznu zatvora u trajanju od šest meseci i novčanu kaznu u iznosu od 50.000,00 dinara, oduzet mu je mobilni telefon i kućište za kompjuter i izrečena mera u smislu člana 89a KZ i primenjena odredba člana 7. stav 1. tačka 2. i 3. Zakona o posebnim merama za sprečavanje. Okrivljeni se u ovom postupku branio ćutanjem, nije priznao izvršenje krivičnog dela.

Navedena presuda je ukinuta, s obzirom da je sadržala bitne povrede odredbi krivičnog postupka jer je izreka presude nerazumljiva i protivrečna sama sebi, a razlozi nejasni i nerazumljivi. Ovo stoga što prvostepeni sud nije opredelio krivično delo za koje je vezao odredbu člana 185b KZ. Naime, odredbom člana 185. KZ propisano je da je izvršilac ovog krivičnog dela onaj ko u nameri izvršenja krivičnog dela silovanje iz stava 4. (dete), obljuba nad nemoćnim licem, obljuba sa detetom, obljuba zloupotrebom položaja, nedozvoljene polne radnje, podvođenje i omogućavanje vršenja polnog odnosa, posredovanje u vršenju prostitucije, iskorišćavanje maloletnog lica za proizvodnju, itd.,i navođenje maloletnog lica na prisustvo polnim radnjama, iskoristi računarsku mrežu ili komunikaciju drugim tehničkim sredstvima, dogovori sa maloletnikom sastanak i pojavi se na dogovorenom mestu radi sastanka, što znači da u konkretnom slučaju se radi o složenom krivičnom delu, a prvostepeni sud nije odredio radnje za koje je vezao odredbu člana 185b stav 1. KZ. U izreci je navedeno da je okrivljeni imao nameru da izvrši nedozvoljenu polnu radnju nad maloletnikom. Dakle, iz izreke ožalbene presude proizlazi da se protivpravno postupanje okrivljenog sastoji u nameri vršenja nedozvoljene polne radnje nad maloletnikom, što bi upućivalo na odredbu člana 182. stav 1. KZ; međutim, tom odredbom propisano je da je izvršilac krivičnog dela onaj ko pod uslovima iz citiranih članova izvrši neku drugu polnu radnju, što dalje govori da je odredba upućuje na uslove, a to su: da je potrebno postojanje prinude, odnosno sile ili pretnje, ili da je oštećeni nemoćno lice, ili da je u odnosu podređenosti ili zavisnosti u odnosu na okrivljenog, pa kako iz činjeničnog opisa krivičnog dela za koje je okrivljeni oglašen krivim ne proizlazi postojanje sile ili pretnje, niti odnos podređenosti ili zavisnosti, to je izreka presude nerazumljiva i protivrečna sama sebi.

poslao joj je poruku u kojoj je naveo da ukoliko želi na lakši način da postane foto-model može da ode kod njegovog šefa, da mu „izdrka“ ili „popuši“, a ako to ne želi da uradi njemu, može imati seksualni ili oralni odnos sa njegovim sinom, nakon čega je tražio broj mobilnog telefona, pa pošto mu ga je ona poslala, oštećenoj je poslao poruku da će broj telefona proslediti šefovom sinu, koji će s njom komunicirati putem mobilnog telefona, potom je kontaktirao, dogovorio se da se sa njom sastane u restoranu, pojavio se na sastanku, rekao joj da ga sačeka da uđe u muški toalet, da će je pozvati odakle i da ga oralno zadovolji, da bi nakon ulaska u toalet pozvao telefonom oštećenu i rekao joj: „Ajde, gde si više, čekam te“. Prvostepenom presudom je oglašen krivim i osuđen na kaznu zatvora u trajanju od šest meseci i novčanu kaznu u iznosu od 50.000,00 dinara, oduzet mu je mobilni telefon i kućište za kompjuter i izrečena mera u smislu člana 89a KZ i primenjena odredba člana 7. stav 1. tačka 2. i 3. Zakona o posebnim merama za sprečavanje. Okrivljeni se u ovom postupku branio ćutanjem, nije priznao izvršenje krivičnog dela.

Navedena presuda je ukinuta, s obzirom da je sadržala bitne povrede odredbi krivičnog postupka jer je izreka presude nerazumljiva i protivrečna sama sebi, a razlozi nejasni i nerazumljivi. Ovo stoga što prvostepeni sud nije opredelio krivično delo za koje je vezao odredbu člana 185b KZ. Naime, odredbom člana 185. KZ propisano je da je izvršilac ovog krivičnog dela onaj ko u nameri izvršenja krivičnog dela silovanje iz stava 4. (dete), obljuba nad nemoćnim licem, obljuba sa detetom, obljuba zloupotrebom položaja, nedozvoljene polne radnje, podvođenje i omogućavanje vršenja polnog odnosa, posredovanje u vršenju prostitucije, iskorišćavanje maloletnog lica za proizvodnju, itd.,i navođenje maloletnog lica na prisustvo polnim radnjama, iskoristi računarsku mrežu ili komunikaciju drugim tehničkim sredstvima, dogovori sa maloletnikom sastanak i pojavi se na dogovorenom mestu radi sastanka, što znači da u konkretnom slučaju se radi o složenom krivičnom delu, a prvostepeni sud nije odredio radnje za koje je vezao odredbu člana 185b stav 1. KZ. U izreci je navedeno da je okrivljeni imao nameru da izvrši nedozvoljenu polnu radnju nad maloletnikom. Dakle, iz izreke ožalbene presude proizlazi da se protivpravno postupanje okrivljenog sastoji u nameri vršenja nedozvoljene polne radnje nad maloletnikom, što bi upućivalo na odredbu člana 182. stav 1. KZ; međutim, tom odredbom propisano je da je izvršilac krivičnog dela onaj ko pod uslovima iz citiranih članova izvrši neku drugu polnu radnju, što dalje govori da je odredba upućuje na uslove, a to su: da je potrebno postojanje prinude, odnosno sile ili pretnje, ili da je oštećeni nemoćno lice, ili da je u odnosu podređenosti ili zavisnosti u odnosu na okrivljenog, pa kako iz činjeničnog opisa krivičnog dela za koje je okrivljeni oglašen krivim ne proizlazi postojanje sile ili pretnje, niti odnos podređenosti ili zavisnosti, to je izreka presude nerazumljiva i protivrečna sama sebi.

Opšte mere zaštite i iskaz deteta u krivičnom postupku

1. Uvod

U poslednjih nekoliko decenija, naročita pažnja na međunarodnom planu posvećena je uspostavljanju delotvorne zaštite dece žrtva savremenih oblika kriminaliteta, posebno imajući u vidu neophodnost preduzimanja zakonodavnih i drugih mera za sprečavanje svih vidova seksualne eksploatacije i seksualnog zlostavljanja dece, kao i potrebu njihove zaštite, uvažavajući da najbolji interesi deteta i pravo deteta da se njegovo mišljenje čuje i uzme u razmatranje predstavljaju jedan od osnovnih principa u ostvarivanju, poštovanju i zaštiti njihovih prava. Države ugovornice, svesne obima i karaktera ovih pojava, posebno povećane međunarodne trgovine decom, iskorišćavanja dece u prostituciji i pornografiji, odnosno sve izražene zloupotrebe računarskih sistema i mreža u cilju regrutovanja dece u pomenute svrhe, pored ostalog, reagovale su i uspostavljanjem novih međunarodnih normi i standarda. U tom smislu, pored jasnog pojmovnog definisanja šta sve treba da sadrže zakonski opisi krivičnih dela na nivou materijalnog krivičnog prava, od izuzetne važnosti su i jasno definisane odredbe koje se odnose na specifičnosti procesnog položaja dece žrtava seksualne eksploatacije i seksualnog zlostavljanja.

Na nivou međunarodnih standarda, posebno se insistira na potrebi ustanovljavanja posebnih mera zaštite i pomoći deci, odnosno definisanju odredbi koje promovišu neophodnost uspostavljanja nacionalne i međunarodne saradnje u prevenciji i suzbijanju seksualne eksploatacije i seksualnog zlostavljanja dece(*). Važan korak predstavlja i uvođenje postavljenih standarda u normativni okvir Republike Srbije ratifikacijom Fakultativnog protokola uz Konvenciju o pravima deteta o prodaji dece, dečjoj prostituciji i dečjoj pornografiji (u daljem tekstu: Protokol(**)) i Konvencije Saveta Evrope o zaštiti dece od seksualne eksploatacije i seksualnog zlostavljanja(***), kao i izmene i dopune relevantnog krivičnoprocesnog okvira u skladu sa ratifikovanim konvencijama.

2. Opšte mere zaštite deteta oštećenog/svedoka u krivičnom postupku

Zakon o ratifikaciji Fakultativnog protokola uz Konvenciju o pravima deteta o prodaji dece, dečjoj prostituciji i dečjoj pornografiji, između ostalog, obavezuje države ugovornice da usvoje odgovarajuće mere za zaštitu prava deteta(****) u svim fazama krivičnog postupka (član 8. Protokola), a naročito:

* Škulić, M. (2002) «Krivičnoprocesne mogućnosti zaštite žrtava krivičnih dela povezanih sa trgovinom ljudskim bićima», Temida, br. 1, str. 14.

** Zakon o potvrđivanju Fakultativnog protokola uz Konvenciju o pravima deteta o prodaji dece, dečjoj prostituciji i dečjoj pornografiji, „Službeni list SRJ - Međunarodni ugovori", br. 02/22.

*** Zakon o potvrđivanju Konvencija Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja, „Službeni glasnik RS - Međunarodni ugovori", br. 2010/1.

**** Vučković-Šahović, N. (2006) Eksploatacija dece s posebnim osvrtom na Fakultativni Protokol uz Konvenciju o pravima deteta o prodaji dece, dečijoj prostituciji i dečijoj pornografiji, Beograd: Centar za prava deteta & Save the Children UK – kancelarija u Beogradu, str. 36.

• priznavanjem ugroženosti dece žrtava i prilagođavanjem postupaka da bi se uvažile njihove posebne potrebe, uključujući njihove posebne potrebe kao svedoka;
• obaveštavanjem dece žrtava o njihovim pravima, njihovoj ulozi i obimu, vremenskom rasporedu i napredovanju postupka i razmatranju njihovih slučajeva;
• dopuštanjem da se u postupku u kom su ugroženi njihovi lični interesi prezentiraju i razmotre gledišta, potrebe i preokupacije dece žrtava, na način koji je u skladu sa pravilima nacionalnog procesnog prava;
• obezbeđivanjem odgovarajućih službi podrške deci žrtvama tokom čitavog pravnog procesa;
• zaštitom, kada je to odgovarajuće, privatnosti i identiteta dece žrtava i preduzimanjem mera u skladu sa nacionalnim pravom kako bi se izbeglo nepodesno širenje informacija koje bi mogle dovesti do identifikovanja dece žrtava;
• obezbeđivanjem, u odgovarajućim slučajevima, bezbednosti dece žrtava, kao i bezbednosti njihovih porodica i svedoka koji svedoče u njihovo ime, od zastrašivanja i odmazde;
• izbegavanjem nepotrebnog odlaganja razmatranja slučajeva i izvršavanja naloga ili uredbi o davanju obeštećenja deci žrtvama.

Takođe, u smislu Protokola: "Države ugovornice će obezbediti da neizvesnost u pogledu stvarne starosne dobi žrtve ne spreči pokretanje krivičnog postupka, uključujući istražne radnje usmerene na utvrđivanje starosne dobi žrtve. Da u postupanju od strane sistema krivičnog pravosuđa, sa decom žrtvama nezakonitih radnji opisanih u ovom Protokolu, najbolji interes deteta bude prioritet". Države ugovornice preduzeće, takođe, mere kako bi obezbedile odgovarajuću obuku, posebno pravnu i psihološku, za lica koja rade sa žrtvama nezakonitih radnji zabranjenih prema ovom Protokolu i usvojiti mere kako bi zaštitile bezbednost i integritet lica i/ili organizacija uključenih u sprečavanje i/ili zaštitu i rehabilitaciju žrtava takvih nezakonitih radnji.

Zakon o potvrđivanju Konvencije Saveta Evrope o zaštiti dece od seksualne eksploatacije i seksualnog zlostavljanja izuzetno detaljno reguliše opšte mere zaštite deteta žrtve u krivičnom postupku, ali i sam način razgovora sa njim. U tom smislu, države ugovornice ove Konvencije se obavezuju na preduzimanje neophodnih zakonodavnih i drugih mera, za zaštitu prava žrtava, kao i njihovih posebnih potreba u ulozi svedoka, u svim fazama krivičnog postupka, a posebno:

a. upoznavajući ih, sem ako oni ne žele da prime takve informacije, sa službama koje im stoje na raspolaganju, njihovim pravima, njihovoj ulozi kao i praćenju i postupku nakon što podnesu tužbu, o opštem toku postupaka, optužbama kao i ishodu njihovog predmeta;

b. staranjem da, barem u slučajevima gde eventualno postoji opasnost za žrtvu ili njenu porodicu, oni mogu da budu obavešteni, ako je neophodno, kada je gonjeno ili osuđeno lice privremeno ili konačno pušteno na slobodu;

c. omogućavanjem da, na način koji je u skladu sa pravilima domaćih postupaka, budu saslušani, izvedu dokaze ili izaberu sredstva putem kojih će predstaviti i na razmatranje staviti svoje stavove, potrebe i interese, neposredno ili preko posrednika;

d. pružajući im odgovarajuće usluge podrške tako da njihova prava i interesi mogu blagovremeno da budu predočeni i uzeti u obzir;

e. zaštitom njihove privatnosti, identiteta i slike o njima i, u skladu sa domaćim propisima, sprečavanjem širenja u javnosti bilo kakvih informacija na osnovu kojih bi se mogao utvrditi njihov identitet;

f. staranjem za njihovu bezbednost, kao i njihove porodice i svedoka u njihovo ime, od zastrašivanja, osvete i obnove viktimizacije;

g. staranjem da se kontakt između žrtava i učinioca u sudu ili organu unutrašnjih poslova izbegne, sem ako nadležni organi ne odrede drugačije u najboljem interesu deteta ili kad je zbog istrage ili postupaka takav kontakt neophodan.

Organizacija postupka, okruženje po meri deteta i jezik prilagođen detetu
Metodi rada, koji su koncipirani tako da budu po meri deteta, treba da omoguće deci da se osećaju bezbedno. Ako decu prati lice u koje oni mogu da imaju poverenja, osećaju se bezbednije i lagodnije tokom postupka.
U zgradama u kojima se nalaze sudovi mogu, kad god je to moguće, biti određene posebne prostorije za razgovore s decom i saslušanje dece, tako što će se uvek voditi računa o najboljim interesima deteta.
Pravosuđe u krivičnom postupku primereno detetu podrazumeva i da deca zaista shvate prirodu i obim odluka koje se donose kao i posledice tih odluka.

Razgovor sa detetom

Zakon o potvrđivanju Konvencije Saveta Evrope o zaštiti dece od seksualne eksploatacije i seksualnog zlostavljanja posebno ustanovljava i obavezu da u situacijama kada se radi o detetu žrtvi seksualnog zlostavljanja, odnosno seksualne eksploatacije, države ugovornice preduzimaju neophodne zakonodavne i druge mere kojima se obezbeđuje:

- da se razgovori sa detetom održe bez neopravdanog odlaganja po prijavljivanju činjenica nadležnim organima;
- da se razgovori sa detetom obave, kada je neophodno, u prostorijama za to projektovanim ili adaptiranim;
- da razgovore sa detetom vodi stručnjak za to osposobljen i po mogućnosti ista osoba;
- da broj razgovora bude što manji i to samo onoliko koliko je preko potrebno za potrebe krivičnog postupka;
- odnosno, da dete prati njegov pravni predstavnik ili kada je odgovarajuće, odrasla osoba po njegovom izboru, sem ako sud ne donese obrazloženu odluku o suprotnom u pogledu te osobe (član 35).

Prilikom razgovora sa maloletnim licem (pogotovo mlađe starosne dobi) važno je.....

1. „spustiti se na nivo“ maloletnog lica (sesti pored njega, ali ne suviše blizu da ne ugrozite njegov prostor),
2. započeti razgovor tako da probudite interesovanje maloletnog lica (počnite razgovor jednostavnim pitanjima, obratite pažnju na neverbalnu komunikaciju – vodite računa i o svom neverbalnom izražavanju ...),
3. objasniti maloletnom licu zašto ste tu i šta nameravate da uradite:
    - Postaviću ti mnogo pitanja ...
    - Ja ću ponavljati ono što si mi rekao, ako pogrešim reci mi da sam pogrešno razumeo;
    - Ukoliko ti treba pauza, reci mi i prekinućemo razgovor na nekoliko minuta;
    - Kada završim sa pitanjima, ukoliko imaš neka pitanja za mene, pokušaću da odgovorim ...

Takođe, važno je imati na umu da deca predškolskog uzrasta imaju kapacitet pamćenja kao i odrasli, ali ne obraćaju uvek pažnju na detalje koje odrasli smatraju relevantnim - problemi vezani za sugestibilnost: maloletna lica (pogotovo mlađeg uzrasta) manje su sugestibilna u pogledu činjenica, nego u pogledu interpretacije tih činjenica;

Maloletna lica ne lažu više od odraslih (već sa pet godina deca razumeju potrebu da govore istinu, dok deca školskog uzrasta već razumeju samu potrebu utvrđivanja činjenica);

Deca već u uzrastu od dve do tri godine mogu jednostavnim jezikom da opišu opaženi događaj;
Sa pet godina, deca su u stanju da koriste složenije rečenice; Sa deset godina, deca su u stanju da opišu vreme, procene trajanje, odrede sukcesiju ili broj događaja; Mlađa deca bolje komuniciraju neverbalno;
Sa mlađom decom treba upotrebljavati jednostavan jezik i izbegavati upotrebu zamenica.

3. Poštovanje principa najboljeg interesa deteta i prava na participaciju u krivičnim postupcima

Najbolji interes deteta predstavlja jedan od osnovnih principa u ostvarivanju, poštovanju i zaštiti prava deteta. Obaveza države, svih relevantnih institucija, pa i suda jeste da u svim postupcima koji se tiču deteta vode računa o njegovim najboljim interesima. Ujedno, najbolji interes deteta predstavlja pravni standard koji se ceni prema okolnostima svakog pojedinačnog slučaja. To znači da se prilikom donošenja svake odluke moraju sagledati okolnosti svakog pojedinačnog slučaja i odluka doneti u najboljem interesu deteta o čijim se pravima odlučuje. Obaveza postupanja u skladu sa najboljim interesom deteta sadržana je u članu 3. stav 1. Konvencije o pravima deteta(*), u kom je propisana obaveza svih javnih ili privatnih institucija socijalnog staranja, sudova, administrativnih organa ili zakonodavnih tela da u svim aktivnostima koje se tiču deteta vode računa o njegovim najboljim interesima(**). U tačkama 8. i 9. Zakona o potvrđivanju Fakultativnog protokola uz Konvenciju o pravima deteta o prodaji dece, dečjoj prostituciji i dečjoj pornografiji se posebno ukazuje na to da je država dužna da obezbedi zaštitu najboljeg interesa deteta žrtve u svim fazama krivičnog postupka uz prevashodno priznavanje principa pravičnosti i nepristrasnosti.

Obaveza poštovanja principa najboljeg interesa deteta sadržana je i u drugim međunarodnim dokumentima, posebno Konvenciji Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja, koju je Srbija ratifikovala, i Smernicama Komiteta ministara Saveta Evrope o pravosuđu po meri deteta, a u kojima je jasno ukazano na obavezu postupanja u skladu sa najboljim interesom deteta u krivičnim postupcima, na obavezu zaštite maloletnog oštećenog (deteta-svedoka-žrtve) u krivičnom postupku, kao i uspostavljanja sistema pravosuđa po meri deteta.

Najvažniji aspekt utvrđivanja najboljeg interesa deteta jeste da se detetu omogući da utvrdi svoj najbolji interes. U tom smislu najbolji interes deteta je usko vezan sa pravom deteta na participaciju tj. s pravom deteta da izrazi mišljenje o pitanjima koja ga se tiču i da to mišljenje bude uzeto u obzir prilikom donošenja odluka.

Prilikom procene najboljih interesa dece koja su u uključena u krivični postupak kao žrtve ili svedoci, važno je uzeti u obzir:

a) njihove stavove i mišljenja;

b) sva druga prava deteta, kao što je pravo na dostojanstvo, slobodu i ravnopravno postupanje treba u svakom trenutku da budu poštovana;

* Konvencija o pravima deteta , "Službeni list SFRJ - Međunarodni ugovori", br. 90/15.

** Vučković Šahović, N., Doek, J., Zermatten, J. (2012) The Rights of the Child in International Law, Berne: Stampfli Publications Ltd., str. 309-303.

c) svi nadležni organi vlasti treba da usvoje sveobuhvatan pristup kako bi na odgovarajući način uzeli u obzir sve interese o kojima se tu radi, uključujući psihološko i fizičko blagostanje i pravne, socijalne i ekonomske interese deteta.

Pravo deteta na participaciju je jedan od osnovnih principa prava deteta. Član 12. Konvencije o pravima deteta sadrži obavezu države da obezbedi detetu koje je sposobno da formira mišljenje pravo na slobodu izražavanja mišljenja o svim pitanjima koja se tiču deteta i da posebno pruži mogućnost detetu da bude saslušano u svim sudskim i administrativnim postupcima koji ga se tiču, bilo neposredno ili preko zastupnika ili odgovarajućeg organa, na način koji je u skladu sa nacionalnim pravilima procesnog zakonodavstva. Participacija deteta je u skladu sa shvatanjem deteta kao subjekta prava koje aktivno participira u ostvarivanju svojih prava. Ovo pravo je usko vezano sa pravom deteta na informisanje i pravom deteta na slobodu izražavanja, a što podrazumeva obavezu postupajućih organa da, pre izražavanja mišljenja deteta, obezbede da dete bude informisano o svim činjenicama koje su od značaja za donošenje odluke, i to na jeziku koji je prilagođen detetu, kao i da mu omoguće da svoje mišljenje izrazi slobodno.

Pravo je svakog deteta da bude obavešteno o svojim pravima, da mu se ukaže na odgovarajuće puteve koji su mu obezbeđeni radi pristupa pravosuđu i da bude konsultovano i saslušano u postupcima u kojima učestvuje ili koji utiču na njega. Decu treba smatrati punim nosiocima prava i tako treba postupati prema njima.

3.1. Krivičnopravni sistem i uvažavanje principa najboljeg interesa deteta i prava na participaciju u krivičnim postupcima u Republici Srbiji

U sistemu sveobuhvatne društvene intervencije u cilju zaštite fizičkog, psihičkog i seksualnog integriteta maloletnih lica zaštitna funkcija krivičnog prava je njegova osnovna i najvažnija funkcija. U istorijskom pogledu, zaštita maloletnika od nasilja, zloupotreba i eksploatacije počinje od sporadičnih mera krivičnopravne represije, da bi se kroz razvoj sistema porodičnopravne zaštite došlo do složenih normativnih modela društvenog reagovanja. Danas, krivično pravo obezbeđuje osnovnu zaštitu maloletnih lica od ponašanja i postupaka koji predstavljaju napad na njihov život, zdravlje, seksualni integritet, ličnost i vaspitanje(*). Obim, domašaj i način delovanja krivičnopravne zaštite razlikuju se od nivoa i sadržaja te zaštite. Ključna uloga prava, naročito krivičnog prava u složenom sistemu društvenih intervencija, proističe iz toga što ono definiše oblike ponašanja koji narušavaju standarde odnosa prema maloletnom licu i izražava stepen „društvene (ne)tolerancije“ na pojedine

* Videti šire: Banić, M., Stevanović, I. (2015) Kako do pravosuđa po meri deteta: zaštita dece žrtava u krivičnim postupcima i stanje u praksi u Republici Srbiji, Beograd: Centar za prava deteta. str. 8-6.

oblike ponašanja. Posmatrano iz ugla krivičnog prava, krivični zakon određuje uslove ili situacije koji opravdavaju određeni tip krivičnopravne reakcije, odnosno ponašanje koje povlači određenu krivičnu sankciju(*).

Na početku dvadeset prvog veka, teško je uočiti krivičnopravne sisteme koji ne poklanjaju znatnu pažnju slučaju kada se kod određenih krivičnih dela maloletno lice javlja kao pasivan subjekt, a za najsavremenije krivičnoprocesne sisteme je karakteristično da posebnu pažnju posvećuju situacijama u kojima se maloletno lice pojavljuje u ulozi oštećenog, odnosno svedoka u krivičnom postupku. U velikoj meri, evropsko kontinentalno pravo sledilo je, u pogledu krivičnopravnog položaja maloletnih lica i njihove zaštite, opšti progres koji je, pre svega, bio uslovljen razvojem krivičnog međunarodnog prava. Drugim rečima, krivično pravo sledilo je u velikoj meri, i samo kao određeni faktor promena, potrebe društva.

Na ovaj način, posmatrano iz ugla krivičnopravnog položaja maloletnog lica u sistemu krivičnopravne zaštite, od pasivnog subjekta kao lica na kome je preduzeta radnja izvršenja, pomera se ka licu čije je dobro povređeno ili ugroženo i gde se država i njeni organi postavljaju kao garanti tih prava i preuzimaju funkciju njihovog zastupanja u situacijama kada su ona ugrožena, odnosno povređena postupcima roditelja ili drugih osoba kojima je povereno staranje o maloletnom licu(**). U Republici Srbiji, krivičnopravni sistem obezbeđuje osnovnu zaštitu maloletnih lica od ponašanja i postupaka koji ugrožavaju njihov život, zdravlje, seksualni integritet, ličnost i vaspitanje. Naravno, krivičnopravni sistem deluje u sadejstvu s ostalim delovima pravnog sistema, odnosno povezano sa drugim institucionalnim sistemima kao što su: sistem socijalne zaštite, zdravstvo, obrazovanje. Ukoliko krivičnopravnu zaštitu maloletnih lica odredimo kao skup pravnih normi kojima se zakonski daje opis krivičnih dela kojima se ugrožava i/ili povređuju život i telesni integritet, zdravlje, emocionalni i seksualni integritet i vaspitanje, možemo konstatovati da Krivični zakonik(***) sve više proširuje zonu inkriminacije, povećavajući i diferencirajući sistem „krivičnih dela na štetu maloletnih lica."
Sa druge strane, Zakon o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica (u daljem tekstu: Zakon o maloletnicima(****)) , kao i Zakonik o krivičnom postupku(*****) sadrže niz odredbi čiji je cilj zaštita prava i interesa maloletnih oštećenih lica u postupku.

Hitnost u postupanju - izbegavanje nepotrebnog odlaganja

Krivični predmeti u kojima se pojavljuju maloletna lica kao oštećena ili svedoci treba da budu rešavani ekspeditivno,

* Stevanović, I.(b) (2014) Moje pravo da budem zaštićen, Beograd: Institut za kriminološka i sociološka istraživanja, str. 36.37.

** Stevanović, I.(a) (2014) „Krivičnopravni sistem i zaštita maloletnih lica (nacionalni normativni aspekt)", u: Vučković Šahović, N. i dr. Zaštita dece žrtava i svedoka krivičnih dela, Beograd: International Management Group, str. 33-32 i Stevanović, I.(b) (2014) op. cit. str. 39.

*** Krivični zakonik, „Službeni glasnik RS" br. 05/88 ,05/85 - ispr., 05/107 - ispr., 09/111 ;09/72 i 13/104 i Zakon o izmenama i dopunama Krivičnog zakonika, «Službeni glasnik RS», br. 2016/94 od 24. novembra 2016

**** Zakon o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica, „Službeni glasnik RS" br. 05/85

***** Zakonik o krivičnom postupku, „Službeni glasnik Republike Srbije", br. 2012/121 ,2011/101 ,2011/72,i 2013/45 i 2014/55.

i može se razmotriti sistem utvrđivanja redosleda po kojima se predmeti uzimaju u ispitivanje prema prioritetu. Treba imati na umu da deca imaju drugačiji doživljaj vremena u odnosu na onaj koji imaju odrasli, kao i da je element vremena njima veoma važan. Sudovi bi trebalo da postupaju po pravilima koja će omogućiti da se uspostavi sistem prvenstva kada je reč o posebno teškim ili hitnim slučajevima, ili onda kada bi, u slučaju da se bez oklevanja ne preduzme neki korak, mogle biti nanete nepopravljive posledice.
Zakon o maloletnicima sadrži posebne odredbe o zaštiti maloletnih lica kao oštećenih u postupku koje propisuju obaveznu specijalizaciju svih postupajućih aktera u ovim postupcima, zaštitu od sekundarne viktimizacije, zabranu suočavanja okrivljenog i oštećenog, načelo hitnosti postupka, obavezno pravno zastupanje.
Tako je članom 150. i 151. Zakona propisana obavezna specijalizacija iz oblasti prava deteta i krivičnopravne zaštite maloletnih lica svih postupajućih organa posebno sudija, javnih tužilaca, advokata, policije.

Član 152. Zakona, radi sprečavanja sekundarne viktimizacije i traumatizacije maloletnog oštećenog u postupku, propisuje da se kao dokaz koriste video i audio-trake kojima se registruje iskaz, pruža mogućnost da se jednom data izjava maloletnika koristi i u kasnijim fazama postupka, da se saslušanje obavi uz pomoć psihologa, pedagoga ili drugog stručnog lica, kao i da se saslušanje obavi u prostorijama van suda, i to u stanu maloletnog oštećenog ili drugoj prostoriji, odnosno ovlašćenoj ustanovi - organizaciji stručno osposobljenoj za ispitivanje maloletnih lica. Javni tužilac, istražni sudija i sudije u veću dužni su da se odnose prema oštećenom vodeći računa o njegovom uzrastu, svojstvima ličnosti, obrazovanju i prilikama u kojima živi, posebno nastojeći da se izbegnu moguće štetne posledice postupka po njegovu ličnost i razvoj.

Članom 153. propisana je i zabrana suočavanja maloletnog lica koje se saslušava kao svedok i okrivljenog, ako je maloletno lice usled prirode krivičnog dela, posledica ili drugih okolnosti, posebno osetljivo, odnosno ako se nalazi u posebno teškom duševnom stanju. Članom 157. Zakona propisana je hitnost postupka, pa su svi organi koji učestvuju u postupku dužni da postupaju najhitnije moguće kako bi se postupak što pre završio.

Zakonik o krivičnom postupku takođe sadrži niz odredbi čiji je cilj zaštita prava i interesa maloletnih lica u postupku, kao što su mogućnost izricanja mera bezbednosti i to mere zabrane prilaženja, sastajanja ili komuniciranja sa određenim licem kojom se učiniocu krivičnog dela može zabraniti približavanje oštećenom na određenu udaljenost zabraniti pristup oko mesta stanovanja ili mesta rada oštećenog i zabraniti dalje uznemiravanje oštećenog ako se opravdano može smatrati da bi dalje vršenje takvih radnji od strane učinioca krivičnog dela bilo opasno po oštećenog (član 197 ,18. i 198).

Posebna pravila postupka o zaštiti maloletnih lica oštećenih u krivičnom postupku

- pravilo obavezne specijalizacije (policijskog službenika, javnog tužioca, predsednika veća koji sudi punoletnim okrivljenim u ovakvim situacijama, punomoćnika oštećenog);
- minimiziranje sekundarne viktimizacije;
- primena posebnih pravila saslušanja maloletnih oštećenih (obavezna stručna asistencija, načelno ograničavanja broja saslušanja u istom krivičnom postupku, omogućavanje saslušanja putem audio-video-linka, procesna mogućnost za saslušanje van sudnice);
- zabrana suočavanja u cilju sprečavanja sekundarne viktimizacije;
- obavezno pravno zastupanje maloletnog oštećenog;
- posebna pravila prepoznavanja;
- načelo hitnosti takvog krivičnog postupka.

Takođe, Zakonik o krivičnom postupku sadrži i pravila za saslušanje posebno osetljivih svedoka, kao i mere posebne zaštite zaštićenog svedoka. Status posebno osetljivog svedoka može se odrediti svedoku koji je s obzirom na uzrast, životno iskustvo, način života, pol, zdravstveno stanje, prirodu, način ili posledice izvršenog krivičnog dela, odnosno druge okolnosti slučaja posebno osetljiv, i u tom smislu ovim Zakonom je predviđena mogućnost određivanja statusa posebno osetljivog svedoka maloletnom oštećenom licu. Rešenje o određivanju statusa posebno osetljivog svedoka donosi javni tužilac, predsednik veća ili sudija pojedinac. Posebno osetljivom svedoku pitanja se mogu postavljati samo preko organa postupka, koji je dužan da se prema njemu odnosi sa posebnom pažnjom, nastojeći da se izbegnu moguće štetne posledice krivičnog postupka po ličnost, telesno i duševno stanje svedoka. Ispitivanje se može obaviti uz pomoć psihologa, socijalnog radnika ili drugog stručnog lica, upotrebom tehničkih sredstava za prenos slike i zvuka, bez prisustva stranaka i drugih učesnika u postupku u prostoriji u kojoj se svedok nalazi. Posebno osetljivi svedok može se ispitati i u svom stanu ili drugoj prostoriji, odnosno u ovlašćenoj instituciji koja je stručno osposobljena za ispitivanje posebno osetljivih lica. Zakonik propisuje i zabranu suočenja posebno osetljivog svedoka sa okrivljenim, osim ako to sam okrivljeni zahteva, a organ postupka to dozvoli vodeći računa o stepenu osetljivosti svedoka i o pravima odbrane (član 103. i 104.)

Status posebno osetljivog svedoka organ postupka može po službenoj dužnosti, ili na zahtev stranke, odnosno samog svedoka, odrediti svedoku koji je posebno osetljiv s obzirom na: uzrast, životno iskustvo, način života, pol, zdravstveno stanje prirodu, način i posledice izvršenog krivičnog dela, odnosno druge okolnosti slučaja.

Posebno osetljivom svedoku pitanja se mogu postavljati samo preko organa postupka.

Posebno osetljiv svedok ne može biti suočen sa okrivljenim, osim ukoliko nisu kumulativno ispunjena dva uslova: 1) potrebno je da sam okrivljeni zahteva suočenje; 2) neophodno je da organ postupka dozvoli suočenje vodeći računa o stepenu osetljivosti svedoka i pravima odbrane.

Zakonik o krivičnom postupku sadrži i posebne odredbe o merama posebne zaštite zaštićenog svedoka koje obuhvataju ispitivanje zaštićenog svedoka pod uslovima i na način koji obezbeđuju da se njegova istovetnost ne otkrije javnosti, a izuzetno ni okrivljenom i njegovom braniocu. Status zaštićenog svedoka sud može odrediti ako postoje okolnosti koje ukazuju da bi svedok davanjem iskaza ili odgovorom na pojedina pitanja sebe ili sebi bliska lica izložio opasnosti po život, zdravlje, slobodu ili imovinu većeg obima (član 106).

Međutim, i pored navedenih odredbi, čiji je cilj da se spreči sekundarna viktimizacija i traumatizacija u postupku posebno osetljivih svedoka, veliki problem predstavlja činjenica da Zakonik o krivičnom postupku ne isključuje mogućnost unakrsnog saslušanja posebno osetljivih svedoka. Naime, članom 98. stav 3. Zakona propisano je da kad svedok završi svoj iskaz, a potrebno je da se njegov iskaz proveri, dopuni ili razjasni, postaviće mu se pitanja koja moraju biti jasna, određena i razumljiva, ne smeju sadržati obmanu, niti se zasnivati na pretpostavci da je izjavio nešto što nije izjavio, i ne smeju predstavljati navođenje na odgovor osim ako se radi o unakrsnom ispitivanju na glavnom pretresu.

Tumačenjem ove odredbe može se zaključiti da je unakrsno ispitivanje posebno osetljivog svedoka moguće na glavnom pretresu. Imajući u vidu da posebno osetljivog svedoka, a naročito oštećenog kome je dodeljen, ovaj status u najvećem broju slučajeva za svedočenje predlaže javni tužilac, to bi značilo da na glavnom pretresu odbrana ima mogućnost da unakrsno ispituje ovog svedoka i da mu postavlja sugestivna, obmanjujuća, neodređena i nerazumljiva pitanja. Ispitivanje maloletnog oštećenog na ovaj način lako može dovesti do sekundarne viktimizacije i traumatizacije, te je potrebno hitno izmeniti i precizirati ovo zakonsko rešenje i jasno isključiti mogućnost unakrsnog ispitivanja lica kojima je dodeljen status posebno osetljivog svedoka, posebno maloletnih lica(*).

* Škulić, M. (2014) «Zaštita dece/maloletnih lica kao oštećenih i svedoka u krivičnom postupku», u: Vučković, Šahović, N. i dr., Zaštita dece žrtava i svedoka krivičnih dela, Beograd: International Management Group - IMG, str. 59-53; Škulić, M. (2016) «Položaj žrtve/oštećenog u krivičnopravnom sistemu Srbije uopšte i u odnosu na Direktivu EU 29-2012», Kaznena reakcija u Srbiji VI deo, (ur. Đ. Ignjatović), edicija Crimen, Beograd: Pravni fakultet Univerziteta u Beogradu, str. 78-77.

Iskazi dece u krivičnom postupku

U predmetu W. S. protiv Poljske, Evropski sud za ljudska prava u Strazburu je sugerisao moguće načine testiranja pouzdanosti iskaza malog deteta koje je žrtva i ukazao je na to da se sve to može postići na način koji je u manjoj meri invazivan od neposrednog ispitivanja. Mogućno je primeniti nekoliko sofisticiranih metoda: saslušanje deteta u prisustvu psihologa, i to tako da se pitanja istovremeno u pismenoj formi daju odbrani, ili tako što će se razgovor voditi u prostoriji koja bi podnosiocu predstavke ili njegovom advokatu omogućio da budu prisutni preko video-linka ili posebno instaliranih jednostranih ogledala.

Uvek treba imati na umu da će, u cilju posebne zaštite ličnosti maloletnog lica oštećenog, predstavnici pravosudnih organa (javni tužioci i sudije) prilikom preduzimanja, zakonom propisanih ovlašćenja (Posebni protokol o postupanju pravosudnih organa u zaštiti maloletnih lica od zlostavljanja i zanemarivanja, 2009):

- postupati sa naročitom hitnošću, obazrivo, vodeći računa o zrelosti, drugim ličnim svojstvima i zaštiti privatnosti maloletnoglica;
- predstaviti se maloletnom licu i na način na koji ono može da shvati, objasniti šta će se događati, šta se od njega očekuje i obavezno proveriti da li je ono to razumelo;
- informisati maloletno lice i njegovog roditelja, usvojioca ili staraoca o njihovim pravima i službama koje im stoje na raspolaganju radi pružanja pomoći i/ili podrške. Obezbediti da se maloletnom licu daju informacije na način koji je prilagođen njegovom uzrastu i zrelosti i na jeziku koji može da razume;
- uvek kada je to moguće, uzeti iskaz od maloletnog lica, posebno maloletnog lica ispod navršenih četrnaest godina života, van prostorija pravosudnih organa, u za njega prirodnom ambijentu;
- uvek kada je to moguće, koristiti posebne tehnike za uzimanje iskaza (združeni intervju), odnosno uzimati iskaz putem audio i video linka;
- onemogućiti (u prostorijama pravosudnih organa) kontakt maloletnog lica žrtve zlostavljanja i zanemarivanja kao davaoca iskaza i okrivljenog;
- ukoliko se iskaz maloletnog lica oštećenog - žrtve zlostavljanja i zanemarivanja uzima u prostorijama pravosudnih organa, osloboditi maloletno lice nelagodnosti/straha, tako što će ga tužilac, sudija ili stručno lice upoznati sa prostorom i pokazati mu zgradu (obavezno proveriti da li se maloletno lice oseća bezbednim);

- iskaz od maloletnog lica uzeti samo za to obučeni tužioci i sudije (koji su stekli posebna znanja iz oblasti prava deteta i krivičnopravne zaštite maloletnih lica);
- uzimanje iskaza od maloletnog lica (pogotovo mlađeg uzrasta - ispod 14 godina života) prilagoditi njegovom uzrastu i ličnim svojstvima - rečnik i intonaciju glasa takođe prilagoditi datim okolnostima;
- obratiti pažnju na ponašanje maloletnog lica (izraz lica, pokrete tela, uznemirenost, da li pokazuje strah) i da tok uzimanja iskaza prilagode sagledanim reakcijama;
- ne insistirati na određenim pitanjima na koja je očigledno da maloletno lice ne želi da da odgovor. Imati u vidu da je maloletno lice (pogotovo mlađeg uzrasta – ispod 14 godina života), uplašeno i da mu je neprijatno da priča o određenim događajima;
- objasniti maloletnom licu da nije krivo za ono što se dogodilo;
- uzimanje obaveštenja od maloletnog lica započeti sa opštim pitanjima, uz obavezno pitanje da li je razumelo postavljeno pitanje, a zatim nastaviti sa pitanja u vezi sa konkretnim činjenicama;
- po završetku uzimanja iskaza, pitati maloletno lice i njegove roditelje, usvojioca ili staraoca, odnosno drugo lice koje je prisustvovalo uzimanju iskaza da li žele da se nešto dopuni, odnosno imaju li eventualne primedbe, što će se uneti u zapisnik i ukoliko to navedena lica zahtevaju izdati im kopiju zapisnika;
- zaštititi maloletno lice i njegovu porodicu od eventualnih medijskih zloupotreba. Prilikom davanja saopštenja ne smeju se navoditi ime, kao ni drugi podaci na osnovu kojih bi se moglo zaključiti o kom licu je reč. Saopštenje može sadržati kratak opis događaja (datum, vreme i šire mesto događaja, kao i podatke o uzrastu i polu maloletnog lica).

3.2. Jedinice za podršku deci žrtvama i svedocima u krivičnom postupku

U okviru projekta „Unapređenje prava deteta kroz jačanje sistema pravosuđa i socijalne zaštite u Srbiji“, Pravosudna akademija i Centar za prava deteta održali su, u periodu od 29. maja do 6. novembra 2016. godine, u 89 osnovnih sudova, informativne sesije na temu: Zaštita maloletnog lica kao oštećenog i svedoka u krivičnom postupku. Ove informativne sesije su organizovane intersektorski, za predstavnike pravosuđa, socijalne zaštite i predstavnike policije. Predavači su bili psiholozi, pedagozi, dečiji psihijatri i drugi iskusni stručnjaci u radu sa decom koji su za to prošli posebnu pripremu, a u okviru pomenutog IPA 2013 projekta.

Na informativnim sesijama prisustvovalo je 1015 učesnika: 393 predstavnika suda, 180 predstavnika tužilaštva, 247 predstavnika centara za socijalni rad, 166 predstavnika policije i 29 predstavnika drugih institucija. Osnovni cilj bio je da se stručnim licima, prevashodno nosiocima pravosudnih funkcija, ali i svima onima koji rade sa decom žrtvama, ukaže na značaj umanjenja posledica sekundarne viktimizacije po dete žrtvu ili svedoka u krivičnom postupku, kako se to čini, da se ukaže na aktivnu ulogu stručnjaka u pripremi maloletnog lica za sam postupak, odnosno o tome šta će se dešavati i koje su uloge stručnih lica koji će sa njim neposredno razgovarati, odnosno ukaže na značaj forenzičkog intervjua s ciljem što efikasnijeg postupanja, a vođenog u skladu sa najboljim interesom deteta.

Veliki značaj održanih sesija ogledao se i u mogućnosti da učesnicima budu predstavljene novoosnovane Jedinice za podršku deci žrtvama/svedocima u krivičnim postupcima s ciljem pružanja podrške posebno ranjivim grupama dece i njihovim porodicama.

Ceo proces bio je praćen definisanjem, publikovanjem i distribucijom Smernice za zaštitu dece u krivičnim postupcima. Jedinice za podršku deci žrtvama i svedocima u krivičnom postupku formirane su u četiri grada: Beogradu, Nišu, Novom Sadu i Kragujevcu, i funkcionišu na regionalnom nivou. Za realizovanje podrške porodici i deci žrtvama i svedocima u krivičnom postupku, formirani su timovi stručnjaka koji su edukovani za pomoć sudiji i tužiocu pri uzimanju iskaza, za pristup detetu u skladu sa uzrastom i vrstom traume, specifičnim načinima razgovora sa malim detetom i adolescentom, pripremu deteta za sud i pružanju podrške nakon sudskog postupka(*).

Timovi su mobilni, realizuju terenski rad na nivou četiri apelaciona suda, poseduju mobilnu opremu za uzimanje iskaza, a usluga je trenutno besplatna. Usluga Jedinice treba da obezbedi;

* Videti šire: Milosavljević-Đukić, I., Tankosić, B., Petković, J., Marković, M. (2017) „ Jedinice za podršku deci žrtvama i svedocima u krivičnom postupku - Domaće pravo i praksa“, Temida, br. 1, str. 59-53.

poštovanje načela hitnosti postupka, saslušanje deteta u prisustvu pedagoga, psihologa ili drugog stručnog lica, mogućnost saslušanja deteta van sudnice, bez prisustva okrivljenog i korišćenjem mobilne opreme, a sve u cilju da se izbegne višestruko saslušanje deteta, suočavanje sa okrivljenim i da se uskladi praksa na celoj teritoriji Republike Srbije.

Podrška Jedinice deci u krivičnom postupku podrazumeva:

1) umanjenje posledica sekundarne viktimizacije u odnosu na maloletna lica žrtve tokom krivičnog postupka i po njegovom okončanju;
2) upoznavanje maloletnog lica sa krivičnim postupkom, odnosno razjašnjavanje uloge svih učesnika na jeziku i način koji je najprilagođeniji uzrastu i zrelosti deteta,
3) povećanje sposobnosti maloletnog lica da spremnije i kvalitetnije da iskaz;
4) povećanje poverenja maloletnog lica i njegove porodice u krivični postupak.
Jedinica ima ulogu da informiše i pripremi maloletno lice i porodicu za sud, da bude podrška tužiocima i sudu prilikom uzimanja iskaza od maloletnog lica, da sprovede forenzički intervju sa maloletnim licem i pruži savetodavnu i terapijsku podršku.

Važno je imati na umu:

Jedinica za podršku deci žrtvama i svedocima u krivičnom postupku je služba koja omogućava sveobuhvatnu podršku svakom detetu, žrtvi ili svedoku, pre, u toku i nakon krivičnog postupka. Korišćenjem usluga Jedinice ,svedočenje za dete postaje manje stresno i neprijatno, odnos poverenja koji se uspostavi sa detetom u toku pripreme omogućava da se dete u prisustvu osobe iz Jedinice oseća opuštenije, iznosi više detalja o događaju, a osigurava se i potpuno razumevanje svih pitanja, kao i poštovanje svih prava deteta, a sa kojima je upoznato u toku pripreme. Ova podrška nije namenjena samo detetu, već i njegovim bližnjim, čija uloga je najznačajnija za emocionalno stanje deteta tokom stresnih događaja.

Preporučena literatura

1. Banić, M., Stevanović, I. (2015) Kako do pravosuđa po meri deteta: zaštita dece žrtava u krivičnim postupcima i stanje u praksi u Republici Srbiji, Beograd: Centar za prava deteta.
2. Milosavljević-Đukić, I., Tankosić, B., Petković, J., Marković, M. (2017) „Jedinice za podršku deci žrtvama i svedocima u krivičnom postupku - domaće pravo i praksa“, Temida, br. 1, str . 64-45.
3. Posebni protokol o postupanju pravosudnih organa u zaštiti maloletnih lica od zlostavljanja i zanemarivanja, 2009, Beograd: Ministarstvo pravde Republike Srbije.
4. Posebnim protokolom o postupanju policijskih službenika u zaštiti maloletnih lica od zlostavljanja i zanemarivanja, 2012, Beograd: Ministarstvo unutrašnjih poslova Republike Srbije, dostupno na sajtu: www.mup.gov.rs
5. Stevanović, I.(a) (2014) „Krivičnopravni sistem i zaštita maloletnih lica (nacionalni normativni aspekt)“, u: Vučković Šahović, N. i dr. Zaštita dece žrtava i svedoka krivičnih dela, Beograd: International Management Group, str. 42-30.
6. Stevanović, I.(b) (2014) Moje pravo da budem zaštićen, Beograd: Institut za kriminološka i sociološka istraživanja.
7. Vučković-Šahović, N. (2006) Eksploatacija dece s posebnim osvrtom na Fakultativni Protokol uz Konvenciju o pravima deteta o prodaji dece, dečijoj prostituciji i dečijoj pornografiji, Beograd: Centar za prava deteta & Save the Children UK – kancelarija u Beogradu.
8. Vučković Šahović, N., Doek, J., Zermatten, J. (2012) “The CRC Committee’s General Comment No. 10”, in: The Rights of the Child in International Law, Berne: Stampfli Publications Ltd.
9. Škulić, M. (2002) „Krivičnoprocesne mogućnosti zaštite žrtava krivičnih dela povezanih sa trgovinom ljudskim bićima“, Temida, br. 1.
10. Škulić, M. (2014) „Zaštita dece/maloletnih lica kao oštećenih i svedoka u krivičnom postupku“, u: Vučković, Šahović, N. i dr. Zaštita dece žrtava i svedoka krivičnih dela, Beograd: International Management Group - IMG, str. 70-43.
11. Škulić, M. (2016) „Položaj žrtve/oštećenog u krivičnopravnom sistemu Srbije uopšte i u odnosu na Direktivu EU 29-2012“, Kaznena reakcija u Srbiji VI deo, (ur. Đ. Ignjatović), edicija Crimen, Beograd: Pravni fakultet

Korisni kontakti

MUP Republike Srbije
Direkcija policije
Uprava kriminalističke policije
Služba za borbu protiv organizovanog kriminala
Odeljenje za borbu protiv visokotehnološkog kriminala
Ul. Bulevar Mihajla Pupina 11070 ,2 Beograd

Odsek za suzbijanje elektronskog kriminala
Kontakt: dr Vladimir Urošević
E-mail: vladimir.urosevic@mup.gov.rs; telefon: 201 20 89 064
Odsek za suzbijanje kriminaliteta u oblasti intelektualne svojine
Kontakt: mr Mikailo Tijanić
E-mail: mikailo.tijanic@mup.gov.rs; telefon: 302 22 89 064

Preporučeni internet resursi

www.osintframework.com
OSINT okvir je fokusiran na onlajn prikupljanje informacija od besplatnih alata i resursa na internet-mreži. Namera je da se istražiteljima pomogne da pronađu besplatne OSINT resurse radi identifikovanja izvršilaca i žrtvi visokotehnološkog kriminala. Neki od sajtova mogu zahtevati registraciju ili nude više podataka za novčanu naknadu, ali je većina alata za onlajn istrage u sajber-prostoru besplatna.

http://pametnoibezbedno.gov.rs/pametno/category/bezbednost_dece_na_internetu/?lng=lat

Strategija informacione bezbednost za dalje jačanje digitalne zaštite
http://www.netpatrola.rs/sr/naslovna.1.1.html

Net-patrola je onlajn mehanizam za podnošenje prijava Centru za bezbedni internet, koji je osnovan u svrhu prijema i obrade prijava o nelegalnim ili štetnim sadržajima na internetu.
www.GetSafeOnline.org
- Internet Safety Advice
- Crime Prevention Advice

www.ThinkUKnow.co.uk
- Child Protection Online Advice
- Public Portal to report suspected child abuse online
- Crime Prevention Advice (Children & Parents)

www.InternetWatchFoundation.org.uk
- Public Hotline for reporting child abuse images, videos or text observed online (for anywhere in the world).

www.ActionFraud.org.uk
- Public Hotline for reporting fraud
- Support and advice about fraud
- Crime Prevention Advice

www.APWG.org
- Anti-Phishing Working Group
- Public Hotline for reporting phishing emails and websites
- Crime Prevention Advice

www.ic3.gov
IC3 je sajt za onlajn prijave internet-kriminala koji za posledicu prevare ima materijalnu štetu. U prijavi je potrebno navesti sledeće informacije: ime oštećenog, adresa, telefon i E-mail, informacije o finansijskim transakcijama (npr. informacije o nalogu, datum transakcije i iznos, i dr.), ime subjekta kojem je novac doznačen, adresa, telefon, E-mail, veb i IP adresa, detalji o tome kako ste bili žrtva prevare i sve druge relevantne informacije koje smatrate da su bitne.

Kontakti:
Save the Children
Francuska 27, 11000 Belgrade, Serbia
info.nwbalkans@savethechildren.org
https://nwb.savethechildren.net