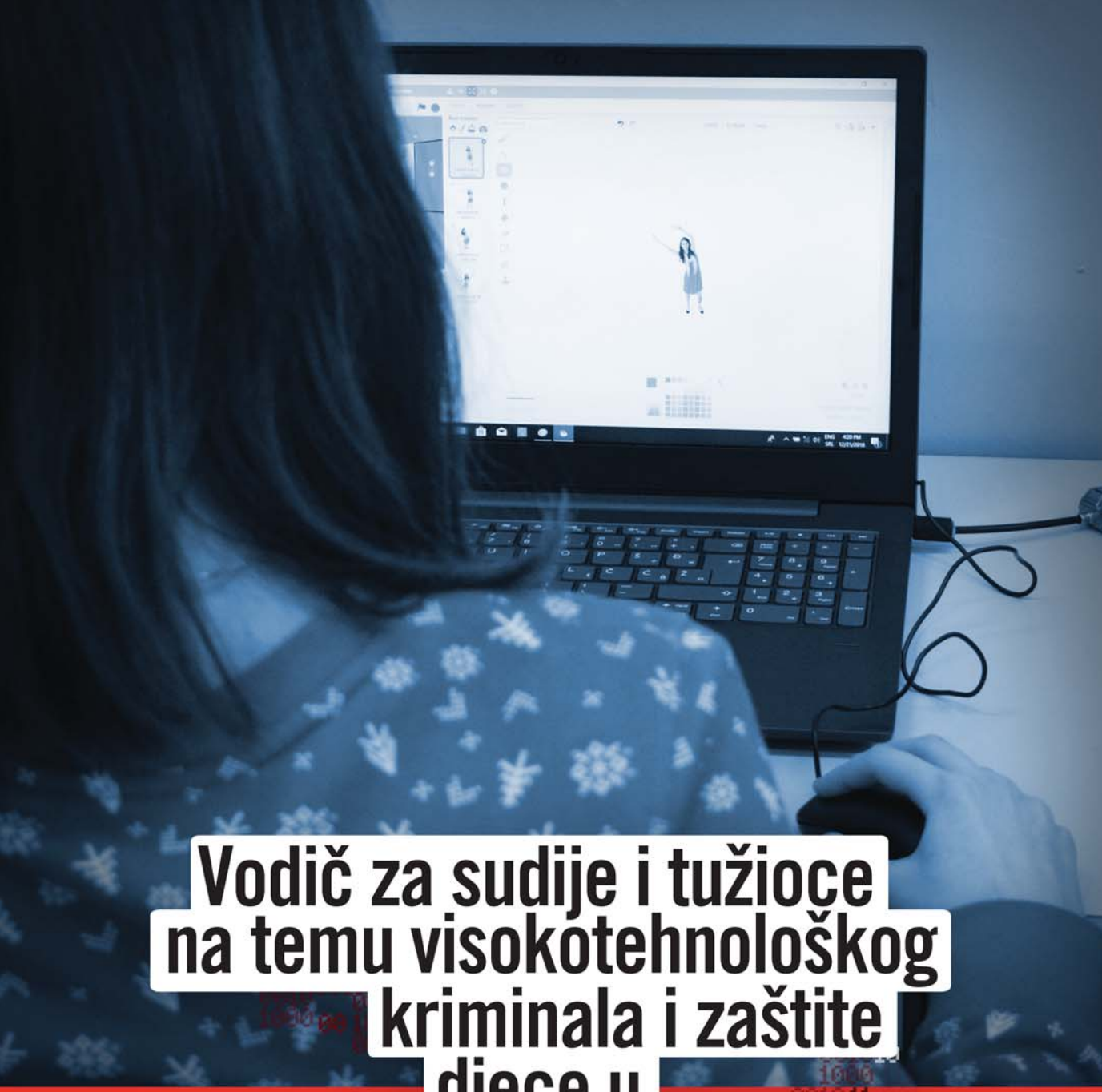

Vodič za sudije i tužioce na temu visokotehnološkog kriminala i zaštite djece u Bosni i Hercegovini

Save the Children
100 YEARS

MEĐUNARODNI FORUM SOLIDARNOSTI - EMMAUS
BOSNA I HERCEGOVINA

unicef
za svako dijete

BOSNA I HERCEGOVINA – БОСНА И ХЕРЦЕГОВИНА – BOSNIA AND HERZEGOVINA
REPUBLIKA SRPSKA – РЕПУБЛИКА СРПСКА
FEDERACIJA BOSNE I HERCEGOVINE – ФЕДЕРАЦИЈА БОСНЕ И ХЕРЦЕГОВИНЕ

ЈАВНА УСТАНОВА ЦЕНТАР ЗА ЕДУКАЦИЈУ СУДИЈА И ЈАВНИХ ТУЖИЛАЦА У РС
JAVNA USTANOVA CENTAR ZA EDUKACIJU SUDIJA I TUŽILACA U FBiH
JAVNA USTANOVA CENTAR ZA EDUKACIJU SUDACA I TUŽITELJA U FBiH
PUBLIC INSTITUTIONS CENTRES FOR JUDICIAL AND PROSECUTORIAL TRAINING
OF THE RS AND THE FBiH

Vodič za sudije i tužioce na temu visokotehnološkog kriminala i zaštite djece u Bosni i Hercegovini

Autori:

Branko Stamenković
Saša Živanović
Bojana Paunović
Ivana Stevanović

Sarajevo, 2021. godine

IMPRESUM

Save the Children vjeruje da svako dijete zaslužuje budućnost. U zemljama sjeverozapadnog Balkana radimo svaki dan kako bismo za djecu osigurali zdrav početak života, priliku za učenje i zaštitu od nasilja. Dajemo sve od sebe za djecu – svaki dan i u vrijeme kriza – mijenjajući njihove živote i budućnost koja je pred nama.

Izdavač: Save the Children

Autori: Branko Stamenković, Saša Živanović, Bojana Paunović, Ivana Stevanović

Tekst prilagodili kontekstu BiH: prof. dr. Elmedin Muratbegović i prof. dr. Haris Halilović

Tekst odobrili: Centar za edukaciju sudija i tužilaca Federacije BiH i
Centar za edukacija sudija i javnih tužilaca Republike Srpske

Grafički dizajn: KOMITET Sarajevo

Štampa: Grafika Šaran, Sarajevo

Tiraž: 150

Ova publikacija izrađena je u okviru projekta „Zaustaviti nasilje nad djecom: Prevencija i rad na sprečavanju seksualnog iskorištavanja i zlostavljanja djece u digitalnom okruženju u Bosni i Hercegovini“, čiju su realizaciju podržali Global Fund to End Violence Against Children i UNICEF.

Stavovi i mišljenja su odgovornost autora i ne odražavaju zvanične stavove ili mišljenja UNICEF-a.

CIP - Katalogizacija u publikaciji
Nacionalna i univerzitetska biblioteka Bosne i Hercegovine, Sarajevo

343.62-053.2:004.738.5(036)

VODIČ za sudije i tužioce na temu visokotehnološkog kriminala i zaštite djece u Bosni i Hercegovini / Branko Stamenković ... [et al.]. - Sarajevo : Save the Children, 2021. - 90 str.

Bibliografija: str. 87-90 ; bibliografske i druge bilješke uz tekst.

ISBN 978-9926-462-28-4

1. Stamenković, Branko

COBISS.BH-ID 42626310

SADRŽAJ

Predgovor

Poštovani čitaoci,

pred vama se nalazi dokument pod nazivom *Vodič za sudije i tužioce na temu visokotehnološkog kriminala i zaštite djece u Bosni i Hercegovini*, koji je prvenstveno namijenjen za podršku u realizaciji osnovnih obuka za sudije i tužioce koji rade ili se žele edukovati za rad na predmetima visokotehnološkog kriminaliteta u kojem se djeca javljaju kao počinioci, žrtve ili svjedoci. Prvi dokument, pod gotovo identičnim nazivom (*Vodič za sudije i tužioce na temu visokotehnološkog kriminala i zaštite maloljetnih osoba u Republici Srbiji)* izrađen je 2017. godine, a namijenjen je tužiocima i sudijama polaznicima Osnovnog programa obuke Pravosudne akademije u Republici Srbiji. U tom smislu vodič prati razvijeni i usvojeni Kurikulum od Programskog odbora ove institucije, koja je ovlaštena za realizaciju specijalizovanih programa obuke za sudije i tužioce nosioce certifikata za rad s maloljetnicima kao počiniocima krivičnih djela, odnosno maloljetnim oštećenim osobama, tj. žrtvama krivičnih djela. S obzirom na sadržaj takvog dokumenta, on se može primijeniti na različitim lokacijama, pa je u saradnji s profesorima Univerziteta u Sarajevu izvršeno njegovo prilagođavanje pravnom okviru u Bosni i Hercegovini. Stoga se ova verzija dokumenta smatra prilagođenom i korisnom za obuke sudija i tužilaca u Bosni i Hercegovini, u okviru programa Centara za edukaciju sudija i tuzilaca u F BiH i RS kroz saradnju sa Save the Children.

Autori vodiča prvenstveno imaju u vidu da je informatička revolucija donijela kvalitativni napredak u životima svih ljudi, toliko jak da je praktično više nemoguće zamisliti civilizaciju bez informatičke podrške u svim svojim oblicima koju nam pružaju informacione tehnologije, ali da je s druge strane ovakav eksplozivan razvoj neumitno proizveo i određene prateće posljedice 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 djela iz ove oblasti i analizira normativni okvir koji reguliše ovu oblast u Bosni i Hercegovini, prvenstveno u sferi krivičnopravne reakcije.

Također, uvažena je i činjenica da je u posljednjih nekoliko decenija naročita pažnja na međunarodnom planu posvećena uspostavljanju djelotvorne zaštite djece žrtava savremenih oblika kriminaliteta, posebno imajući u vidu neophodnost poduzimanja zakonodavnih i drugih mjera za sprečavanje svih vidova seksualne eksploatacije i seksualnog zlostavljanja djece, kao i potrebu njihove zaštite, uvažavajući da najbolji interesi djeteta i pravo djeteta da se njegovo mišljenje čuje i uzme u razmatranje predstavljaju jedan od osnovnih principa u ostvarivanju, poštovanju i zaštiti njihovih prava. Države ugovornice, svjesne obima i karaktera ovih pojava, posebno povećane međunarodne trgovine djecom, iskorištavanja djece u prostituciji i pornografiji, odnosno sve izraženije zloupotrebe računarskih sistema i mreža u cilju regrutovanja djece u spomenute svrhe, pored ostalog reagovale su i uspostavljanjem novih normi i standarda koji će biti posebno istaknuti i dale su jasna uputstva za njihovu neposrednu primjenu od nosilaca pravosudnih funkcija.

Vodič sadrži i jasna uputstva za postupanje u slučajevima krivičnih djela na štetu djece i maloljetnika u djelu 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 povezanim s njima. Posebna pažnja posvećena je i praktičnim primjerima iz oblasti visokotehnološkog kriminala uz naglasak na neophodnost unapređenja međunarodne i međuresorne saradnje svih akterima u sferi zaštite djece i ojačavanja sistema.

Sve navedeno autori su uobličili u četiri tematske cjeline:

- Uvod u visokotehnološki kriminal i savremeni trendovi u izvršenju krivičnih djela iz ove oblasti (Branko Stamenković, Posebni tužilac za visokotehnološki kriminal);
- Prvo reagovanje na elektronske dokaze (Saša Živanović, načelnik Odjeljenja za visokotehnološki kriminal UKP MUP Republike Srbije);
- Visokotehnološki kriminal kao krivično djelo u domaćem zakonodavstvu s posebnim osvrtom na tzv. *cyberbullying* i *grooming* (Bojana Paunović, Sudija Apelacionog suda u Beogradu;
- Opće mjere zaštite i iskaz djeteta u krivičnom postupku (dr. Ivana Stevanović, Viši naučni saradnik Instituta za kriminološka i sociološka istraživanja).

Poštovane kolegice i kolege, poštovani čitaoci, nadamo se da će Vodič biti od koristi za bolje razumijevanje složene problematike o kojoj smo pisali i predstavljati još jedan korak naprijed ka uspostavljanju „pravosuđa po mjeri djeteta" u Bosni i Hercegovini.[1]

"Pravosuđe po mjeri djeteta" označava pravosudni sistem koji jamči poštovanje i djelotvorno sprovođenje svih prava djeteta na najvišem mogućem nivou… To je prije svega pravosuđe koje je dostupno, primjereno uzrastu, efikasno, prilagođeno potrebama i pravima djeteta i usredsređeno na te potrebe i prava, uz poštovanje prava djeteta, uključujući pravo na postupak u skladu sa zakonom, pravo da učestvuje u postupku i da razumije postupak, na poštovanje privatnog i porodičnog života i na integritet i dostojanstvo. Ostvarivanje „pravosuđa po mjeri djeteta podrazumijeva pravosuđe prilagođeno na način da bude primjerenije djetetu i efikasne postupke dostupne djeci uz osiguranje neophodne nezavisne pravne reprezentacije. Na ovaj način se omogućava djeci da kada dođu u kontakt s pravosudnim sistemom, bilo kao svjedoci, žrtve (oštećeni) ili kao počinioci krivičnih djela, tužioci i podnosioci pritužbi budu u mogućnosti da na adekvatan način zaštite svoja prava i interese.

Prilagođavanje pravosuđa da bude primjerenije djeci u Evropi dio je Agende Evropske unije o pravima djeteta[2] i predstavlja jedan od najvažnijih standarda u oblasti prava djeteta. Uvažavanje osnovnih načela „pravosuđa (pravde) po mjeri djeteta" podrazumijeva primjenu osnovnih principa: principa participacije, uvažavanje najboljih interesa djeteta, poštovanje dostojanstva djeteta, zaštitu od diskriminacije i vladavinu prava (Smjernice Komiteta ministara Vijeća Evrope o pravosuđu po mjeri djeteta – III Osnovna načela – od A do E).

Uvažavanje navedenih principa od posebne je važnosti u svjetlu zaštite maloljetnih osoba kao oštećenih/svjedoka savremenih oblika kriminaliteta od posljedica sekundarne viktimizacije u krivičnom postupku.

[1] *Smjernice Komiteta ministara Vijeća Evrope o pravosuđu po mjeri djeteta*, usvojene 17. novembra 2010. na 1.098. zasjedanju zamjenika ministara Vijeća Evrope – Redigovana verzija od 31. maja 2011.

[2] *Agenda Evropske unije o pravima djeteta* usvojena od Evropske komisije Evropske unije 52011DC0060 od 15. februara 2011. godine 52011DC0060, (52011DC0060, 15. februar 2011. godine).

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

1. Uvod

Revolucija u informacionim tehnologijama je suštinski promijenila društvo i nastavljat će ga mijenjati i ubuduće. Mnogi poslovi su postali jednostavniji za obavljanje. Doskora i u samo određenim dijelovima društva radi racionalizacije radnih procedura korištene su informacione tehnologije u svakodnevnom radu. Danas je teško zamisliti bilo koji dio društva bez utjecaja primjene računara i računarskih sistema. Informacione tehnologije su na sveobuhvatan način danas umiješane i iskorištene u svakom aspektu ljudske aktivnosti.

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

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

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

Ipak, domaći je zakonodavni okvir generalno ograničena teritorija nacionalnog zakonodavstva. Iz tih razloga problemi u ovoj oblasti morali su se riješiti na međunarodnom nivou kroz međunarodni pravni okvir koji je iznjedrio usvajanje adekvatnih međunarodnih pravnih instrumenata. Danas takav instrument predstavlja Konvencije o kibernetičkom kriminalu Vijeća Evrope (CETS 185)[3], čiji je cilj da se suprotstavi ovoj vrsti izazova, uz dužno poštovanje ljudskih prava u novom informatičkom i postinformatičkom društvu.

[3] Budimpešta, 23.11.2001. godine, stupila na snagu 01.07.2004. godine, stupila na snagu u odnosu na BiH 01.09.2006. godine; objava „Službeni glasnik BiH" – Međunarodni ugovori broj: 06/2006

2. Međunarodni značaj računarskog kriminala

Prema nekim izvorima[4] koji prate globalni trend izvršenja krivičnih djela u oblasti računarskog, to jest kibernetičkog kriminala, motivaciju koja stoji iza izvršenja ovog, ali i drugih oblika protivpravnog društvenog ponašanja, moguće je podijeliti na pet glavnih grupa, i to kao motivaciju uperenu ka:

- računarskim – visokotehnološkim krivičnim djelima (kibernetičkom kriminalitetu),
- „haktivizmu“,
- kibernetičkoj špijunaži,
- kibernetičkom 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 promjena u odnosu između ovih grupa, što je moguće vidjeti već na uporednom prikazu podataka koji su obrađeni u junu 2015. i novembru 2016. godine i koji ukazuju na to da prostor koji zahvata računarski kriminal raste iz godine u godinu značajnom stopom. Tako, npr., 2015. godine procijenjeni je udio računarskog, to jest visokotehnološkog kriminala u odnosu na druge grupe iznosio 59,5%, dok je već u 2016. godini taj udio porastao na 82,7%. Najveći pad su doživjele aktivnosti koje pripadaju tzv. „haktivizmu“, o čemu će biti više riječi detaljnije u daljem tekstu, dok su grupe kojima pripadaju kibernetička špijunaža i ratovanje, kao i ostali oblici izvršenja ovih djela ili događaja ostali na približno istim nivoima.

Što se pravaca izvršenja ovih krivičnih djela tiče, primijećeno je da je dosta prisutno uvjerenje da su žrtve, tj. oštećeni u ovoj oblasti ponajviše fizičke osobe. Ipak, podaci govore drugačije i ukazuju na to da ustvari najveću grupu oštećenih čine pravne osobe, tj. poduzeća koja obavljaju komercijalnu djelatnost. Odmah iz ove grupe i to s vrlo sličnim procentom (oko 21%), dolaze državni organi kao mete i žrtve kibernetičkih napada. Tek nakon ove dvije grupe (koje zajedno zauzimaju skoro 44% od ukupnog broja izvršenja ovih krivičnih djela) dolazi grupa koja pripada fizičkim osobama, i to s procijenjenim procentom od oko 12% od ukupnog broja. Nakon ove tri glavne grupe meta napada (ujedno i žrtava) skoro ravnomjerno raspoređeno dolaze razne organizacije, obrazovne institucije, finansijski sektor itd.

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

Što se prepoznatih sredstava i pravaca tiče, najveći dio pripada raznim oblicima malicioznog softvera koji je korišten za napade na komercijalne usluge koje pružaju razne pravne osobe s namjerom ostvarivanja zarade. Nakon malicioznog softvera pojavljuje se tzv. „otimanje naloga“, tj. neovlašteno preuzimanje korisničkih naloga na raznim platformama, uključujući one

[4] www.hackmageddon.com

koje pripadaju društvenim mrežama, elektronskoj pošti, bankarskim uslugama i sl. Za ovim kategorijama slijede specifični oblici kao što su SQL injekcije, Distribuisani DoS napadi, izmjena naslovnih strana određenih internetskih prezentacija (*defacement*) i sl.

Kada govorimo o šteti koja nastaje protivpravnim ponašanjem putem korištenja računara i računarskih mreža, a posebno krivičnih djela koja se mogu označiti kao visokotehnološka, treba imati na umu procjenu određenih javnih izvora[5] 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 djela kao i novčanih i materijalnih sredstava koja su fizičke i pravne osobe uložile u otklanjanje štete i dodatnu preventivnu zaštitu nakon ovakvih događaja. Stvarna šteta procijenjena je na iznos od 114 milijardi USD, dok je otklanjanje štete i podizanje nivoa sigurnosti koštalo 274 milijardi USD.

Poređenja radi, svjetska trgovina najpopularnijim nelegalnim narkoticima, tj. opojnim drogama, kao što su marihuana, kokain i heroin, procijenjena je na godišnjem nivou na iznos od 288 milijardi USD, dok je ukupna svjetska trgovina nelegalnim narkoticima procijenjena zbirno na iznos od 411 milijardi USD.

Iz jednostavnog poređenja iznosa procijenjene štete od računarskog kriminala i vrijednosti trgovine opojnim drogama proizilazi jasan zaključak da trgovina potonjim tek za nekih 23 milijarde USD premašuje prethodni iznos, što u svjetskim razmjerama zaista ne predstavlja značajnu brojku. Ovaj podatak je značajniji tim prije što izvršenje krivičnih djela koje za svoj objekat imaju opojne droge podrazumijeva prisustvo izuzetnog rizika po izvršioce ovih krivičnih djela u vidu reakcije državnih organa kako pojedinačnih zemalja, tako i koordinisani nastup i saradnju ovih organa na svjetskom nivou radi suzbijanja ove vrste kriminaliteta, koji u velikom broju slučajeva podrazumijeva i upotrebu fizičke sile i vatrenog oružja.

S druge strane, u svom najvećem dijelu izvršenje krivičnih djela tzv. kibernetičkog kriminala podrazumijeva upravo suprotno, tj. još uvijek postoji odsustvo značajnijeg angažovanja državnih organa kao i, skoro sigurno, odsustvo primjene jakih mjera represivne državne sile.

Navedeni primjeri ustvari dodatno pojašnjavaju prisutni trend koji se kreće u pravcu pomjeranja aktivnosti pripadnika kriminogenih sredina iz oblasti visoko rizičnih krivičnih djela 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 je trend uočen kako na globalnom, tako i lokalnom nivou.

3. Razvoj računarskog kriminala u Bosni i Hercegovini

Nesumnjivo je da je visokotehnološki kriminal u Bosni i Hercegovini mnogo stariji od njegovog inkriminisanja i implementacije zakonskih opisa ovih krivičnih djela u domaće krivičnopravne propise. Kao začetak u procesu inkriminisanja visokotehnološkog kriminala u Bosni i Hercegovini

[5] http://resources.infosecinstitute.com

možemo smatrati reformu krivičnog zakonodavstva iz 2003. godine, koja je obuhvatila kako materijalno, tako i procesno krivično pravo. Na području materijalnog krivičnog prava to je značilo uvođenje novih krivičnih djela u zakonske propise, dok je na području krivičnog procesnog prava to značilo definisanje pojmova visokotehnološkog kriminala kako bi se olakšalo procesuiranje ovih krivičnih djela, posebno u dijelu koji se odnosio na radnje dokazivanja. Ipak, značenja pojmova „kompjuterski sistem" i „kompjuterski podatak" u cilju adekvatnijeg suprotstavljanja ovom vidu kriminala bivaju implementirana u zakonske propise na području krivičnog postupanja tek 2009. godine. Bez ikakve dileme, a prateći razvoj informatičkih tehnologija, kojem smo u posljednjih skoro tri decenije mogli i lično posvjedočiti, možemo utvrditi kako se propisivanje ovih krivičnih djela kao i pojmova s ovog područja u Bosni i Hercegovini događa prilično kasno. Jedno od provedenih istraživanja na temu ponašanja djece na internetu rezultiralo je zaključkom da se djeca od devet do 17 godina u Bosni i Hercegovini gotovo bez izuzetka koriste savremenim informaciono-komunikacijskim tehnologijama, i što je vrlo relevantno, korisnici su interneta.[6]

Današnji statistički pokazatelji o obimu ovih krivičnih djela vode ka zaključku kako ona ne predstavljaju veću društvenu opasnost, s čime bismo se međutim teško mogli složiti. Možda je prije riječ o tome da otkrivanje, a potom i adekvatno procesuiranje ove vrste krivičnih djela još nije na nivou koji bismo mogli smatrati zadovoljavajućim. Navodimo neke od tih pokazatelja:

Osuđeni punoljetni počinioci krivičnih djela protiv sistema elektronske obrade podataka u Federaciji BiH za period 2010–2017.[7]

Godina	2010.	2011.	2012.	2013.	2014.	2015.	2016.	2017.	UKUPNO
Broj osuđenih punoljetnih počinilaca	10	18	22	4	-	5	8	4	**60**

Osuđeni punoljetni počinioci krivičnih djela protiv sigurnosti računarskih podataka u Republici Srpskoj za period 2011–2017.[8]

Godina	2011.	2012.	2013.	2014.	2015.	2016.	2017.	UKUPNO
Broj osuđenih punoljetnih počinilaca	-	2	2	-	2	-	2	**8**

[6] Muratbegović, E., Kobajica, S. i Vujović, S. (2016). *Nasilje nad djecom putem informaciono-komunikaijskih tehnologija u Bosni i Hercegovini*, CPRC, Save the Children, Sarajevo, str. 149.

[7] Statistika pravosuđa 2017, Statistički bilten br. 272/2018, Bosna i Hercegovina, Federalni zavod za statistiku, Sarajevo, 2018.

[8] Pravosuđe, Statistički godišnjak Republike Srpske, Republika Srpska, Republički zavod za statistiku, Banja Luka, 2018., 2017., 2016, 2015., 2014., 2013. i 2012.

U vezi s dinamikom nastanka i razvoja fenomena visokotehnološkog kriminala u Bosni i Hercegovini, između ostalih, posebno se ističu sljedeće karakteristike i okolnosti:[9]

1. zakonodavni problemi;
2. socio-ekonomska situacija;
3. otvorenost granica;
4. porast broja korisnika kompjutera.

Svaka od navedenih okolnosti kao i sve zajedno u svojoj ukupnosti doprinose otežavanju suzbijanja visokotehnološkog kriminala u našoj državi. Za očekivati je da će bosanko-hercegovačko društvo u vremenu koje slijedi ipak pronaći načina da adekvatnije odgovori ovakvom vidu kriminalnog ponašanja koje će sigurno iz mnoštva razloga, pa i onih posve banalnih, kao što je kontinuirano povećanje broja korisnika ovog vida tehnologija, dovesti i do većeg stepena njihove zloupotrebe. U tom smislu bit će potrebno poduzeti mnoštvo mjera, ne samo u vidu propisivanja novih inkriminacija ili pukom preuzimanju različitih pojmova iz međunarodnih dokumenata da bi se samo nominalno ispunile međunarodne obaveze već konkretnih mjera na edukaciji specijalizovanog osoblja, kao i mjera na uspostavi posebnih organizacijskih jedinica u okviru pravosuđa i policijskih agencija specijalizovanih za otkrivanje i procesuiranje ove vrste krivičnih djela.

4. Konvencija Vijeća Evrope o visokotehnološkom (kibernetičkom) kriminalu (CETS 185)

Konvencija o visokotehnološkom (kibernetičkom) kriminalu Vijeća Evrope je prvi međunarodni sporazum, tj. pravni akt, koji reguliše materijalni, procesni i međunarodni pravni okvir za krivična djela koja su izvršena putem računara, računarskih mreža, kao i korištenjem interneta i drugih računarskih mreža međunarodnog ili lokalnog karaktera.

Konvencija postavlja osnove pravnih normi koje se tiču kršenja prava intelektualne svojine, prevara izvršenih korištenjem računara, zloupotrebe maloljetnika u pornografske svrhe, protivpravnog pristupa zaštićenom računaru i računarskoj mreži, presretanju podataka itd. Ovom konvencijom su propisane i radnje i mjere kako materijalno, tako i procesno-pravne prirode, koje su usmjerene ka negativnom sankcionisanju društveno štetnog ponašanja u ovoj oblasti i koje primjenjuju savremene istražne metode prilikom otkrivanja i gonjenja izvršilaca krivičnih djela, kao što su pretraga računarskih mreža i presretanje računarskih podataka, čiji je glavni cilj gonjenje izvršilaca krivičnih djela i uspostavljanje zajedničke krivično pravne politike koja je usmjerena ka zaštiti društva od svih oblika visokotehnološkog, tj. kibernetičkog kriminala, posebno kroz usvajanje odgovarajućih pravnih normi i uspostavljanje operativne međunarodne saradnje u ovoj oblasti.

Konvencija o kibernetičkom kriminalu Vijeća Evrope je nakon višegodišnjeg perioda usaglašavanja izvornog teksta otvorena za potpisivanje od strane članica Vijeća Evrope 23. novembra 2001.

[9] V. Budimlić, M. i Puharić, P. (2009) *Kompjuterski kriminalitet: kriminološki, krivičnopravni, kriminalistički i sigurnosni aspekti, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije*, Sarajevo str. 47–48.

godine, kao i za potpisivanje od strane zemalja koje nisu članice ove organizacije, a koje imaju interes da primjenjuju odredbe Konvencije i da učestvuju u međunarodnoj saradnji.

Činjenica je da ova konvencija trenutno predstavlja jedini međunarodno pravno priznati i kontinentalno rašireni 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 djelotvornog međunarodnog mehanizma, koji je sastavljen od više organskih cjelina na nivou pojedinih zemalja koje su potpisale ili ratifikovale ovu konvenciju.

Ove zemlje kroz na taj način 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. kibernetičkog kriminala, koje pred njih stavljaju izvršioci ovih krivičnih djela.

Do 1. jula 2017. godine više od 59 zemalja ratifikovalo je ovu konvenciju, zatražilo pristupanje ovoj konvenciji ili ju je potpisalo. Osam zemalja nisu članice Vijeća 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 trenutku, samo Republika Irska i Švedska nisu i ratifikovale ovu konvenciju, ali je jesu potpisale, dok su sve ostale zemlje članice Evropske unije Konvenciju i ratifikovale, te se ona u skladu s unutrašnjim pravnim porecima zemalja potpisnica aktivno primjenjuje kroz unutrašnje materijalno, procesno i međunarodnopravne odredbe.

4.1. Cilj i struktura Konvencije Vijeća Evrope o visokotehnološkom kriminalu

Konvencija Vijeća Evrope o visokotehnološkom kriminalu za svoj cilj ima na prvom mjestu harmonizaciju domaćih materijalnih krivičnopravnih odredbi u oblasti računarskog kriminala, omogućavanje domaćem krivičnom procesno-pravnom okviru da nadležnim državnim organima pruži ovlaštenja koja su neophodna za efektno otkrivanje i gonjenje izvršilaca ovih krivičnih djela, 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. **Mjere koje se trebaju poduzeti na domaćem nivou – materijalno i procesno pravo,**
III. **Međunarodna saradnja i**
IV. **Završne odredbe.**

Prvi odjeljak druge glave predviđa odredbe o sankcionisanju kriminala koji je izvršen pomoću računara i računarskih mreža i koji određuje devet općih krivičnih djela koja su podijeljena u četiri različite kategorije.

Krivična djela koja su određena konvencijom su:

1. **neovlašteni (protivpravni) pristup,**
2. **neovlašteno (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 djela dječije pornografije i**
9. **krivična djela autorskih i srodnih prava.**

U odjeljku 2 druge Glave, kada govorimo o procesnim odredbama, predviđeno je:

1. **hitno čuvanje pohranjenih podataka,**
2. **hitno čuvanje i djelimično otkrivanje podataka o saobraćaju,**
3. **naredba za dostavljanje,**
4. **pretraga i zapljena računarskih podataka,**
5. **prikupljanje podataka o saobraćaju u realnom vremenu,**
6. **presretanje podataka o saobraćaju.**

U trećem odjeljku 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 izručenje. Poglavlje govori o tradicionalnoj međunarodnoj saradnji u krivičnoj materiji u dvije situacije:

- kada ne postoji pravna osnova u vidu sporazuma, reciprociteta itd. između strana potpisnica konvencije, u kojem se slučaju primjenjuju odredbe same konvencije, kao i u slučajevima kada takva osnova postoji,
- kada se primjenjuju odredbe tih pravnih okvira uz pomoć primjene same konvencije.

Također, u glavi III su sadržane odredbe o posebnim oblicima prekograničnog pristupa pohranjenim računarskim podacima koji ne zahtijevaju postupak međunarodne pravne pomoći, kao i uspostavljanje takozvane „24/7“ mreže za hitno reagovanje, radi omogućavanja brze i efektivne saradnje između nadležnih organa strana potpisnica.

4.2. Pojmovna određenja

U okviru poglavlja I Konvencija na opći način definiše pojmove kao što su računarski sistem, računarski podaci, pružalac usluga, podaci o saobraćaju itd., što je preneseno 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 i izlazne uređaje, kao i uređaje za pohranjivanje. Također, on može biti sačinjen kao samostalan uređaj koji nije povezan na računarsku mrežu ili kao uređaj koji je povezan na mrežu s drugim sličnim uređajima.

Pod automatskom obradom podataka smatra 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 koji može biti izvršen od računara radi postizanja određenih tj. željenih rezultata. Računari mogu koristiti različite programe.

Računarski sistem obično se 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 s glavnom procesorskom jedinicom, kao što su štampači, videobimovi, 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 korištenjem oba načina. 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 također 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 također postoje, bez obzira na to jesu li ili nisu povezane na internet i međusobno su osposobljene da komuniciraju razmjenom 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 prosljeđivanju podataka između drugih računara i računarskih sistema. Ono što je esencijalno bitno je to da podaci upotrebom ovakvih sistema mogu i jesu razmijenjeni putem mreže, tj. međusobne povezanosti.

Konvencija se prilikom definisanja računarskih podataka oslanja na definiciju takvih podataka prema takozvanim ISO-standardima. Ova definicija sadrži izraze koji su pogodni za procesuiranje, tj. korištenje. Ovo znači da su podaci da bi imali kvalitet računarskih sastavljeni u takvoj formi da mogu biti direktno obrađeni – procesuirani od računarskog sistema.

Da bi bilo potpuno jasno da podaci na koje se odnosi Konvencija trebaju biti podvedeni pod podatke u elektronskoj ili u drugoj formi koja je podobna za računarsko procesuiranje, izraz „računarski podaci“ uveden je i definisan.

Na osnovu ove definicije računarski podaci su oni podaci koji su u smislu krivičnopravnog zakonodavstva automatski procesuirani i mogu biti meta, tj. predmet izvršenja krivičnih djela koja su definisana navedenom Konvencijom, kao i objekat primjene neke od istražnih mjera koje su njome predviđene.

4.3. Pružalac usluga

Termin pružalac internetskih usluga tj. *Internet service provider* („ISP"), obuhvata široku kategoriju fizičkih i pravnih osoba koje imaju određene uloge u odnosu na komunikaciju ili procesuiranje podataka u računarskim sistemima. Pod ovom definicijom jasno je 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. Primjer zatvorene grupe mogu biti zaposleni u okviru privatnog poduzeća kojima je ovakva vrsta komunikacije omogućena od kompanijske mreže.

U okviru ove definicije jasno je da se izraz pružalac usluga također 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 procesuiraju podatke u ime i za račun korisnika servisa koji su spomenuti pod ovom definicijom.

Naprimjer, 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 naprimjer osoba koja sklopi ugovor s kompanijom za takozvano „web-hostovanje" radi „hostovanja", tj. čuvanja i prikazivanja njegove/njene web-stranice – prezentacije, nije obuhvaćan ovom definicijom, ukoliko entitet kod koga se navedeni sadržaj nalazi također ne pruža komunikacione ili obrađivačke usluge podataka.

4.4. Podaci o saobraćaju

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

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

Posljedično, 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 djela.

S tim u vezi, uobičajene procedure, radnje i mjere koje u standardnom vođenju krivičnog postupka od nadležnog organa otkrivanja ili gonjenja bivaju poduzete radi utvrđivanja postojanja krivičnog djela 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 primjenu standardnih istražnih metoda mogu predstavljati jednu od ključnih prepreka za uspješno gonjenje u ovoj krivičnopravnoj oblasti.

Konvencija taksativno nabraja kategorije podataka o saobraćaju i to u vidu porijekla – izvora komunikacije, njenog odredišta, puta, vremena, datuma, veličine, trajanja i vrste usluge koja je pružena. Vrijedno je spomenuti da neće sve ove kategorije biti uvijek tehnički dostupne, posebno kada imamo u vidu raznolikost tehničke opremljenosti i obučenost zaposlenih u raznim poduzećima koja se bave uslugom pružanja pristupa internetu ili omogućavanju korištenja određenih kategorija usluga koje su vezane za korištenje računarskih mreža, kako međunarodnih tako i lokalnih, javnih i privatnih.

Porijeklo komunikacije se odnosi na broj telefona, adresu internetskog protokola ili sličnu identifikaciju komunikacione opreme kojoj pružalac internetskih usluga pruža usluge.

Odredište predstavlja uporedivu indikaciju o uređajima koji služe za komunikaciju i kako je sama komunikacija (tj. podaci) usmjerena, prenesena ili isporučena.

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

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

U tom smislu materijalnopravne odredbe kao i procesnopravne odredbe koje se primjenjuju ili mogu biti primijenjene mogu biti različite, tj. varirati u odnosu na osjetljivost samih podataka.

4.5. Krivična djela

Konvencija u drugoj Glavi u okviru trećeg dijela 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 kao i gonjenja specifičnog oblika, tj. vrste kriminaliteta koji se izvršava pomoću računara i u računarskom okruženju uz korištenje računarskih mreža.

Uspostavljanjem zajedničkog minimalnog standarda u propisivanju krivičnih djela i njihovih bitnih obilježja, 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 podrazumijevati harmonizaciju kako na nacionalnom, tako i na međunarodnom nivou.

Ukoliko bi ovakva harmonizacija materijalnopravnih krivičnih odredbi izostala, primjena drugih međunarodno pravnih instrumenata, kao što je naprimjer 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 primjenjuju 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 uspješno gonjenje izvršilaca krivičnih djela.

Osnovni postulat pružanja međunarodne pravne pomoći u krivičnim stvarima je postojanje kažnjivosti u krivičnopravnom smislu određenog ljudskog ponašanja, koje mora biti propisano kako materijalnopravnim odredbama krivičnog zakonodavstva zemlje molioca, kao i zamoljene zemlje. U slučaju nedostatka harmonizacije materijalnopravnih propisa u ovoj oblasti, kao i u svakoj drugoj oblasti krivičnopravog progona neumitno bi dovelo do neželjenog ishoda u vidu nemogućnosti poduzimanja radnji koje su na 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 djela koja su navedena Konvencijom kibernetičkog kriminala Vijeća 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 dekade aktivno je radio i radi na osavremenjivanju tumačenja i metoda primjene osnovnih odredbi same Konvencije kroz tzv. „uputstva“ (*Guidelines*), koja bi trebale detaljnije pojasniti mogućnost primjene određenih odredbi Konvencije u savremenom životu kao i u savremenom otkrivanju i gonjenju krivičnih djela iz ove oblasti.

Ipak, može se odati priznanje tvorcima teksta ovog međunarodnopravnog akta, koji su u drugoj polovini 90-tih godina XX vijeka uspjeli skoro u potpunosti definisati, propisati i predvidjeti preovlađujuće oblike tzv. kibernetičkog kriminaliteta te ih utkati u tkivo Konvencije, koja i poslije skoro 20 godina od nastanka prvobitnog teksta, uz manje korekcije, donošenjem dodatnog protokola i izdavanjem prethodno spomenutih uputstava uspijeva u svijetu koji se skoro dnevno mijenja, kao što je svijet informaciono-komunikacionih tehnologija i socijalnog umrežavanja korištenjem tih tehnologija, odgovoriti na izazove koji se nalaze pred onim pripadnicima društva kojima je data ustavna i zakonska nadležnost da to štite od štetnih društvenih pojava.

Kriminalizacija tih ponašanja u vidu protivpravnog pristupa, protivpravnog presretanja, ometanja podataka, ometanja sistema i zloupotrebe uređaja, kao i krivičnih djela kao što su računarski falsifikat, računarska prevara, zloupotreba maloljetnika u pornografske svrhe (dječija pornografija), kao i krivična djela 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 osoba u ovoj oblasti, ukazuje na to da i pored proteka već navedenog perioda i brze promjene navedenih tehnologija, u svojoj biti izvršenje krivičnih djela, uključujući i njihove nove oblike i nove načine izvršenja u tzv. kibernetičkom svijetu, mogu se uspješno predvidjeti, definisati i sankcionisati.

Time se otvara put da primjenom alata generalne i specijalne krivičnopravne prevencije ovi oblici kriminaliteta budu, u najboljem slučaju, iskorijenjeni 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 svijeta današnjice, a koja predstavljaju glavni pokretački motiv postupanja službenih osoba koje se nalaze u sistemu krivičnopravne zaštite i koji su posvećeni borbi protiv svih oblika kriminaliteta.

Treba imati u vidu da se u ovoj oblasti pored redovnog seta vještina s kojima pripadnici ovih organa moraju raspolagati, podrazumijeva da policajci, tužioci i sudije moraju raspolagati i dodatnim znanjima i vještinama, često tehničkog i tehnološkog karaktera, kako bi bili u mogućnosti da pravovremeno, kvalitetno i uspješno odgovore izazovima ovog kriminaliteta.

4.6. Procesno pravo

Tehnološka revolucija, a posebno revolucionarni razvoj informacionih tehnologija, koja svoj poseban uspon doživljava od početka XXI vijeka i u okviru toga nezapamćeni razvoj društvenih zajednica koje su u svom nastanku i razvoju koristile usluge internetskih protokola i internetskih tehnologija, međusobno su povezane kroz podjelu zajedničkih resursa na lokalnom i na globalnom nivou, čime neminovno dolaze u kontakt i s kriminogenim sredinama, često bivajući otvorene ili ranjive za zloupotrebu od 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 djela, tako i krivičnih djela koja su specifična za upotrebu informacionih tehnologija. S tim u vezi, nije dovoljno da samo materijalno krivično pravo bude u korak s ovakvim razvojem društvene stvarnosti i njenim zloupotrebama već i procesno pravo s istražnim tehnikama koje su propisane i neophodne za uspješno postupanje u ovoj oblasti također mora biti, čak i više nego materijalno pravo, u skladu sa IKT (informaciono-komunikacionom tehnologijama), pa čak pri tome pokušavajući da bude i korak ispred savremenih tehnoloških zbivanja.

Naravno, zaštitne mjere koje postoje ili su predviđene da budu kontrolni mehanizam za narastajuća ovlaštenja državnih institucija također moraju biti u korak s razvojem tehnologije i krivičnopravnog materijalnog i procesnog okvira.

Jedan od najvećih izazova u borbi protiv visokotehnološkog kriminala u mrežnom okruženju je poteškoća identifikacije izvršioca krivičnog djela i procjena obima štete koju izvršenje takvog krivičnog djela izaziva. Jedan od povezanih problema je osjetljivost elektronskih podataka koji mogu biti vrlo lako izmijenjeni, pomjereni ili izbrisani u nekoliko sekundi. Naprimjer, 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 Vijeća Evrope prilagođava tradicionalne procesne mjere kao što su pretresanje stana i prostorija novom tehničkom okruženju. S tim u vezi, mogu se kreirati i upotrijebiti nove mjere i radnje, kao što su ubrzano čuvanje podataka u cilju osiguravanja da tradicionalne mjere i radnje mogu ostati i dalje upotrebljive u vrlo osjetljivom tehnološkom okruženju.

S obzirom na to da novo tehnološko okruženje nije uvijek 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, također mogu i jesu prilagođene novim okolnostima u namjeri da dozvole prikupljanje elektronskih podataka koji nastaju ili su sastavni dio procesa komunikacije.

Ovom prilikom napominjemo da su neke od ovih mjera navedene i u preporuci Vijeća Evrope broj R (95) 13 u vezi s problemom krivičnoprocesnog prava koji je u vezi s informacionim tehnologijama.

Krivičnopravne materijalne i procesne odredbe se u svom općem obliku odnose na sve tipove podataka, uključujući i tri specifična tipa računarskih podataka koji se mogu podijeliti 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 podoblika i to u:

1. pohranjenom obliku i
2. u obliku korištenja u realnom vremenu u toku komunikacije.

Konvencija predviđa definicije ovih izraza u svojim članovima 1. i 18. Primjenjivost 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 se odnosi i usmjereno je ka uključivanju i održavanju tradicionalnog rječnika koji je poznat u zakonicima o krivičnom postupku, kao što je „pretres stana i prostorija“, „oduzimanje predmeta“ itd., u odnosu na korištenje novih i više tehnoloških orijentisanih računarskih termina kao što je „pristup“ i „kopiranje“, koji su danas već standardno uključeni u tekstove međunarodnog okruženja u vezi s ovim pitanjima.

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

Također, pojam nadležnih organa je posebno u zemljama okruženja u posljednjih deset godina značajno promijenjen, u smislu da su ovlaštenja u istražnom postupku značajno ili u potpunosti

prenesena na državna tužilaštva, u kom smislu je kao *sui generis* ovlaštenje sudske vlasti ostalo staranje o institutima kojima se ograničavaju ljudska prava i slobode, tj. institutima čije je određivanje neophodno radi uspješnog vođenja pretkrivičnog i krivičnog postupka, kao što su tajne mjere nadzora komunikacije, prikupljanje podataka o sadržaju komunikacije itd.

Obuhvat procesnih odredbi, kada govorimo o računarskom kriminalu i "Budimpeštanskoj konvenciji" tj. Konvenciji o kibernetičkom kriminalu Vijeće Evrope, podrazumijeva da će sve zemlje koje su ratifikovale ovu Konvenciju usvojiti takav normativni okvir koji će dalje dati ovlaštenja nadležnim državnim organima da uspješno otkrivaju i gone krivična djela koja su predviđena Konvencijom, druga krivična djela koja su izvršena putem računarskih sistema, kao i prikupljanje dokaza u elektronskoj formi radi vođenja postupka za izvršenje ovih krivičnog djela.

S druge strane, uspostavljanje i primjena ovakve vrste ovlaštenja kroz procesne odredbe treba se pažljivo posmatrati i usmjeriti ka mogućnosti uvjetovanja 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 primjene ovih ovlaštenja kako u općim, tako i u posebnim slučajevima, a čije će propisivanje biti u skladu s 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 podrazumijeva da takav pristup zahtijeva usklađenost potrebe i zahtjeva organa otkrivanja, tj. pripadnika Ministarstva unutrašnjih poslova i sigurnosnih agencija da postupaju u skladu s odredbama Konvencije i drugih međunarodnih i pravnih akata, kojima se osigurava određena zaštita ljudskih prava i sloboda.

U tom smislu Konvencija izričito navodi i time uvažava da države koje su je ratifikovale potječu iz različitih pravnih sistema i kultura te da nije moguće taksativno navesti kao i konkretno odrediti jasno primjenjive uvjete i zaštitne odredbe za svako moguće ovlaštenje 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 primijeni međunarodne instrumente koji su doneseni u ovoj oblasti i koji uključuju Evropsku konvenciju o zaštiti ljudskih prava i osnovnih sloboda iz 1950. godine sa svojim dodatnim protokolima broj 1, 4, 6, 7 i 12, kao i Međunarodnu konvenciju o građanskim i političkim pravima iz 1960. godine, ne isključujući u određenim pravnim sistemima i geografskim dijelovima planete primjenu 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 uvjete za uspostavljanje ovih mehanizama Konvencija specifično zahtijeva da se takvi uvjeti koji se smatraju odgovarajućim u smislu odredbi procesnih zakonodavstava, odnose na pravosudne ili druge nezavisne organe nadzora, koji u okvirima svojih ovlaštenja mogu odobriti na određeni način krivičnopravne procesne alate u smislu vođenja krivičnih postupaka, kao i njihovo eventualno ograničavanje radi osiguravanja i poštovanja ljudskih prava i sloboda.

Imajući ranije navedeno u vidu u smislu procesnih odredbi, Konvencija podrazumijeva takve mehanizme i alate koji podrazumijevaju hitno čuvanje pohranjenih računarskih podataka, koji su propisani članovima 16. i 17. Konvencije, i koji se odnose na podatke koji su već prikupljeni i

sačuvani od držaoca podataka, kao što su naprimjer pružaoci internetskih servisa. Ove odredbe se ne odnose na prikupljanje podataka u realnom vremenu, prikupljanje podataka o budućem saobraćaju ili pristup komunikacijama u realnom vremenu. Mjere koje su opisane u ovom članu se odnose samo na podatke koji već postoje i koji su pohranjeni.

Treba naglasiti da se čuvanje podataka mora razlikovati od pohranjivanja podataka. Iako su na prvi pogled ovi pojmovi slični, postoji bitna razlika između ovih termina u odnosu na njihovo korištenje 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 utjecati na njihov kvalitet ili uvjete u kojima bi oni eventualno bili izmijenjeni ili oštećeni.

„**Retencija podataka**" označava čuvanje podataka koji se trenutno proizvode – generišu u nečijem posjedu od sadašnjeg momenta ka budućnosti. Retencija podataka dalje označava akumulaciju podataka u sadašnjosti i njihovo čuvanje za buduće i u budućem periodu. Retencija podataka je ustvari postupak odlaganja podataka, dok je prezervacija podataka aktivnost koja označava čuvanje podataka na sigurnom i osiguranom mjestu.

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 koji su prikupljeni od pružalaca internetskih servisa ili drugog entiteta, tj. privrednog subjekta u toku obavljanja njihovih poslova. Prezervacija/očuvanje podataka se odnosi i primjenjuje na računarske podatke koji su pohranjeni od strane sredstava računarskog sistema, što prethodno podrazumijeva 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 djelimično pohranjivanje podataka o saobraćaju** (član 17.),
- **naredbu o dostavljanju podataka** (član 18.),
- **pretragu i zapljenu 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 mjera posebno je interesantno osvrnuti se na tzv. „naredbu o pružanju podataka", koja predstavlja fleksibilnu mjeru koju bi pripadnici organa otkrivanja mogli primijeniti u različitim slučajevima, posebno u onim momentima kada druge vrste mjera, kao što su naredbe o pretresu, zapljeni, presretanju komunikacija i slično, zahtijevaju ispunjavanje značajnijih i zahtjevnijih pravnih i tehničkih uvjeta.

Primjena ovog proceduralnog mehanizama posebno je korisna i može se odnositi na računarske podatke ili podatke o pretplatniku koji se nalaze u posjedu ili kontroli određene osobe ili pružaoca. Naravno, ova je mjera primjenjiva ukoliko osoba ili pružalac servisa takvu

vrstu podataka čuva. *Treba biti svjestan da u pojedinim zemljama u svijetu ne postoji obaveza pružaoca internetskog servisa da ovakve vrste podataka čuvaju, tj. pohranjuju.*

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

Također, pojam pretplatnika uključuje široki pojam klijenata pružalaca servisa, od osoba koje su na osnovu ugovornog odnosa korisnici usluga tog poduzeća, do onih koji su povremeni pretplatnici samo za određenu priliku i u određenom ograničenom vremenskom trajanju, pa sve do onih koji usluge određenog pružaoca koriste bez nadoknade.

U toku krivične istrage pretplatnička informacija će se najverovatnije zatražiti u dvije situacije, tj. primjera. U prvom primjeru pretplatnička informacija potrebna je radi identifikacije koje je servise i tehničke mjere određena osoba koristila ili ih još koristi, a ta je osoba pretplatnik, kao što su tip telefonskog servisa (je li mobilna ili fiksna linija), tip drugih pridruženih servisa tj. usluga (kao što je, naprimjer, prosljeđivanje poziva, govorna pošta itd.), telefonski broj ili tehnička adresa (IP-adresa, e-mail adresa).

U drugom primjeru, kada je tehnička adresa poznata, pretplatnička informacija će se zatražiti i bit će potrebna radi ustanovljavanja identiteta osobe u pitanju.

Druge pretplatničke informacije, kao što su komercijalne informacije o naplati, tj. uvjetima plaćanja koje pretplatnik ima, također mogu biti od značaja za vođenje krivične istrage, posebno u slučajevima kada se istraga vodi radi utvrđivanja krivičnog djela i odgovornosti za računarsku prevaru za "klasično" krivično djelo prevare, kao i druga krivična djela koja su usmjerena protiv imovine osobe, platnog prometa i privrede.

Također, podaci o pretplatniku nisu ograničeni samo na informacije koje se odnose na direktnu upotrebu komunikacionih servisa. One također mogu podrazumijevati bilo koju informaciju, osim informacija o saobraćaju ili o sadržaju saobraćaja, na osnovu kojih 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 također mogu obuhvatiti i podatke gdje je određena komunikaciona oprema instalirana (kablovski modem, naprimjer), a ta je informacija na raspolaganju na osnovu ugovora o zasnivanju pretplatničkog odnosa i instalaciji navedenog uređaja od ovlaštene servisne osobe pružaoca internetskog servisa, tj. poduzeća.

Pored informacije o mjestu i adresi gdje je navedena oprema instalirana, ovakva vrsta informacije je također bitna sa stanovišta utvrđivanja činjenice da takva vrsta opreme nije lako pokretna, već da je na osnovu tehničkih pokazatelja u okviru rada navedenog poduzeća – pružaoca internetskog servisa, potvrđeno da je takva vrsta opreme funkcionalna na adresi na kojoj je i instalirana od ovlaštenih osoba, shodno čemu je jasno da podaci koji se nalaze u ugovoru o zasnivanju pretplatničkog odnosa odgovaraju realnom stanju stvari.

Treba naglasiti da su ova ovlaštenja vezana s odredbama članova 14. i 15. Konvencije o visokotehnološkom kriminalu Vijeća 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 za ovakve vrste radnji po svim elementima ili samo u nekima za koje se može smatrati da su osjetljivi sa stanovišta zaštite ličnih podataka, može tražiti kontrola pravosudnih ili drugih samostalnih i nezavisnih organa.

4.7. Međunarodna saradnja

Konvencija o visokotehnološkom kriminalu Vijeća Evrope u svom trećem poglavlju reguliše u članovima od 23. do 35. međunarodnu pravnu pomoć u krivičnim stvarima u oblasti tzv. kibernetičkog 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 umanjiti svaki negativni utjecaj na brz i neometan protok informacija i dokaza u međunarodnom okruženju.

Također, međunarodna saradnja bi trebala biti usmjerena i obuhvatati i sva krivična djela koja se odnose na računare i računarske sisteme kao i podatke koji su generisani od računara, koji su upotrijebljeni ili na drugi način iskorišteni u toku računarske komunikacije kao i prikupljanje dokaza u elektronskoj formi u vezi s izvršenjem krivičnih djela. Ovo znači da, bez obzira na to je li krivično djelo izvršeno upotrebom računara, računarskog sistema ili se radi o uobičajenom vršenju krivičnog djela koje nije izvršeno putem računara, ali uključuje elektronske dokaze, članovi Konvencije u ovoj Glavi mogu i trebaju biti primijenjeni.

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 primjene ovih mjera, kada se radi o međunarodnoj saradnji.

Posebno je bitno naglasiti da međunarodna saradnja u oblasti kibernetičkog kriminala treba biti u skladu s odredbama ove glave i kroz primjer, ali i kroz primjenu svih relevantnih međunarodnih sporazuma u vezi s 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 osjetljivi te da uz nekoliko pritisaka na računarsku tastaturu ili usljed izvršenja automatskog programa, navedeni podaci mogu biti izbrisani ili na drugi način trajno uništeni, čime bi identifikacija izvršioca krivičnog

djela ili upotreba možda kritičnog djela dokaznog materijala kojim bi se dokazalo postojanje krivičnog djela i krivičnopravna odgovornost njegovog počinioca bila onemogućena. Neki oblici računarskih podataka pohrane se samo u vrlo kratkom periodu prije nego što se obrišu, tj. učine na drugi način trajno nedostupnim. U drugim slučajevima značajna šteta može se pričiniti kako ljudima, tako i imovini, ukoliko se ova vrsta dokaza ne prikupi vrlo brzo.

U takvim hitnim slučajevima ne samo slanje zahtjeva na hitan način već i odgovor na hitan način moraju se omogućiti i izvršiti. Iz tog razloga od krucijalne je važnosti omogućavanje ubrzavanja procesa ostvarivanja međunarodne pravne pomoći u krivičnim stvarima, upravo u cilju izbjegavanja gubitaka kritičnih informacija ili dokaza, koji bi, ukoliko se ovakva vrsta i način postupanja i izvršenja ne bi preuzeli, 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 razmjena pismene dokumentacije ili dokumentacije kroz diplomatske kanale ili poštanski sistem vrlo spora te da zahtijeva korištenje složenih međunarodnih procedura. Ovakav način pružanja međunarodne pravne pomoći u oblasti visokotehnološkog kriminala praktično predstavlja jednu od glavnih, ako ne i glavnu prepreku uspješnom krivičnom gonjenju ulasti kriminaliteta.

Iz tih razloga se ističe neophodnost pružanja međunarodne pravne pomoći na način kao što je to navedeno, tj. omogućavanje da se ona vrlo brzo postigne kroz primjenu takvih mjera 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 se korištenje modernih sredstava komunikacije, kao što su elektronska pošta, faks, VOIP-komunikacija, videokonferencije, upotreba direktne komunikacije i razmjene podataka putem mobilnih uređaja koji koriste internetsko okruženje itd. postavlja kao uvjet bez kojeg se ne može postići željeni cilj.

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

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

Bitno je imati u vidu da radnje koje mi poduzimamo za tastaturom našeg računara u toku, naprimjer, radnog vremena, skoro trenutno imaju posljedice i 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 međunarodnopravnoj pomoći u krivičnim stvarima zahtijeva dodatne kanale komunikacije i saradnje upravo radi davanja odgovora svim ovim izazovima koje donosi informatičko i postinformatičko doba. Dobra iskustva grupe „G-8“, koja je također za potrebe saradnje te grupe zemalja formirala sličnu „24/7 mrežu“ kontakata i saradnje, ukazala su na mogućnost uspostavljanja takvog modaliteta direktne saradnje u hitnim slučajevima na osnovu, kao i u okvirima ove konvencije Vijeća Evrope.

Članom 35. ove konvencije svaka zemlja koja ju je ratifikovala ima obavezu da odredi tačku kontakta koja će biti na raspolaganju 24 sata dnevno, sedam dana u sedmici, tokom cijele godine, radi omogućavanja hitnog, tj. trenutnog 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 primjene Konvencije i omogućavanja efektivnog odgovora organa otkrivanja, organa gonjenja i sudova na izazove koje nam donosi savremeni računarski kriminalitet.

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

Zemlje koje su ratifikovale Konvenciju zadržavaju slobodu da odrede gdje će se navedena tačka kontakta uspostaviti. Najbolje rezultate u okviru do sada uspostavljene prakse pružaju kontaktne tačke koje su na prvom mjestu uspostavljene u javnim/državnim tužilaštvima, inistarstvima pravde.

Razlog uspješnosti saradnje državnih, tj. javnih tužilaštava leži u tome što se u skoro svim zemljama koje su sada ratifikovale ovu Konvenciju primjenjuju odredbe Zakonika o krivičnom postupku, koje omogućavaju državnim tužiocima vođenje tzv. „tužilačke istrage“, koja mijenja klasični koncept istrage i sprovođenje istrage od istražnog odjeljenja/istražnog sudije suda, čime se znatno s jedne strane ubrzava vođenje krivične istrage, dok s 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 mjere koje pripadnici ministarstava unutrašnjih poslova primjenjuju.

Ovo je posebno stoga što se u stavu 2. člana 35. Konvencije navodi da je jedan od ključnih zadataka koje kontaktne tačke ove mreže trebaju ispuniti upravo mogućnost uspostavljanja brzog izvršenja onih funkcija i zadataka koji su neophodni radi brzog postupanja u ovoj krivičnopravnoj materiji. Naprimjer, ukoliko je tačka kontakta „24/7“ 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, naprimjer, ovlašteno ministarstvo za izvršavanje međunarodne pravne pomoći, javno tužilaštvo itd., radi postizanja pravovremene i pravilne reakcije na određeni međunarodni zahtjev koji može biti ispostavljen u bilo koje doba dana ili noći. Također, ne treba zanemariti ni potrebu da tačka kontakta ima takav kapacitet da na najbrži mogući način izvrši komunikaciju s drugim članicama, tj. drugim kontaktnim tačkama ove mreže na najbrži mogući način.

5. Direktiva 2013/40/EU

Direktivu 2013/40/EU donio je Evropski parlament 20. augusta 2013. godine i odnosi se na napade usmjerene protiv informacionih sistema. Direktiva mijenja okvirnu odluku Vijeća 2005/222/JHA i predstavlja sastavni dio tzv. *Acqui 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 koji se odnose na definiciju krivičnih djela i odgovarajućih krivičnopravnih sankcija, kao i unapređenje saradnje između nadležnih organa koji uključuju pripadnike policije i drugih specijalizovanih agencija za sprovođenje zakona članica Unije, kao i nadležnih specijalizovanih agencija i tijela same Evropske unije kao što su EUROJUST, EUROPOL i njegov Evropski centar za računarski kriminal (EC 3), kao i uključivanje u rad Evropske agencije za mrežnu i informatičku sigurnost (ENISA).

Informacioni sistemi u okviru ove direktive su identifikovani kao ključni element političke, društvene i ekonomske interakcije u samoj uniji. Društva su trenutno veoma, a u bliskoj budućnosti će još više biti, u odnosu zavisnosti od korištenja navedenih sistema. Neometana upotreba, kao i njihova sigurnost u okviru zemalja članica unije, od vitalnog je interesa za razvoj kako internih tržišta tako kao i moderne, inovativne i kompetitivne tržišne ekonomije. Ovakve vrste napada predstavljaju prijetnju postizanju cilja sigurnijeg informatičkog društva te prijetnju i oblasti sloboda, sigurnosti i pravde. Iz tih razloga zahtijevaju odgovor na nivou Evropske unije kroz unapređenje saradnje i koordinacije na međunarodnom nivou.

Činjenica je da postoji veliki broj objekata u svom fizičkom ili softverskom obliku koji predstavljaju dijelove kritične infrastrukture te bi prekidanje rada ili uništenje ovakve vrste infrastrukture imalo za posljedicu nanošenje značajne štete kako direktno stanovnicima Evropske unije, tako i njihovoj imovini. Postalo je jasno da postoji potreba da se kritična infrastruktura definiše kao sredstvo, sistem ili dio sredstava iz sistema, koji su od esencijalne važnosti 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, čije bi narušavanje ili uništenje dovelo do, vrlo je moguće, katastrofalnih posljedica.

Postoje dokazi koji ukazuju na tendenciju rastuće opasnosti i ponavljanja napada u velikom obimu i snazi koji su usmjereni protiv informatičkih sistema, a koji su od kritičnog značaja za zemlje članice unije. Ova tendencija je popraćena i razvojem sofisticiranih metoda kao što su proizvodnja i korištenja tzv. *bot netova*, koji uključuju nekoliko nivoa izvršenja krivičnog djela, gdje svaki od tih nivoa može predstavljati značajan rizik za javni interes.

Ova direktiva između ostalog uvodi krivične sankcije za novo krivično djelo u vidu pravljenja i korištenja *bot netova*, kao čin uspostavljanja udaljene kontrole nad značajnim brojem računara putem njihovog inficiranja kroz instalaciju malicioznog softvera, a kroz precizno usmjerene kibernetičke napade. Jednom kad se takva mreža kreira, ona 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 izmjenu komercijalno bitnih povjerljivih informacija i podataka. Posebna pažnja treba se usmjeriti ka podizanju svijesti malih i srednjih poduzeća u cilju identifikacije ovakve vrste opasnosti, kao i ranjivosti tih poduzeća u ovom smislu, a kroz njihovu rastuću zavisnost od korištenja informacionih sistema. Bitno je također naglasiti da ova direktiva propisuje visinu krivičnih sankcija, tj. barem za ona krivična djela koja se ne smatraju kao manje društveno opasna.

Države članice unije mogu propisati šta predstavlja manje društveno opasna djela u skladu s njihovim nacionalnim zakonodavstvima i praksom. Naprimjer, krivično djelo u tom smislu može biti nanošenje štete integritetu računara, računarskih sistema i podataka u takvoj mjeri i na takav način koji ne prelazi određeni prag krivičnopravne odgovornosti koja zahtijeva reakciju organa otkrivanja i gonjenja u okviru krivičnog postupka.

S druge strane direktiva, posebno u oblasti napada protiv informacionih sistema, zahtijeva efektivno, proporcionalno i dovoljno odvraćajuće krivičnopravne sankcije i njihovu visinu, kao i unapređenje saradnje među pravosudnim i drugim nadležnim organima, a što se sve ne može postići samo od pojedinačnih zemalja članica, već bi se trebalo postići na nivou same Evropske unije, iz kojih razloga unija može ostvariti takve vrste mjera koje su u skladu s principom supsidijariteta koje je propisano članom 5. Ugovora o Evropskoj uniji.

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

- „**Pravna osoba**“ predstavlja entitet koji ima status pravne osobe pod primjenjivim zakonom, ali ne uključuje države, tj. državne ili javne organe, institucije ili tijela koja postupaju u ime države, kao ni javne međunarodne organizacije.
- „**Bez prava**“ označava postupak na koji se odnosi dio Direktive koji uključuje pristup, ometanje ili presretanje koji nije ovlašten od vlasnika ili drugog ovlaštenog nosioca određenog prava na sistemu ili njegovom dijelu, ili nije dozvoljeno na osnovu domaćeg zakonodavstva.

U svom daljem tekstu Direktiva daje elemente bića krivičnih djela kao što su neovlašteni pristup informacionom sistemu, neovlašteno ometanje sistema, neovlašteno ometanje podataka, korištenje sredstava za izvršenje ovih krivičnih djela.

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 moraju uvesti takve vrste krivičnih sankcija za navedena krivična djela koje će biti efektivne, proporcionalne i dovoljno odvraćajuće u odnosu na izvršioce krivičnih djela.

S tim u vezi, Direktiva predviđa obavezu da se za navedena krivična djela zaprijeti kazna zatvora s najdužim rokom trajanja od najmanje dvije godine i to za krivična djela koja se ne smatraju manje društveno opasnim.

Također, krivična djela neovlaštenog ometanja sistema i neovlaštenog ometanja podataka kada su učinjena s umišljajem, moraju biti zaprijećena s maksimumom od najmanje tri godine, kada je došlo do značajnijeg oštećenja informacionog sistema i njihovog broja kroz korištenje alata na koje se odnosi član 7. Direktive, tj. uređaja i programa koji su dizajnirani ili adaptirani prvenstveno u tu svrhu.

Također, za krivična djela iz članova 4. i 5. Direktiva predviđa da treba biti zaprijećena, tj. propisana najviša kazna od najmanje pet godina zatvora u slučajevima:

- kada su ovakva krivična djela izvršena od kriminalne organizacije definisane kroz okvirnu odluku 2008/841/JHA, bez obzira na kaznu koja je propisana za samu organizaciju;
- ukoliko je izvršenje krivičnog djela načinilo ozbiljnu štetu ili
- ukoliko je krivično djelo izvršeno protiv informacionog sistema kritične infrastrukture.

U svom članu 17. Direktiva je obavezala Evropsku Komisiju da do 4. septembra 2017. godine podnese izvještaj Evropskom parlamentu i Vijeću u okviru kojeg će postojati procjena primjene ove direktive od zemalja članica, u smislu jesu li poduzele neophodne mjere radi poštovanja Direktive i, ukoliko je to potrebno, dostavljanje zakonodavnih predloga. Komisija će također uzeti u obzir i tehnički i pravni razvoj u oblasti kibernetičkog kriminala, posebno imajući u vidu obuhvat ove direktive.

6. Normativni i institucionalni okvir u Bosni i Hercegovini

6.1. Konvencije, protokoli i zakonski okvir u Bosni i Hercegovini[10]

Odluka o ratifikaciji Konvencije o kibernetičkom kriminalu iz 2006. godine.[11] Potvrđivanjem navedene Konvencije Bosna i Hercegovina se obavezala na usvajanje pojmova u vezi s kompjuterskim kriminalom ustanovljenih Konvencijom, usklađivanje svog materijalnog i procesnog krivičnog prava kao i međunarodnu saradnju na polju suzbijanja kompjuterskog kriminala.

Odluka o ratifikaciji Dodatnog protokola uz Konvenciju o kibernetičkom kriminalu, a u vezi s kažnjavanjem djela rasističke i ksenofobične prirode učinjenih putem kompjuterskih sistema također iz 2006. godine.[12] Navedenim protokolom je predviđeno inkriminisanje djela rasističke i ksenofobične prirode učinjenih putem kompjuterskih sistema koja nisu bila obuvaćena prethodno donesenom Konvencijom.

Odluka o ratifikaciji Fakultativnog protokola uz Konvenciju o pravima djeteta koji se odnosi na prodaju djece, dječiju prostituciju i dječiju pornografiju iz 2002. godine.[13] Navedenim Protokolom predviđa se, između ostalog, obaveza implementacije mjera zaštite prava djeteta u krivičnom postupku, mjera kojima bi se osigurala odgovarajuća obuka za osobe koje rade sa žrtvama protupravnih radnji zabranjenih prema ovom Protokolu i propisuje obavezu ustanovljavanja mjera kako bi se zaštitila sigurnost i integritet osoba i/ili organizacija uključenih u sprečavanje i/ili zaštitu i rehabilitaciju žrtava takvih nezakonitih radnji.

[10] Zakonodavni okvir bliže će biti razmatran u takstovima koji slijede.
[11] „Službeni glasnik BiH" – Međunarodni ugovori, br. 6/06
[12] „Službeni glasnik BiH" – Međunarodni ugovori, br. 6/06
[13] „Službeni glasnik BiH" – Međunarodni ugovori, br. 2/05

Odluka o ratifikaciji Konvencije Vijeća Evrope o zaštiti djece od seksualnog iskorištavanja i seksualne zloupotrebe iz 2012. godine[14], koja za cilj ima suzbijanje seksualnog iskorištavanja i seksualnog zlostavljanja djece, zaštitu prava djece žrtava seksualnog iskorištavanja i seksualnog zlostavljanja te unapređenje nacionalne i međunarodne saradnje u borbi protiv seksualnog iskorištavanja i seksualnog zlostavljanja djece.

Krivični zakon Bosne i Hercegovine[15] ne definiše izraze od važnosti za kompjuterski kriminal. U ovom zakonu nisu propisana krivična djela visokotehnološkog, odnosno kompjuterskog kriminala osim što pojedini zakonski opisi krivičnih djela koriste pojmove računarski program i sl. (v. npr. krivično djelo Nedozvoljeno korištenje autorskih prava čl. 243. st. 3.).

Krivični zakon Federacije Bosne i Hercegovine[16] propisuje krivična djela iz domena kompjuterskog kriminala u Glavi XXXII pod nazivom „Krivična djela protiv sistema elektronske obrade podataka“ čl. 393−398. Krivično gonjenje se vrši po službenoj dužnosti. On, međutim, ne definiše značenje izraza od važnosti za kompjuterski kriminal.

Krivični zakonik Republike Srpske[17] propisuje krivična djela kompjuterskog kriminaliteta, također u Glavi XXXII pod nazivom „Krivična djela protiv sigurnosti kompjuterskih podataka“. Osim ove grupe krivičnih djela visokotehnloški kriminal je dijelom i drugih inkriminacija iz ovog zakona, a zbog njegove posebne važnosti izdvajamo krivično djelo iz čl. 178. Iskorištavanje kompjuterske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih djela seksualnog zlostavljanja ili iskorištavanja djeteta. Krivično gonjenje za ova djela se vrši po službenoj dužnosti osim za djelo iz čl. 413. Neovlašteno korištenje kompjutera ili kompjuterske mreže koje se vrši na prijedlog oštećenog. Navedeni Zakon samo djelimično definiše značenje izraza od važnosti za kompjuterski kriminal. U tom smislu vidjeti npr. čl. 123. st. 18., u okviru kojeg se pod pokretnom stvari ima podrazumijevati i svaki registrovani podatak koji je rezultat elektronske obrade podataka (kompjuterski podatak ili program).

Krivični zakon Distrikta Brčko Bosne i Hercegovine[18] kao i prethodna dva zakona također propisuje krivična djela visokotehnološkog kriminala. Inkriminisana su Glavi XXXII kao „Krivična djela protiv sistema elektroničke obrade podataka“. Krivično gonjenje za ova krivična djela poduzima se po službenoj dužnosti, a navedeni zakon ne definiše značenje izraza od važnosti za ovo područje.

Zakon o krivičnom postupku Bosne i Hercegovine[19] u skladu s načelom zakonitosti krivičnog postupanja utvrđuje pravila čiji je cilj da niko nevin ne bude osuđen, a da se počiniocu krivičnog djela u zakonito provedenom postupku izrekne krivičnopravna sankcija pod uvjetima koje propisuje Krivični zakon BiH, ali i drugi zakoni u Bosni i Hercegovini kojima su propisana krivična djela. Zakon o krivičnom postupku BiH kao i drugi zakoni o krivičnom postupku koji su na snazi u Bosni i Hercegovini predstavljaju temeljne pravne izvore u reguliranju procesuiranja

[14] „Službeni glasnik BiH“ – Međunarodni ugovori, br. 11/12
[15] „Službeni glasnik BiH”, br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10, 47/14, 22/15, 40/15 i 35/18
[16] „Službene novine FBiH”, br. 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16 i 75/17
[17] „Službeni glasnik RS”, br. 64/17 i 104/2018 – Odluka US
[18] „Službeni glasnik Distrikta Brčko BiH”, br. 10/03, 45/04, 05/05, 21/10, 52/11, 9/13 i 50/18
[19] „Službeni glasnik BiH”, br. 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09, 72/13 i 65/18

počinilaca krivičnih djela, pa tako i onih s područja kompjuterskog kriminala. Pored propisivanja prava i dužnosti procesnih subjekata te formi radnji koje se poduzimaju u postupku, vrijedi napomenuti da zakon posebno propisuje odgovarajući okvir radnji dokazivanja te posebnih istražnih radnji koje su od iznimne važnosti za dokazivanje, a time i adekvatno procesuiranje svih krivičnih djela, uključujući tu dakako i djela visokotehnološkog kriminala. Zakonom su definisani i izrazi od važnosti za visokotehnološki kriminal. U tom smislu vidjeti odredbe čl. 20. u) i v), kojima su određeni pojmovi „kompjuterski sistem" i „kompjuterski podatak".

Zakon o krivičnom postupku Federacije Bosne i Hercegovine.[20] Sve izneseno u vezi s ZKP BiH vrijedi i za ZKP FBiH.

Zakon o krivičnom postupku Republike Srpske.[21] Prethodno izneseno u vezi s ZKP BiH i ZKP FBiH vrijedi i za ZKP RS.

Zakon krivičnom postupku Distrikta Brčko Bosne i Hercegovine.[22] Isto tako, vidjeti izneseno uz ZKP BiH te entitetske zakone.

Zakon o zaštiti i postupanju s djecom i maloljetnicima u krivičnom postupku Federacije Bosne i Hercegovine iz 2014. godine.[23] Navedenim zakonom propisana su posebna pravila postupanja s djecom koja su u sukobu sa zakonom, mlađim punoljetnim osobama i djecom na čiju je štetu počinjeno krivično djelo, odnosno koja se pojavljuju kao svjedoci u postupku.

Zakon o zaštiti i postupanju s djecom i maloljetnicima u krivičnom postupku Republike Srpske iz 2010. godine.[24] Navedeno u pogledu odredbi Zakona o zaštiti i postupanju s djecom i maloljetnicima u krivičnom postupku F BiH vrijedi i za Zakon Republike Srpske uz napomenu da je Zakon o zaštiti i postupanju s djecom i maloljetnicima u krivičnom postupku RS zapravo i prvi zakon na području maloljetničkog prestupništva koji je donesen u Bosni i Hercegovini.

Zakon o zaštiti i postupanju s djecom i maloljetnicima u krivičnom postupku Distrikta Brčko Bosne i Hercegovine iz 2011. godine.[25] Sve naprijed navedeno u pogledu Federacije BiH i Republike Srpske vrijedi i za Zakon Distrikta Brčko BiH.

Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima iz 2009. godine.[26] Navedenim se zakonom uređuje način i postupak pružanja međunarodne pravne pomoći u krivičnim stvarima ukoliko međunarodnim ugovorom nije drugačije uređeno.

Zakon o komunikacijama Bosne i Hercegovine iz 2003. godine[27], kojim se uređuje oblast komunikacija u Bosni i Hercegovini te uspostavlja i reguliše rad Regulatorne agencije za komunikacije Bosne i Hercegovine (RAK) u skladu s Ustavom Bosne i Hercegovine, koji predviđa uspostavljanje i funkcionisanje zajedničkih i međunarodnih komunikacijskih sredstava.

[20] „Službene novine FBiH", br. 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 09/09, 12/10, 08/13 i 59/14
[21] „Službeni glasnik RS", br. 53/12, 91/17 i 66/18
[22] „Službeni glasnik Distrikta Brčko BiH", br. 10/03, 48/04, 06/05, 12/07, 14/07, 21/07 i 27/14
[23] „Službene novine FBiH", br. 7/14
[24] „Službeni glasnik RS", br. 13/2010, 61/2013 i 68/20
[25] "Službeni glasnik Distrikta Brčko BiH", br. 44/11
[26] „Službeni glasnik BiH", br. 53/2009 i 58/2013
[27] "Službeni glasnik BiH", br. 31/03, 75/06, 32/10 i 98/12

6.2. Podzakonski akti

Pravilo 69/2013 o uvjetima pružanja javnih telekomunikacijskih usluga i odnosima s krajnjim korisnicima Regulatorne agencije za komunikacije Bosne i Hercegovine[28], kojim se određuju osnovni principi pružanja javnih telekomunikacijskih usluga, obaveze operatera javnih telekomunikacijskih usluga u pogledu odnosa s krajnjim korisnicima te se pobliže određuju obaveze propisane posebnim propisima.

Odluka o posebnim obavezama pravnih i fizičkih osoba koje pružaju telekomunikacijske usluge, administriraju telekomunikacijske mreže i vrše telekomukacijske djelatnosti u pogledu obezbjeđenja i održavanja kapaciteta koji će omogućiti ovlaštenim agencijama da vrše zakonito presretanje telekomunikacija, kao i kapaciteta za čuvanje i obezbjeđivanje telekomukacijskih podataka[29] **te njena Odluka o izmjenama i dopunama**[30], kojom se uređuje područje zakonitog presretanja u Bosni i Hercegovini u skladu s rezolucijom Vijeća Evropske unije o zakonitom presretanju telekomunikacija od 17. januara 1995. (OJ 96/C 329/01) i odgovarajućim standardima i preporukama Evropskog instituta za telekomunikacijske norme (ETSI). Odluka ima izuzetan značaj i za definisanje niza pojmova u vezi sa zakonitim presretanjem telekomunikacija.

Pravilnik o provođenju odredbi Zakona o zaštiti ličnih podataka u Regulatornoj agenciji za komunikacije[31], kojim se uređuju uvjeti prikupljanja, obrade i objavljivanja ličnih podataka u skladu sa Zakonom.

7. Institucionalni okvir

U Bosni i Hercegovini ne postoji niti na jednoj od zakonodavnih razina posebno tijelo koje bi isključivo bilo nadležno za gonjenje krivičnih djela visokotehnološkog kriminala kao što je to slučaj npr. s Republikom Srbijom i Posebnim tužilaštvom za borbu protiv visokotehnološkog kriminala. U skladu s tim krivični progon za ova krivična djela ili u vezi s njima vrše odgovarajuće tužilačke institucije na nivoima entiteta Federacije BiH i Republike Srpske te Distrikta Brčko BiH koje su općenito nadležne i za gonjenje svih drugih krivičnih djela. Od policijskih agencija u Bosni i Hercegovini jedino je u okviru MUP-a Republike Srpske uspostavljeno odjeljenje za borbu protiv visokotehnološkog kriminala. Nesumnjivo da i u okviru ostalih policijskih agencija na svim razinama u Bosni i Hercegovini postoje istražioci unutar različitih kriminalističko-istražnih odjela educirani upravo za ovu vrstu kriminala, ipak bez postojanja posebno ustrojenog organizacijskog odjela specijalizovanog za ovu vrstu krivičnih djela može se postaviti pitanje efikasnosti njihovog rada. Ovo sve posebno imajući u vidu da se radi o formi kriminala koja će *pro futuro* samo dobivati na svom obimu. Sa stajališta presuđenja, također ne postoji posebno određen sud ili sudovi koji bi u okvirima svoje nadležnosti postupali u predmetima visokotehnološkog kriminala. Dakle, postupaju sudovi opće nadležnosti.

[28] Regulatorna agencija za komunikacije Bosne i Hercegovine, br. 01-02-929-1/13 od 01.04.2013. godine.
[29] "Službeni glasnik BiH", br. 104/06
[30] "Službeni glasnik BiH", br. 58/07
[31] Regulatorna agencija za komunikacije Bosne i Hercegovine, br. 01-02-3-2364-1/15 od 25.09.2015. godine.

Treba napomenuti da značajnu ulogu na području uređenja sistema pružanja komukacijskih, odnosno telekomunikacijskih usluga u Bosni i Hercegovini, a time i stanovitog vida prevencije visokotehnološkog kriminala imaju i Ministarstvo komunikacija i saobraćaja Bosne i Hercegovine te Regulatorna agencija za komunikacije (RAK). **Ministarstvo komunikacija i saobraćaja Bosne i Hercegovine** vrši aktivnosti na izradi i predlaganju zakonskih propisa na području komunikacija, odnosno telekomunikacija, praćenju primjene zakona i drugih propisa, aktivnostima na međunarodnoj saradnji i sl. **Regulatorna agencija za komunikacije**, s druge strane, kao funkcionalno nezavisna i neprofitna institucija sa statusom pravne osobe prema zakonima Bosne i Hercegovine obavlja svoje dužnosti u skladu s ciljevima i regulatornim principima kao što su regulisanje emiterskih i javnih telekomunikacionih mreža i usluga, uključujući izdavanje dozvola, utvrđivanje cijena, međupovezivanje i definisanje osnovnih uvjeta za osiguravanje zajedničkih i međunarodnih komunikacijskih sredstava i dr.

8. Savremeni trendovi

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

Prilikom kratkog osvrta na početke računarskog kriminaliteta u Republici Srbiji konstatovali smo da je isti više od 40 godina prisutan i da je u decenijama koje su slijedile skoro dekadno doživljavao određene izmjene kako u motivaciji, tako i u načinu izvršenja. Čini se da se zakonitosti „Murovog zakona" (*„broj tranzistora u integrisanom računarskom kolu svake dvije godine biva dupliran")* skoro mogu primijeniti u određenom smislu i na svijet računarskih krivičnih djela. Naime, za razliku od ranijeg perioda, u posljednjih nekoliko godina trendovi izvršenja krivičnih djela se značajno češće mijenjaju kako u svojim osnovnim, tako i u svojim pratećim oblicima, slijedeći ponajviše put kojim svjetska tehnologija i ekonomija idu.

Imajući navedeno u vidu, čini se da je brzina razvoja računarskih i komunikacionih tehnologija kao i ekonomskih kretanja direktno proporcionalna razvoju, trendu i obimu izvršenja krivičnih djela računarskog, tj. kibernetičkog kriminala.

Trendovi izvršenja krivičnih djela u posljednjih nekoliko godina na svjetskom i domaćem nivou mogli su se podijeliti u sedam glavnih pravaca:

1. **Računarski kriminal na mobilnim platformama;**
2. **Intenzivno korištenje bankarskih malvera 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 kriptovaluta (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 vijeka u vidu tzv. „laptop", „notebook", „handheld", „palmtop" i drugih varijanti manjih računarskih uređaja koji su mogli biti lako transportovani, vrlo često i u džepovima odjeće. Prava eksplozija prisustva i korištenja ovakvih uređaja nastaje pojavom prvog pametnog telefona u vidu Apple Inc. iPhone mobilnog telefonskog uređaja, koji u isto vrijeme ima i značajne računarske kapacitete. Svijet današnjice se praktično ne može zamisliti bez prisustva pametnih mobilnih telefona, koji su ustvari mali računarski uređaji koji se prvenstveno koriste za računarsku, a manje originalnu namjenu, tj. obavljanje telefonskih razgovora.

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

8.2. Intenzivno korištenje bankarskih malvera i trojanaca

Računari i mobilni računarski uređaji postali su sastavni dio poslovanja pravnih i fizičkih osoba 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 dio poslovanja finansijskih institucija u javnom i privatnom sektoru. Naravno, imajući u vidu značajan potencijal za stjecanje protivpravne dobiti, ovo polje korištenja računara je postalo jedno od omiljenih i za kriminalnu zloupotrebu.

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

8.3. „Haktivizam“ i zloupotreba računarskih mreža

Prema slobodnim izvorima “**haktivizam**”[32] predstavlja subverzivnu upotreba računara i računarskih mreža za promovisanje političke agende ili socijalnih promjena. S korijenima u kulturi hakera i hakerskoj etici, njegovi ciljevi su često povezani sa slobodom govora, ljudskim pravima ili pokretima koji promovišu slobodan protok informacija. Termin je ušao u upotrebu 1994. godine. Primjetno je da postoje razlike u bližem određivanju ove vrste aktivizima na internetu. Dok neke definicije podrazumijevaju akte kibernetičkog terorizma (*Anonymous*), druge pokušavaju da daju opravdanje upotrebi neovlaštenog pristupa računarima da bi se izvršile društvene promjene.

Ipak, haktivizam u najvećem broju slučajeva predstavlja radnje usmjerene na zlonamjerne i destruktivne radnje pojedinaca koje ustvari podrivaju sigurnost interneta kao tehničke, ekonomske i društvene platforme.

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

8.4. Savremene povrede prava intelektualne svojine

Povrede prava intelektualne svojine spadaju u krivičnopravnom smislu u grupu krivičnih djela koja su dobro poznata javnim tužiocima, zamjenicima javnih tužilaca i sudijama. Može se slobodno konstatovati da je upravo izvršenje ovih krivičnih djela tokom devedesetih godina prošlog i početkom ovog vijeka, 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 procjenama Američke privredne komore[33] u Republici Srbiji do 2015. godine zabilježen je pad neovlaštene upotrebe autorskih prava u oblasti računarskih programa do procenta od 67%. Naravno, taj procent nikako nije zadovoljavajući, imajući u vidu da u zemljama Evropske unije iznosi oko 29% i obavezuje na dalje djelovanje državnih organa.

Posebnu pažnju treba skrenuti na prodaju putem interneta falsifikovanih lijekova i medicinskih preparata. Trend kupovine ovih proizvoda putem računarkih mreža je u uzlaznoj liniji, ali su zabilježeni značajni slučajevi prodaje nelegalnih kopija medikamenata putem internetskog oglašavanja i dostavljanja na kućnu adresu. U nekim od ovih slučajeva je došlo i do životnog ugrožavanja osoba koje su konzumirale ove preparate usljed djelovanja na organizam

[32] https://en.wikipedia.org/wiki/Hacktivism
[33] https://www.amcham.rs

supstanci od kojih su isti bili napravljeni. Nažalost, u svijetu su zabilježni i smrtni slučajevi usljed ovakvog pribavljanja i konzumacije.

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

Ciljani napadi predstavljaju novi oblik izvršenja krivičnih djela u čijoj se osnovi nalazi takozvani „socijalni“ tj. društveni inženjering. Glavne odlike izvršenja ovih krivičnih djela su da njihovi izvršioci na svom raspolaganju imaju široki spektar programskih alata i zlonamjernih programa putem kojih se infiltriraju i preuzimaju kontrolu nad ciljanim računarom i mrežom, ili vrše prismotru tih sistema radi pribavljanja podataka koji nisu javni. Također, ciljani napadi se mogu okarakterisati i kao uporni iz razloga što jednom ostvaren uvid i kontrola nad računarskim procesima mete/žrtve, ne napušta se već koristi do momenta otkrivanja. Ponekad se koristi i dodatni atribut ovih napada u smislu prijetnje koju oni stvaraju, imajući u vidu postojanje specifičnog cilja, obuke, motivisanosti, organizovanosti i postojanja izvora finansiranja.

Trenutno najprisutniji načini izvršenja ovakve organizovane kriminalne akcije se mogu vidjeti u ranije spomenutim predmetima „BEC“ prevara, gdje cilj predstavlja presretanje i kontrola poslovnih komunikacija između dva i/ili više poslovnih entiteta radi preusmjeravanja procesa plaćanja na prevarne račune.

8.6. Pojava i zloupotreba kriptovaluta (Bitcoin, Ethereum, Ripple itd.)

Kriptovalute predstavljaju računarsko programsko digitalno sredstvo dizajnirano radi upotrebe kao sredstvo plaćanja ili razmjene dobara i usluga, koristeći kriptografiju radi osiguranja transakcija i kontrole stvaranja dodatnih jedinica valute. Kriptovalute su klasifikovane kao podskup digitalnih i alternativnih valuta. *Bitcoin* predstavlja prvu poznatu kriptovalutu koja je nastala 2009. godine. *Bitcoin* i njegovi derivati koriste decentralizovanu kontrolu nasuprot centralizovanim elektronskim novčanim i bankarskim sistemima. Naime, kriptovalute ne predstavljaju novac koji izdaje centralna bankarska institucija određene zemlje, već računarski podatak koji se stvara korištenjem određenih programa koji se koriste na internetu i koji se čuva u isključivo elektronskom obliku prolazeći kroz niz različitiih provjera korisnika interneta koji učestvuju u tim transakcija, s obzirom na to da ove vrste valuta ne postoje u “pravom”, tj. štampanom ili kovanom obliku.

Kriptovalute se koriste na različite načine i danas je moguće elektronskim putem kupiti veliki broj dobara i usluga na internetu korištenjem ovog “kibernetičkog novca”. Ipak, bitno je naglasiti da i pored jake promocije ovih valuta od “boraca za slobode i privatnost interneta” kriminalci i kriminalne grupe od samog njihovog nastanka intenzivno koriste ovakav vid plaćanja imajući u vidu poteškoće s kojim se državni organi suočavaju prilikom praćenja ovih transakcija i zapljene kriptovaluta. Posebno treba spomenuti da na manje pristupačnim dijelovima interneta, kao što su *Deep* ili *Dark Web* korištenje ovih valuta predstavlja pravilo prilikom kupoprodaje narkotika, vatrenog oružja, trgovine ljudima i dječijom pornografijom, pa čak i prilikom naručivanja ubistava.

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

Internet stvari predstavlja međuumrežavanje fizičkih objekata, vozila (što se odnosi i na „povezane" i „pametne uređaje"), zgrada i drugih stvari s ugrađenom elektronikom, programima, senzorima koji omogućavaju predmetima da razmjenjuju podatke s 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, pritom se zasnivajući na postojećim i interoperabilnim informacionim i komunikacionim tehnologijama u razvoju". U tu svrhu termin stvar predstavlja „predmet fizičkog svijeta (fizičkih stvari) informacija ili riječ (virtualne stvari), koji je moguće identifikovati i koji može biti integrisan u komunikacionim mrežama".

IoT omogućava da objekti budu opaženi i kontrolisani daljinski putem postojeće mrežne infrastrukture, stvarajući tako priliku za direktniju integraciju fizičkog svijeta 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 internetske infrastrukture. Stručnjaci procjenjuju da će IoT do 2020. godine imati između 26 i 30 milijardi predmeta.

U kontekstu ovog priručnika ova oblast korištenja računara i računarskih mreža predstavlja zaista budućnost kriminala koja je na pomolu. Načini zloupotrebe mogu biti značajni i primjeri koji su već sada zabilježeni u vidu, naprimjer, daljinske kontrole motornih vozila od hakera, aktiviranja i kontrole kućnih uređaja koji su povezani na internet, i to onih čijom se zloupotrebom može nadgledati, pa i utjecati na događaje koji se odvijaju u određenom prostoru, u ovom slučaju privatnom, ukazuju na to da se posebna pažnja mora posvetiti ovoj nastupajućoj opasnosti kao i novim oblicima izvršenja krivičnih djela koji će predstavljati direktni proizvod ovog razvoja tehnologije.

Prvo reagovanje na elektronske dokaze

1. Uvod

U okviru projekata "Spojeni i sigurni – u susret kibernetičkoj sredini koja je sigurna za djecu" stvorila se potreba za dodatnim usavršavanjem te je izvršena edukacija nosilaca pravosudnih funkcija u cilju upoznavanja za prvo reagovanje na elektronske dokaze[34], koja je od vitalnog značaja da pripadnici policije i tužilaštva imaju alatke za efikasno sprečavanje i otkrivanje visokotehnološkog kriminala, što predstavlja novi izazov koji se umnogome razlikuje od konvencionalnih krivičnih istraga.

Savremena tendencija prikupljanja elektronskih dokaznih radnji prilikom postupanja policijskih službenika kako u tradicionalnim krivičnim djelima, tako i u krivičnim djelima visokotehnološkog kriminala tokom privremenog oduzimanja predmeta inicirala je donošenje „Obavezne instrukcije o prikupljanju i osiguranju elektronskih dokaza", kojom se utvrđuje metodologija za prikupljanje elektronskih dokaza tj. njihovo otkrivanje, osiguranje, prikupljanje i evidentiranje u cilju jedinstvenog postupanja policijskih službenika Ministarstva unutrašnjih poslova Republike Srbije s elektronskim dokazima. Navedena instrukcija predstavlja standard za pravilno rukovanje elektronskim dokazima s ciljem sprečavanja njihovog oštećenja, gubitka, modifikacije, transporta i osiguranja autentičnosti elektronskih dokaza neophodnih da se osigura proglašenje osumnjičenog krivim. Ovakva instrukcija ne postoji trenutno u Bosni i Hercegovini.

2. Strategija za prikupljanje digitalnih dokaza

U ovo doba tehnološke revolucije skoro da je nemoguće zamisliti scenarij gdje ne bi bilo moguće da dokaz ili obavještajni podatak nisu snimljeni u nekom elektronskom tj. digitalnom obliku. Imajući to na umu, policijski službenici koji s tužilaštvom istražuju krivična djela trebali bi uvijek uzeti u obzir strategiju za prikupljanje elektronskih dokaza od početka svih svojih upita. Najčešći uređaji koji mogu sadržati elektronske dokaze su: sistemi videonadzora, 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.), digitalni fotoaparati i videokamere, digitalni audiosnimači, digitalni videorekorderi s memorijskim modulima, igračke konzole, MP3 i MP4 plejeri, GPS uređaji, ruteri, pametni kućni aparati poput pametnog TV-a, media plejera, uređaji set top box i dr. Također, veoma je bitno i da se prikupe informacije u pogledu dužine vlasništva nad računarskom opremom, umreženih računara, korištenim

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

operativnim sistemima, ko su sve vlasnici i korisnici računarske opreme, onlajn korisničkih naloga za skladištenje podataka tj. naloga elektronske pošte, podatka koji se odnose na kriptografsku zaštitu, davaoce internetskih usluga i korištenja računarskih mreža, skladištenja elektronskih podataka na drugom lokalitetu i skrivenih uređaja za pohranjivanje podataka.

2.1. Sistemi videonadzora

Sistemi videonadzora sada preovladavaju na većini javnih mjesta. Za sva mjesta izvršenja krivičnog djela, uključujući njihove pristupne i odstupne putanje, trebalo bi provjeriti postoje li sigurnosne kamere. Većina sistema videonadzora će sačuvati snimke samo ograničen period. Da bi se izbjegao gubitak dokaza, policijski službenici moraju poduzeti korake kako bi osigurali dokaze sa sistema videonadzora što je moguće prije.

2.2. Podaci iz otvorenog internetskog izvora

Informacije koje su važne za istragu mogu se objaviti na internetu. Ovi se podaci mogu izgubiti ukoliko policijski službenik ne djeluje brzo kako bi ih sačuvao. Razlog gubitka ne mora biti eventualno uklanjanje elektronskih dokaza tj. podataka od izvršioca ili neke druge osobe, oni mogu nestati zbog vremenskog ograničenja trajanja određenog internetskog domena ili drugom kriminalnom aktivnošću trećih osoba npr. ubacivanjem malicioznih programa tzv. ransomvera[35], 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*[36]), što im daje mogućnost da im pristupe s bilo kog računara ili drugog uređaja. Često se kopije ovih podataka ne čuvaju na lokalnim računarima. Elektronska pošta, tekstualni dokumenti i fajlovi s multimedijalnim sadržajima (slike, muzika i videosnimci) su tipični primjeri. 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.

2.4. Elektronska evidencija i komunikacioni podaci (zadržani podaci)

Internet, telekomunikaciona industrija i druge onlajn organizacije proizvode tokom poslovanja raznu elektronsku evidenciju koja se bilježi kroz zadržane podatke kao što su adresa

[35] *Ransomware* (u pojedinim slučajevima taj tip malvera označava se i kao kriptovirus, kriptotrojani ili kriptocrv) obuhvata klasu malvarea koja ograničava pristup računarskim sistemima koje inficira te zahtijeva plaćanje otkupnine (ucjene) kreatorima malicioznih programa kako bi se ograničenje uklonilo. Izvor: http://www.nod32.com.hr/ThreatCenter/ThreatTest/tabid/2556/Default.aspx#ransomware

[36] Tako naprimjer Evropska unija u svom strateškom dokumentu „Oslobađanje potencijala klaud kompjutinga u Evropi" navodi da: „Klaud kompjuting (*Cloud Computing*) u pojednostavljenom smislu može shvatiti kao čuvanje, obrađivanje i korištenje 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/

internetskog protokola, podaci o saobraćaju, podaci o lokaciji i dr. Ova evidencija može biti od neprocjenjive važnosti za policijskog službenika i kao dokaz i u smislu obavještajnih podataka. U nekim slučajevima to će biti jedine informacije koje povezuju osumnjičenog s krivičnim djelom. Ovakve evidencije u skladu sa čl.128. Zakona o elektronskim komunikacijama ("Sl. glasnik RS", br. 44/2010, 60/2013 - odluka US i 62/2014) čuvaju se 12 mjeseci od dana obavljene komunikacije, a u čl. 129. navedenog zakona definisane su vrste zadržanih podataka. Stoga je potrebno da policijski službenici reaguju brzo da ne bi izgubili dokaze.

2.5. Podaci s uređaja krajnjeg korisnika

„Uređaj krajnjeg korisnika" je opći 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, videokamere, muzički plejeri, Sat-Nav, GPS, optički diskovi i memorijski stikovi i dr. Svi ovi uređaji će imati mogućnost da pruže vitalne dokaze, ali se mora poštovati stroga procedura kada se njima rukuje.

Strategija za prikupljanje digitalnih dokaza bi trebala uzeti u obzir četiri faze u nastavku opisane.

2.5.1. Osiguranje nestalih dokaza

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

- moguće je nasnimiti nešto preko snimaka sistema videonadzora;
- 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 namjerno izmijenjeni, obrisani ili da se preko njih nešto nasnimi;
- očuvanje se može osigurati oduzimanjem uređaja koji sadrži prvobitne podatke, uzimanjem kopije tih podataka ili zahtijevajući od treće osobe da ih sačuva za kasniju potrebu.

Policijski službenik mora biti upoznat s općim principima oduzimanja elektronskih dokaza (uvrštenih u ovaj priručnik) kako bi se osiguralo da ono što poduzme ne ugrozi dokaznu vjerodostojnost podataka.

2.5.2. Elektronsko traganje

Postoje dva aspekta elektronskog traganja:

- utvrđivanje porijekla svake elektronske informacije,
- traganje za osumnjičenim(a) 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 s određenim računarom i korisničkim nalogom.

U većini slučajeva ovo će značiti identifikovanje autora ili kreatora elektronskih podataka preko internetskog protokola tj. IP-adrese računara koji je korišten. Za ovo će vam biti potrebni i tačan datum i vrijeme (uključujući vremenske zone) da je informacija zabilježena. Ova informacija može biti dostavljena pružaocima usluga korištenja internetskih mreža (internetskim pružaocima servisa – ISP), koji će utvrditi ime osobe koja je koristila taj internetski nalog. Tradicionalne policijske vještine će i dalje biti neophodne kako bi se osumnjičeni doveo u vezu s identifikovanim računarom ili internetskim nalogom.

2.5.3. Pretres i zapljena

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 trebali imati na umu prilikom svakog procesa pretresanja i oduzimanja.

2.5.4. Računarsko-digitalno vještačenje

Kada se oduzmu uređaji krajnjeg korisnika, potrebno je da idu na digitalno forenzičko vještačenje kako bi se izvukli svi elektronski dokazi u obliku koji je prihvatljiv za sudove. Bit će potrebno da se elektronski dokazi prikupljeni tokom istrage protumače i predstave tako da oni koji nisu poznavaoci tehnike ili nisu prethodno bili upoznati sa slučajem mogu jednostavno shvatiti povezanost tih dokaza sa slučajem. Ovo je postupak za koji su potrebni specijalističke vještine i znanja.

3. Opći principi

Ovaj vodič između ostalog pruža najbolju praksu u radu s elektronskim dokazima. Postoje četiri opća principa kojih se policijski službenici moraju pridržavati kako bi se očuvala vjerodostojnost dokaza.

Prvi princip

Nikakva akcija koju poduzmu policijske službe ne bi trebala izmijeniti datum na računaru ili uređaju za skladištenje podataka na šta bi naknadno moglo da se računa na sudu. Stoga, potrebno je izvršiti planiranje pretresa elektronskih dokaza, prikupiti informacije o osumnjičenom, lokacijama i procjeni ljudskih kapaciteta i potrebne opreme.

Drugi princip

U slučaju da policijski službenik smatra da je neophodno da pristupi prvobitnom datumu na računaru ili uređaju za skladištenje podataka, on mora biti kompetentan za to i sposoban da pruži dokaz uz objašnjenje zašto je to relevantno i na šta ukazuje taj njihov postupak.

Treći princip

Trebalo bi napraviti i sačuvati trag revizije ili neku drugu evidenciju svih postupaka primijenjenih na elektronske dokaze s računara ii drugog uređaja. Nezavisna treća strana bi trebala pregledati ove postupke i dobiti isti rezultat.

Četvrti princip

Policijski službenik zadužen za istragu (nadležan za taj predmet) u potpunosti je odgovoran da osigura da se postupa po zakonu i ovim principima.

4. Osiguranje dokaza sa sistema videonadzora

U oblasti sigurnosti i praćenja sistemi videonadzora 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 videonadzora, policijski službenik bi se trebao povezati s operaterom sistema i zatraži od njega da sarađuje u osiguranju odgovarajućih snimaka.

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

Noviji digitalni sistemi obično snimaju na interni hard disk preko čega će nakon određenog perioda automatski biti nasnimljen novi snimak. Ovaj period će zavisiti od veličine hard diska i konfiguracije sistema videonadzora. Policijski službenik bi trebao tražiti od operatera na sistemu videonadzora da nabavi kopiju traženih snimaka. Većina sistema će imati opciju za kopiranje podataka na eksterni uređaj (DVD, CD, USB).

U slučajevima kada je dokaz osiguran na samom uređaju sistema videonadzora i ukoliko ga nije moguće kopirati na eksterni uređaj ili optički kompakt disk, policijski službenik bi trebao u skladu sa Zakonikom o krivičnom postupku privremeno oduzeti takav uređaj.

Nakon što se osiguraju podaci sa sistema videonadzora, potrebno je da se predoče na uobičajen način, a potom predaju policijskoj jedinici za obradu videomaterijala. Oni će pohraniti originalni primjerak i pripremiti dokazne kopije podataka u obliku koji je pogodan za potrebe suda.

5. Evidencije i podaci pružalaca komunikacionih usluga

5.1. Dobivanje podataka o komunikaciji

Odlukom Vijeća ministara Bosne i Hercegovine o posebnim obavezama pravnih i fizičkih osoba koje pružaju telekomunikacijske usluge, administriraju telekomunikacijske mreže i vrše telekomunikacijske djelatnosti, u pogledu osiguranja i održavanja kapaciteta koji će omogućiti ovlaštenim agencijama da vrše zakonito presretanje telekomunikacija, kao i kapaciteta za čuvanje i osiguranje telekomunikacijskih podataka i Odlukom o izmjeni te odluke, uspostavljeni su centri interfejsa za zakonito presretanje za potrebe policijskih organa i Obavještajno-sigurnosne agencije (u daljnjem tekstu: OSA-e). Centar za zakonito presretanje interfejsa imat će direktan elektronski pristup sistemu za upravljanje presretanjem kod operatera telekomunikacija, mrežnih operatera, davalaca usluga i davalaca pristupa u Bosni i Hercegovini, kao i sisteme kojima će se osigurati dostavljanje sadržaja telekomunikacije i informacija u vezi s presretanjem centrima za snimanje i monitoring policijskih organa i OSA-e (čl.. 7).

U skladu sa čl. 8. Odluke operateri telekomunikacija, mrežni operateri, davaoci usluga i davaoci pristupa obavezni su osigurati neophodne tehničke i organizacijske preduvjete, iz vlastitih resursa i o vlastitom trošku, da bi omogućili da se zakonito presretanje telekomunikacijskih usluga i aktivnosti provodi od centra interfejsa za zakonito presretanje.

Obaveze operatera telekomunikacija, mrežnih operatera, davalaca usluga i davalaca pristupa su:

- *ugradnja opreme za zakonito presretanje i interfejsa za fiksnu mrežu, mobilnu mrežu i internetsku mrežu u skladu sa ETSI ili drugim standardima;*
- *ugradnja neophodne telekomunikacijske opreme i infrastrukture te tehničkih rješenja u domenu upravljanja telekomunikacijskim mrežama, kojima se omogućuje upravljanje dostavljanjem ciljanih telekomunikacija od centra interfejsa za zakonito presretanje;*
- *dostava sadržaja, kao i podataka u vezi s presretanjem svih ciljanih telekomunikacija s cijelog prostora koji pokriva operater centru interfejsa za zakonito presretanje uz upotrebu minimalnog broja konekcija dovoljnog kapaciteta;*
- *procedure i stručni kadar kojima se osigurava dostava presretanih ciljanih telekomunikacija centru interfejsa za zakonito presretanje u skladu s garantovanim LJoS standardima (čl. 9.).*

5.2. Dobijanje sadržaja komunikacije

"Zakonito presretanje" je navedenom Odlukom određeno kao presretanje i dostavljanje ciljanih telekomunikacija u toku njihovog prijenosa tako da, osim za pošiljaoca ili ciljanog primaoca telekomunikacije, dio ili cijeli sadržaj telekomunikacije i s njom povezanih telekomunikacijskih podataka postane dostupan i ovlaštenoj agenciji, kako je to određeno za posebne istražne ili obavještajne radnje, a u skladu s odredbama zakona u Bosni i Hercegovini (čl. 3. t).

Operateri telekomunikacija, mrežni operateri, davaoci usluga i davaoci pristupa smiju koristiti podatke u vezi s presretanjem i signale, ali ne i sadržaj telekomunikacija dobijen primjenom funkcije zakonitog presretanja, i to samo za potrebe održavanja funkcije zakonitog presretanja i samo na način koji predvidi ili odobri Zajednički upravni odbor (čl. 13. st. 2.).

U skladu s članom 14. Odluke funkcija zakonitog presretanja sastoji se od presretanja telekomunikacija u toku njihovog prenosa, isporuke sadržaja i informacija u vezi s presretanjem i ostalih zahtjeva.

Sa stajališta krivičnog postupanja za provođenja radnji koje imaju karakter zakonitog presretanja potrebna je naredba sudije za prethodni postupak. Ovo se odnosi na primjenu posebnih istražnih radnji kao nezaobilaznog vida prikupljanja dokaza u savremenim uvjetima. Određeni vidovi zakonitog presretanja u hitnim okolnostima mogući su i temeljem naredbe tužioca. Ovdje mislimo na naredbu operateru telekomunikacija ili drugoj pravnoj osobi koja vrši pružanje telekomunikacionih usluga da dostavi podatke o korištenju telekomunikacionih usluga te osobe, ako bi takvi podaci mogli biti dokaz u krivičnom postupku ili poslužiti prikupljanju informacija koje mogu biti od koristi u krivičnom postupku.

5.3. Dobijanje podataka od drugih onlajn usluga u Bosni i Hercegovini

Iz analize dostupnih propisa za Bosnu i Hercegovinu nije bilo moguće utvrditi na koji način se zakonito dobivaju podaci od drugih onlajn usluga. Nema sumnje da bi i u takvim okolnostima trebalo postupiti u skladu s već navedenim odredbama zakona o krivičnom postupku koje se odnose na posebne istražne radnje te privremeno oduzimanje predmeta u smislu dostavljanja podataka o korištenju telekomunikacijskih usluga osobe u pogledu koje postoje osnovi sumnje na počinjenje krivičnog djela.

5.4. Dobijanje podataka iz inozemstva

Postoji mnogo onlajn usluga koje pružaju organizacije koje se nalaze izvan Bosne i Hercegovine i međunarodne organizacije koje svoje podatke drže izvan Bosne i Hercegovine. U tom slučaju je možda neophodna pomoć strane policijske službe. Ovi upiti su često spor postupak. Da bi se spriječio gubitak podataka dok traje postupak međunarodnih upita, preporučuje se da se vlasniku podataka (pružaocu internetskog servisa i dr.) izda Zahtjev za očuvanje podataka, kojim se on obavještava o tome koje informacije se traže. Ovo omogućuje da se podaci očuvaju dok se čeka dobijanje odgovarajućeg pravnog dokumenta tj. međunarodne zamolnice za pružanje pravne pomoći. Zahtjevi za očuvanje podataka trebali bi se upućivati preko kontakt-tačke 24/7 pri Odjeljenju za borbu protiv visokotehnološkog kriminala ili Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala.

Također, veliki pružaoci internetskih usluga poput servisa Facebook, Google, Yahoo i dr. ostvaruju neposrednu komunikaciju s nadležnim institucijama zaduženim za vođenje pretkrivičnog postupka. Primjera radi, kompanija Facebook autorizovanim institucijama za sprovođenje zakona u skladu sa svojom poslovnom politikom i primjenjivim zakonom na

obrazloženi zahtjev nadležnog tužilaštva dostavlja zadržane podatke o svojim korisnicima (internetski protokol i elektronske adrese i dr.).

Više informacija o saradnji u krivičnim istragama s kompanijom Facebook možete naći na internetskoj stranici društvene mreže Facebook[37], koja daje detaljna pravna uputstva poput informacija za policijske službe, zahtjeva na osnovu sudskih rješenja u SAD, podatka o nalogu koje otkrivaju isključivo u skladu sa svojim uvjetima korištenja usluge i važećim zakonom, uključujući savezni Zakon o sačuvanoj komunikaciji (*Stored Communications Act*, *SCA*), 18. tom Kodeksa SAD (U.S.C.), odjeljci 2701–2712., zahtjeva na osnovu međunarodnih sudskih rešenja, čuvanja naloga, zahtjeva u hitnim slučajevima, pitanja vezana za sigurnost djece, zadržavanja i dostupnosti podataka, obliku zahtjeva, pristanku korisnika naloga (ako pripadnik policijske službe traži informacije o korisniku Facebooka 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 s naloga), obavještavanje korisnika naloga čija se provjera traži (politika kompanije Facebook nalaže da ljude koji koriste njihovu uslugu obavijeste o zahtjevima za pristup njihovim informacijama prije nego što te informacije otkriju, osim kada im zakon to zabranjuje ili u izuzetnim okolnostima, kao što su slučajevi eksploatacije djece, hitni slučajevi ili slučajevi u kojima bi obavještenje bilo kontraproduktivno), vještačenja, nadoknade troškova i podnošenja zahtjeva s adresom.

Svi zahtjevi nadležnog tužilaštva moraju sadržavati detaljne informacije o traženim podacima, kao i sljedeće stavke:

- naziv organa koji ga je izdao (navesti nadležno tužilaštvo), broj značke/identifikacionog dokumenta zaduženog policijskog službenika, e-adresu s 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 profila na Facebooku.

6. Podaci iz otvorenih internetskih izvora

Informacija iz otvorenog izvora se definiše kao: “Svaka informacija koja nije označena kao povjerljiva, u bilo kojem sredstvu informisanja, koja je opće dostupna 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 upotrijebiti kao dokaz ili obavještajni podatak u prilog slučaju koji se obrađuje, kao npr. identifikacioni podaci o osobi koje možemo uvezati s nekim elektronskim nalogom ili fotografijom, kućna adresa, telefonski broj, imovina, geografski podaci tj. lokacije, poslovanje i finansijski podaci, povezanost osoba po različitim osnovama, interesovanja i mnogo drugih podataka na osnovu kojih je moguće izvršiti kvalitetnu analizu i profilisanje osoba.

[37] https://www.facebook.com/safety/groups/law/guidelines

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 s bilo kojeg 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 se često naziva „računarstvo u oblacima". U mnogim slučajevima kopije ovih fajlova neće se čuvati na ličnom računaru neke osobe, već će se ti onlajn podaci vjerovatno čuvati u šifrovanom obliku na serverima izvan teritorije Bosne i Hercegovine. Najčešće vrste fajlova koji se u današnje vrijeme skladište onlajn su elektronske poruke, razni dokumenti u različitim formatima i multimedijalni fajlovi (fotografije, muzika i videozapisi). Pristup ovim podacima često može biti izazov za policijske službenike.

Oštećeni i svjedoci

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

Osumnjičeni

Kada se obavlja razgovor s osumnjičenima, važno je pitati ih imaju li pristup bilo kojem onlajn nalogu gdje se mogu pohraniti elektronski podaci. Kada se utvrdi da osumnjičeni ima nalog, trebalo bi ga upitati želi li dobrovoljno pristati 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 osoba dobrovoljno predala svoja korisnička imena i šifre za svoje elektronske naloge policijskim službenicima.

8. Uređaji krajnjeg korisnika (oštećeni/svjedoci)

Kada se obavlja razgovor s oštećenom osobom ili svjedokom, važno je utvrditi da li posjeduje ili kontroliše bilo kakav uređaj koji može sadržati elektronske dokaze. Osjetljivost elektronskih podataka je takva da lako mogu biti oštećeni ili uništeni. Stoga je potrebno poduzeti mjere da se sačuva njihova dokazna vjerodostojnost.

Ukoliko je moguće, policijski službenik bi trebao od oštećene osobe ili svjedoka tražiti da sarađuje i pristane osigurati uređaj kako bi se vještačenjem moglo doći do bilo kakvih dokaza.

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

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

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

Kada policajski službenik ima ovlaštenje da oduzme bilo koji materijal u elektronskom obliku, on može zahtijevati da taj materijal sačini u obliku koji se može ponijeti, da je jasan i čitak.

8.1. Profesionalni svjedoci

U radu s profesionalnim svjedocima koji drže elektronske dokaze kao dio evidencije koju prikupljaju u poslovanju ili pružanju usluga kroz određene internetske prezentacije, kao što su pružaoci internetskih servisa, pružaoci usluga mobilne telefonije i administratori internetskih prezentacija, policijski službenik bi trebao postupiti po sljedećim odjeljcima ovog priručnika:

- Evidencija i podaci pružalaca komunikacionih usluga,
- Specijalne procedure na osnovu najbolje prakse koje ne utječu na izmjenu elektronskih dokaza.

9. Elektronsko traganje

Postoje dva aspekta elektronskog traganja:

- utvrđivanje pravog identiteta neke osobe putem onlajn identifikatora,
- utvrđivanje ko je autor određene elektronske informacije na osnovu adrese internetskog protokola.

9.1. Onlajn identifikator

Skoro svaki pružalac usluga preko interneta koji dozvoljava interakciju korisnika (više od samog pregledanja objavljenih sadržaja) zahtijeva da se kreira korisnički nalog. Ovi nalozi služe da se osigura izvjestan stepen odgovornosti i revizorske funkcionalnosti pružaocu usluga. Stepen verifikacije identiteta koji se odnose na onlajn naloge se u velikoj mjeri razlikuje među pružaocima. U nekim slučajevima se traži veoma malo ličnih podataka da bi se otvorio nalog i ništa od navedenih podataka se ne provjerava. U tim slučajevima navedeni podaci se ne mogu

sa sigurnošću smatrati tačnim. S druge strane postoje nalozi u vezi s kojima se primjenjuju znatne sigurnosne mjere kako bi se potvrdio tačan identitet osobe koja otvara nalog ili mu pristupa. Kada je lični identitet sadržan u onlajn nalogu, dužnost je policijskog službenika da utvrdi njegovo porijeklo prije nego što postupi po toj informaciji.

9.2. Adresa internetskog protokola (IP)

Računari povezani s internetom između sebe komuniciraju koristeći internetski protokol (IP). Svaki računar povezan s internetom mora imati 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 s IP-adresiranjem je u tome što su im jedinstveni identifikatori dodijeljeni za stalno dok IP-adrese često dodjeljuje pružalac internetskog servisa (ISP) svojim klijentima (pretplatnicima) u vidu kratkoročnog zakupa i te adrese nazivamo dinamičkim. Iz tog razloga policijski službenik obavezno mora utvrditi tačan datum i vrijeme (uključujući vremensku zonu) za koje je zainteresovan u vezi s datom IP-adresom. To dozvoljava da pružalac internetskog servisa provjeri svoju evidenciju i utvrdi kojem pretplatniku je dodijeljena posebna IP-adresa u bilo koje vrijeme, kako bi se identifikovao autor određene elektronske informacije. Međutim, ISP čuva ovu evidenciju samo tokom ograničenog perioda. U većini slučajeva je to period od 12 mjeseci. Policijski službenik mora djelovati brzo kako bi osigurao da se ne izgube podaci koji su od ključnog značaja za ulaženje u trag osumnjičenom.

Primjer 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 da računari u okviru neke mreže mogu međusobno komunicirati, ali ne direktno s internetom. Ukoliko računari s 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 = vrijednost između 0 i 255]
- 192.168.xxx.xxx [xxx = vrijednost 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 identifikovati određenu privatnu mrežu ili računar. Važno je da prvo identifikuje internetsku kapiju (*gateway*), što potom vodi identifikaciji privatne mreže.

9.3. Utvrđivanje onlajn identifikatora

Bez obzira na to pokušavate li identifikovati osobu iza nekog „onlajn identiteta" ili pripisujete internetski sadržaj određenoj osobi, metodologija će biti ista. Policijski službenik mora tražiti podatke od pružaoca internetskog servisa ili onih koji posjeduju podatke tj. evidencije o

korisničkim pristupima. Uz verifikovane naloge to može biti dovoljno informacija za djelovanje. U drugim slučajevima može biti neophodno da se zahtijeva istorijat logovanja određenog naloga ili traži IP-adresa koja je povezana s određenom informacijom ili transakcijom (nemojte zaboraviti vrijeme i datum). Napredak u internetskim upitima kako bi se dobile najkvalitetnije informacije koje je moguće verifikovati je vještina koja se razvija isključivo praksom. Policijski službenici i tužioci se ohrabruju da u svom radu upućuju upite koji se tiču interneta jer će to neizostavno proširiti njihove istražne vještine. Internetski upiti o korisnicima opsega IP-adresa koji se nalaze kod jednog od pet svjetskih regionalnih internetskih 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*)[38] najčešće se vrše preko sljedećih onlajn internetskih servisa: https://centralops.net, http://www.infosniper.net i dr.

Nakon što se utvrdi IP-adresa, trebalo bi biti moguće da se ona poveže s nalogom pretplatnika preko odgovarajućeg pružaoca internetskog servisa.

Zapamtite da svi zahtjevi koje se tiču IP-adresa i drugih upita upućenih operaterima telekomunikacija i pružaocima internetskih servisa podliježu Zakoniku o krivičnom postupku i Zakonu o elektronskim komunikacijama.

10. Savjet o pretresanju

10.1. Prije pretresa

Potrudite se da prikupite što više informacija o vrsti, mjestu i konekciji svakog računarskog sistema. Ukoliko planirate pretresanje poslovne prostorije gdje postoje korporativne mreže, potrebno je da se za savjet obratite Posebnom tužilaštvu za borbu protiv visokotehnološkog kriminala ili Odjeljenju za borbu protiv visokotehnološkog kriminala.[39]

10.2. Brifing

Veoma je važno da svi službenici koji prisustvuju mjestu pretresanja budu adekvatno informisani. U ovoj fazi bi trebalo dati savjet o tome kako da se sigurno pribavi svaki dokaz s računara. Trebalo bi dati stroga upozorenja kako bi neobučeni službenici bili spriječeni da pristupaju računarima i nosačima memorija. Timove za pretresanje bi trebalo posavjetovati da se za savjet obrate Posebnom tužilaštvu za borbu protiv visokotehnološkog kriminala prije nego što oduzmu bilo koji računar koji je dio korporativne mreže.

[38] Izvor: https://en.wikiversity.org/wiki/Whois/IP_address

[39] Naglašavamo da u okviru organizacije tužilaštava u Bosni i Hercegovini, odnosno entitetima Federacija BiH i Republika Srpska, kao i u Brčko distriktu BiH nema posebno ustanovljene tužilačke institucije koja bi bila nadležna za procesuiranje ove vrste krivičnih djela.

10.3. Priprema za pretres

Provjerite da li oprema za pretresanje mjesta izvršenja krivičnog djela sadrži odgovarajući materijal za oduzimanje računara, uređaja za pohranjivanje elektronskih podataka i svaki drugi dokaz koji ima veze s tim.

Šta ponijeti:

- fotoaparat i/ili kameru za snimanje lica mjesta i informacija na ekranu,
- rukavice za jednokratnu upotrebu (za sve službenike koji vrše pretres),
- alatke (baterijsku lampu, makaze, šarafciger, kliješta i rezače žica),
- naljepnice za dokazni materijal,
- kese za zaštitu od neovlaštenih izmjena 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 obilježavanje šifri i naziva predmeta koji su uzeti,
- kutije na sklapanje.

10.4. Pretresanje mjesta izvršenja krivičnog djela

Pri dolasku na mjesto izvršenja krivičnog djela ili tokom pretresanja prostorija gdje postoji mogućnost da se nalazi elektronski dokaz na računaru, policijski službenik bi trebao preuzeti kontrolu nad tim mjestom pobrinuvši se da se osobe odmaknu od računara ili drugih uređaja na kojima bi mogli utjecati na dokaz.

Nakon što se osigura prostorija, trebalo bi je snimiti kamerom ili fotografisati prije početka pretresa. Naročito bi trebalo obratiti pažnju na radno mjesto u računarskim sistemima i oko njih te utvrditi da li ima DVD/CD medija u uređaju.

Ukoliko su računari isključeni, nemojte ih uključiti. Ukoliko su uključeni, nemojte pasti u iskušenje da vršite pretragu na njima tražeći dokaze. Za pretragu računara je potrebna posebna vještina. Pristupanje računaru bez primjene odgovarajuće procedure vještačenja će izmijeniti podatke i kompromitovati dokaze.

Što se tiče laptopa, imajte na umu da se neki mogu automatski uključiti samim podizanjem poklopca. Uključivanjem računara promijenit će se datum u operativnom sistemu, što može kompromitovati vjerodostojnost dokaza na njemu.

Uvijek se pridržavajte savjeta o oduzimanju računara navedenih u „Obaveznoj instrukciji o prikupljanju i osiguranju elektronskih dokaza'', donesenoj 26.02. 2013. godine i zavedenoj pod broj: 01-1000/13-12. (UKP br.03/4 1633/13 od 01.03.2013.).

Sjetite se da potražite lozinke koje su često zabilježene u dnevnicima ili bilješkama oko računara.

Potražite priručnike s uputstvima za softver ili oduzete uređaje. To može biti korisno vještaku 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 prenesen na taj odvojeni dio i više nije dostupan na uređaju. Uređaj za skladištenje može fizički biti veoma mali, a da može pohraniti veliku količinu podataka, pa je neophodna temeljna pretraga.

Svi oduzeti predmeti bi trebali biti pažljivo zapakovani i priloženi na uobičajen način. Predmeti bi trebali biti priloženi pojedinačno, osim u slučaju veće količine sličnih predmeta pronađenih na istom mjestu. Naprimjer, svi kompakt diskovi pronađeni na radnom stolu mogu se priložiti zajedno, dok se svi hard diskovi mogu priložiti kao sljedeći dokaz. Međutim, ove dvije vrste predmeta ne bi trebalo izmiješati u jedan dokazni predmet.

Sve dokazne predmete čuvajte dalje od magneta i radioodašiljača.

Sve dokazne materijale bi trebalo evidentirati kao spisak dokaznih materijala u potvrdama o privremeno oduzetim predmetima i zapisnicima i zalijepiti na njih naljepnice na kojima je navedeno mjesto oduzimanja i mjesto za skladištenje.

Kako oduzeti računar (kada je isključen)

- Nemojte uključivati računar.
- Imajte na umu da se laptopi mogu uključiti samim podizanjem poklopca.
- Nemojte dozvoliti osumnjičenima da pristupe uređaju.
- Fotografišite računar i radni sto/mjesto gdje se nalazi.
- Fotografišite kablove koji idu do/od računara.
- Isključite kabel za struju iz zadnjeg dijela računara, a ne iz zida.
- Nacrtajte dijagram i označite kablove za kasnije raspoznavanje povezanih uređaja.
- Posebno pogledajte postoji li bilo kakva internetska 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 mjestu.
- Oduzmite sve priručnike za upotrebu tih uređaja.
- Oduzmite sve bilješke u blizini računara.
- Dokumentujte sve što ste radili.

Laptop

Imajte na umu da se laptopi mogu uključiti samim podizanjem poklopca.

Da biste osigurali da se laptop slučajno ne uključi, preporučuje se da izvadite bateriju.

Kako oduzeti računar (kada je uključen)

- Osigurajte oblast gdje se nalazi kompjuterska oprema.
- Udaljite ljude od računara i napajanja za struju.
- Nemojte dozvoliti da osumnjičeni prilaze bilo kojim uređajima.
- Nemojte koristiti računar niti pretraživati po njemu tražeći dokaze.
- Evidentirajte ono što je na ekranu (fotografija i bilješke).
- Nemojte koristiti tastaturu.
- Ako je aktivan čuvar zaslona, pokret miša bi ga trebao skloniti, koristite miš da prelazite preko otvorenih prozora s *task bara*.
- Ukoliko neka aplikacija briše podatke – odmah isključite računar izvlačeći kabel za struju iz zadnjeg dijela računara. Pojedinim vrstama podatka bi moglo biti nemoguće ponovo pristupiti nakon što bi se isključio računar. Ukoliko sumnjate da neka od otvorenih aplikacija možda sadrži dokaze, prije nego što nastavite trebali biste se obratiti za savjet Odjeljenju za VTK ili Službi za specijalne istražne metode radi eventualnog kreiranja forenzičke kopije RAM[40] memorije.
- Razmislite o tome da pitate korisnika o bilo kojoj od otvorenih aplikacija.
- Vodite pisanu evidenciju o svemu što ste poduzeli.
- Pustite da svi štampači završe štampanje.
- Fotografišite računar i radni sto/mjesto gdje se nalazi.
- Izvadite kabel za napajanje strujom iz zadnjeg dijela 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 postoji li bilo kakva internetska 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 mjestu.
- Oduzmite sve priručnike za upotrebu softvera i oduzetih uređaja.
- Oduzmite sve bilješke u blizini računara.
- Pustite da se oprema ohladi prije premještanja.
- Dokumentujte sve korake poduzete u postupku oduzimanja.

[40] 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 ona 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 sljedećem uključenju računara) ona je potpuno prazna.

Laptopi

Skidanje kabla s laptopa vjerovatno ga neće isključiti jer će se prebaciti na baterijsko napajanje. Da biste ga isključili, pritisnite i držite dugme *on/off* pet do deset sekundi (dok se ne isključi). Potom izvadite bateriju.

Ukoliko su otvorene neke aplikacije (kao što su šifrovane), možda bi bilo bolje da laptop ostavite uključen na baterijskom punjenju i prenesete ga direktno u Upravu kriminalističke policije, Službu za specijalne istražne metode, ukoliko je to moguće. To bi moglo 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 koristeći jedan od sljedeća dva načina:

- ADSL Broadband (npr. BT telefonska linija)[41],
- optički kabel (npr. SBB SOLUTIONS kablovski internet).

Obično pružalac internetskog servisa isporučuje internetsku uslugu Broadband preko modema koji je fizički povezan s telefonskom linijom korisnika. Modem je jednostavan elektronski uređaj koji konvertuje digitalne podatke s računara tako da se mogu prenijeti 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 razmjenjivali podatke i sredstva (kao što su štampači i internetske konekcije). Ruteri daju jednaku mogućnost računarima da budu povezani fizički (Ethernet Cable) ili bežično (WiFi). U praksi nije neuobičajeno da se modem i ruter kombinuju 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. Trebali biste imati na umu da pored desktop računara i laptopa, i drugi portabl uređaji mogu pružiti pristup internetu, poput pametnih telefona, PDA uređaja, igračkih konzola, tablet računara, TV-a koji u sebi sadrže memorijske jedinice i dr.

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

- Osigurajte oblast gdje se nalazi računarska oprema.
- Udaljite ljude od svih računara i napajanja za struju.
- Nemojte dozvoliti da osumnjičeni prilaze bilo kojim uređajima.
- Utvrdite gdje je modem/ruter i isključite ga iz telefona i napajanja.
- Utvrdite gdje su uređaji krajnjeg korisnika (računari, telefoni, personalni digitalni asistent – PDA itd.).

[41] Širokopojasni pristup internetu koji omogućuje velike brzine prijenosa podataka korištenjem telefonske infrastrukture, dok BT telefonska linija podrazumijeva više telefonskih linija kroz jedan priključak.

- Obradite svaki uređaj (odredite prioritete u oduzimanju): je li uređaj uključen (dajte mu prednost u odnosu na isključene), brišu li se podaci (izvucite kabel za struju da biste ga isključili).
- Nemojte koristiti računare niti pokušavati vršiti pretrage na njima tražeći dokaze.
- Sistematski se pozabavite svakim računarom kao što je gore navedeno.

Oduzimanje modema i rutera

Od prirode vaše istrage će zavisiti da li biste trebali oduzeti internetski modem/ruter. Ovi uređaji se ne koriste za skladištenje ličnih fajlova, ali mogu sadržavati fajlove o logovanju i informacije o konfiguracijama koji mogu pomoći pri identifikaciji uređaja koji su preko njih konektovani na internet. Neki od ovih uređaja će izgubiti ove informacije ako se isključe. Ukoliko mislite da informacije s modema/rutera mogu biti od koristi za vaše istrage, onda vas molimo da se dodatno posavjetujete s Odjeljenjem za borbu protiv VTK (bit će vam potrebni detalji i model modema/rutera).

Alternativne metode pristupa internetu

Trebali biste imati na umu činjenicu da pored konvencionalnih internetskih 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, dijeljenje mreže preko pametnih telefona, tablet računara i sl.

Također je moguće da se neko konektuje preko nesigurnog bežičnog rutera nekog u komšiluku (sa ili bez njegovog znanja o tome) ili u nekom restoranu, hotelu, internet-kafeu i sl.

Mrežni serveri i poslovne mreže

Kada se susretnete s poslovnom mrežom i serverom složene infrastrukture, prije nego što bilo šta poduzmete, morate se obratiti za dalju pomoć nekome iz Službe za specijalne istražne metode.

Utvrdite ko je mrežni ili sistemski administrator kako bi pripadnici Službe za specijalne istražne metode mogli s njim razgovarati o mogućim načinima da se osiguraju dokazi.

Imajte na umu da bi ta osoba mogla biti osumnjičena u određenim slučajevima.

Osigurajte to mjesto i nemojte dozvoliti da bilo ko koristi bilo koji od računarskih sistema dok se ne dobiju odgovarajuće smjernice.

UPOZORENJE

Izvlačenje utikača moglo bi:

- ozbiljno oštetiti sistem,
- izazvati gubitak ključnih dokaza,
- omesti zakonito poslovanje,

- stvoriti mogućnost za poduzimanje 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 uskladištiti dokazne podatke direktno na internu memoriju, SIM-karticu ili dodatnu memorijsku karticu. U daljem tekstu je detaljno navedeno kako pravilno oduzeti i sačuvati ove uređaje i s njima povezane dodatne dijelove.

- Ako je uređaj isključen, nemojte ga uključiti.
- Ako je uređaj uključen:
  - fotografišite ili zabilježite sve što je na ekranu,
  - obratite pažnju na to koji datum i vrijeme su na ekranu, a koji su stvarni datum i vrijeme.
- Za uobičajen slučaj oduzimanja isključite telefon.
- Za slučaj opasnosti po život ostavite uređaj uključen.
- Ne padajte u iskušenje da pretražujete po uređaju tražeći dokaze.
- Ukoliko ga posjedujete, stavite telefon u torbu s efektom Faradejevog kaveza[42].
- Pitajte vlasnika želi li dobrovoljno predati PIN ili lozinke.
- Oduzmite sve kablove (uključujući one za napajanje strujom) i držite ih s uređajem.
- Oduzmite sve uređaje za skladištenje (memorijske kartice).
- Dokumentujte sve korake koje ste poduzeli pri oduzimanju uređaja i komponenata.

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

Obavještenje

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 se podaci mogu izmijeniti ili preko njih nasnimiti novi od dolazećih poziva i tekstualnih poruka. Policijski službenici će morati sami procijeniti šta je najbolje da urade u datoj situaciji.

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

Pored računara i mobilnih telefona postoje mnogi drugi digitalni ili elektronski uređaji krajnjih korisnika koji imaju mogućnost da pruže dokazne podatke. Neki od uobičajenih primjera 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 skladištiti podatke koristeći internu memoriju ili dodatne dijelove. U daljem tekstu su navedena uputstva za oduzimanje nosivih uređaja krajnjeg korisnika i s njima povezanih dodatnih dijelova.

- Ako je uređaj isključen, nemojte ga uključivati.
- Ako je uređaj uključen:
- fotografišite ili zabilježite sve što je na ekranu o PDA ostavite uključenim (Pogledajte savjet o PDA). Ostale uređaje isključite.
- Pokupite sve kablove (uključujući one za napajanje strujom i kućišta uređaja).
- Oduzmite sve dodatne uređaje za skladištenje (memorijske kartice).
- Pitajte vlasnika želi li dobrovoljno reći lozinke.
- Dokumentujte sve korake koje ste poduzeli pri oduzimanju uređaja i komponenata.

Savjet o PDA

Isključivanje personalnog digitalnog asistenta (PDA) bi moglo aktivirati traženje lozinke, što sprečava ili odgađa 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 uvijek 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, gdje se može pohraniti i pregledati na odgovarajući način.

Računarsko vještačenje

Policijski službenici nikada ne bi trebali pasti u iskušenje da uključe ili pretražuju sadržaje bilo kojih računara, mobilnih telefona, ostalih elektronskih uređaja krajnjeg korisnika ili s njima povezanih uređaja kada postoji mogućnost da imaju dokaznu vrijednost. 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 bi trebalo smatrati zamjenom za temeljno vještačenje računara. Međutim, to je koristan postupak za utvrđivanje je li oduzet pravi uređaj ili da se odredi prioritet u ispitivanju oduzetih predmeta.

- Savjet o tome je li neki slučaj pogodan za trijažu potražite od Službe za specijalne istražne metode.
- Ispitivanje računara, mobilnih telefona i drugih digitalnih uređaja krajnjeg korisnika zahtijeva vještine specijaliste za digitalno forenzičko vještačenje.
- Zaposleni u Službi za specijalne istražne metode su prošli opsežnu obuku kod akreditovanih organizacija i posjeduju potrebno znanje i iskustvo za obavljanje temeljnog vještačenja, a svoja otkrića predstavljaju u formatu pogodnom za sudske postupke.

- U svim slučajevima u kojima su zajedno s računarima radi ispitivanja oduzeti i mobilni telefoni, njih će obraditi Služba za specijalne istražne metode. Zahtjevi za ovim ispitivanjima se podnose u skladu s postupkom dodjele zadatka Službi za specijalne istražne metode.
- U slučajevima kada su oduzeti samo mobilni telefoni, policijski službenik se za savjet i uputstva mora obratiti Službi za specijalne istražne metode.
- Svi zahtjevi za digitalnim forenzičkim veštačenjem se moraju dostavljati preko Službe za specijalne istražne metode, koja će odrediti prioritete.

Visokotehnološki kriminal kao krivično djelo u domaćem zakonodavstvu s posebnim osvrtom na tzv. cyberbullying i grooming

1. Uvod

U svjetlu globalnog trenda kibernetičkog druženja i života u kibernetičkom prostoru neminovno je da se suočimo s viktimizacijom mladih na društvenim mrežama. Tome nesumnjivo doprinosi nedovoljna kompjuterska informaciona pismenost roditelja, ali mnogo više nedovoljna svijest 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. S njima ih najprije upoznaju roditelji dajući im svoje mobilne telefone ili tablet-računare da se zanimaju dok su oni zauzeti poslom ili su u kafiću, u posjeti kod prijatelja. Djeca se tako zabavljaju, upoznaju svijet, igraju igrice koje nisu uvijek edukativne, uče komunicirati, a da ne moraju da izgovore nijednu riječ. Vremenom djeca smatraju postojanje interneta prosto pitanjem života i bez njega ne bi mogli funkcionisati. Pri svemu tome roditelji neminovno počnu kaskati s umješnošću upotrebe najnovije tehnologije, čiji je razvoj 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 djece na internetu pa i neznanja da sami prepoznaju opasnosti koje vrebaju. Sposobnost roditelja da kontrolišu djecu na internetu zavisi od više faktora, od kojih su neki stepen otvorenosti i bliskosti s djecom, obrazovanje roditelja, posvećenost djeci i dr. S jedne strane roditelji su svjesni da je internet neiscrpan izvor informacija i zabave te da bi samim isključivanjem djece iz svih tih aktivnosti mogli ugroziti socijalizaciju djece, ali istovremeno svjesni i da pojačan nadzor može dovesti do sukoba s djecom. Kod činjenice da ne manjkaju odrasli koji internet koriste na različite zlonamjerne načine, te da djeca također brzo nauče kako da ga zloupotrijebe, današnje društvo se suočava s ozbiljnim problemom – nesigurnošću djece na internetu, naročito na društvenim mrežama.

Organizacija za evropsku sigurnost i saradnju sistematizovala je rizike kojima su izložena djeca kao korisnici interneta. Svi rizici su podijeljeni na rizike usljed izlaganja neprimjerenim sadržajima *(content risk)* i na rizike usljed nesigurnih kontakata s drugim korisnicima *(contact risk)*.

Neprimjereni sadržaji se mogu podijeliti na one čije je cirkulisanje zakonom zabranjeno, na sadržaj neprimjeren uzrastu djece 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 dječije pornografije (nelegalni sadržaji). Scene nasilja i pornografski sadržaji spadaju u materijale neprimjerene uzrastu, dok bi davanje savjeta za samopovređivanje i samoubistvo ili propagiranje poremećaja u ishrani poput anoreksije mogli okarakterisati kao utjecaj na usvajanje negativnih obrazaca ponašanja.

Nesigurne kontakte na internetu eksperti OEBS-a dijele na 1) kontakte putem kojih se stvaraju preduvjeti kako bi se kasnije ostvario kontakt, pri kojem bi dijete moglo biti viktimizovano (građenje odnosa u kojima dijete stječe povjerenje u osobe s kojima kontaktira – *grooming*, da bi se potom ostvarila seksualna eksploatacija djeteta), 2) kontakte usljed kojih su djeca izložena agresivnom ponašanju drugih korisnika (vrijeđanje i podsmijeh obično od drugih vršnjaka ili *cyberbullying*) 3) kontakte putem kojih zbog nepromišljenosti dijete doprinosi nastanku štetne posljedice (kockanje na internetu, učestvovanje u pirateriji koje može uvjetovati kasniju odgovornost i sl.).[43]

2. Krivični zakoni, pojmovna određenja i zaštita djece i maloljetnika

Prema odredbama Krivičnog zakona Bosne i Hercegovine – u daljem tekstu: KZ BiH, djetetom se smatra osoba koja nije navršila 14 godina, dok se pod maloljetnikom podrazumijeva osoba koja nije navršila 18 godina života (čl. 1. st. 13. i 14.). Identične odredbe sadrže Krivični zakon Federacije BiH – u daljem tekstu: KZ FBiH i Krivični zakon Distrikta Brčko BiH, dok Krivični zakonik Republike Srpske – u daljem tekstu: KZ RS u čl. 123. 7) pod djetetom ako je žrtva krivičnog djela, podrazumijeva osobu koja nije navršila 18 godina života. Zakoni o zaštiti i postupanju s djecom i maloljetnicima u krivičnom postupku koji su na snazi u entitetima i Distriktu Brčko BiH definišu dijete kao osobu koja nije navršila 18 godina života (čl. 2. st. 1. ZZPDMKP FBiH, čl. 2. st. 1. ZZPDMKP RS i ZZPDMKP BD BiH). U vezi s navedenim ipak treba praviti razliku između, u krivičnopravnom smislu „djeteta žrtve“, zapravo djeteta na čiju štetu je počinjeno krivično djelo u kojem slučaju se radi o osobi (djetetu) koja nije navršila 18 godina života i „djeteta u sukobu sa zakonom“ zapravo počinitelja krivičnog djela, u krivičnopravnom smislu maloljetnika, kojim se označava osoba (dijete) od navršenih 14 pa do navršenih 18 godina života.

U pogledu značenja izraza „kompjuterski sistem“ i kompjuterski podatak“ krivični zakoni u Bosni i Hercegovini ne sadrže odredbe o značenju navedenih izraza i oni su određeni zakonima o krivičnom postupku. Tako Zakon o krivičnom postupku Bosne i Hercegovine – u daljem tekstu: ZKP BiH u čl.20. u. kao kompjuterski sistem definiše svaku napravu ili grupu međusobno spojenih ili povezanih naprava, od kojih jedna ili više njih na osnovu programa automatski obrađuju podatke, i v) kao „kompjuterski podatak“ definiše svako iskazivanje činjenica, informacija ili koncepata u obliku prikladnom za obradu u kompjuterskom sistemu, uključujući i program koji je u stanju prouzrokovati da kompjuterski sistem izvrši određenu funkciju. Identične odredbe sadrže i Zakon o krivičnom postupku Federacije BiH – u daljem tekstu: ZKP FBiH u čl. 20. u) i v), zatim Zakon o krivičnom postupku Republike Srpske – u daljem tekstu: ZKP RS u čl. 20. r) i s) te Zakon o krivičnom postupku Distrikta Brčko BiH – u daljem tekstu: ZKP BD BiH u čl. 20. u) i v). Treba napomenuti da sva četiri zakona definišu i značenje „telekomunikacijska adresa“, što je pojam u direktnoj vezi s procesuiranjem kompjuterskog kriminala. U tom smislu „telekomunikacijska adresa“ predstavlja svaki telefonski broj, linijski ili mobilni ili e-mail ili internet adresu koju posjeduje ili koristi određena osoba [ZKP BiH čl. 20. s); ZKP FBiH čl. 21. s); ZKP RS čl. 20. p) i ZKP BD BiH čl. 20. s)].

[43] OEBS

Krivična djela kompjuterskog kriminala propisana su entitetskim krivičnim zakonima i Krivičnim zakonom BD BiH. KZ FBiH propisuje krivična djela kompjuterskog kriminala u Glavi XXXII pod nazivom „Krivična djela protiv sistema elektronske obrade podataka". Radi se o slijedećim krivičnim djelima:

1. Oštećenje računarskih podataka i programa (čl. 393);
2. Računarsko krivotvorenje (čl. 394);
3. Računarska prevara (čl. 395);
4. Ometanje rada sistema i mreže elektronske obrade podataka (čl. 396);
5. Neovlašteni pristup zaštićenom sistemu i mreži elektronske obrade podataka (čl. 397) i
6. Računarska sabotaža (čl. 398).

KZ RS krivična djela kompjuterskog kriminaliteta propisuje također u Glavi XXXII pod nazivom „Krivična djela protiv bezbjednosti kompjuterskih podataka". To su:

1. Oštećenje kompjuterskih podataka i programa (čl. 407);
2. Kompjuterska sabotaža (čl. 408);
3. Izrada i unošenje kompjuterskih virusa (čl. 409);
4. Kompjuterska prevara (čl. 410);
5. Neovlašteni pristup zaštićenom kompjuteru, kompjuterskoj mreži, telekomunikacijskoj mreži i elektronskoj obradi podataka (čl. 411);
6. Sprečavanje i ograničavanje pristupa javnoj kompjuterskoj mreži (čl. 412) i
7. Neovlašteno korištenje kompjutera ili kompjuterske mreže (čl. 413);

KZ BD BiH kao i prethodna dva zakona krivična djela kompjuterskog kriminala također propisuje u posebnoj glavi. Inkriminisana su u Glavi XXXII kao „Krivična djela protiv sistema elektroničke obrade podataka". Radi se o slijedećim krivičnim djelima:

1. Oštećenje računarskih podataka i programa (čl. 387);
2. Računarsko krivotvorenje (čl. 388);
3. Računarska prevara (čl. 389);
4. Ometanje rada sistema i mreže elektroničke obrade podataka (čl. 390);
5. Neovlašteni pristup zaštićenom sistemu i mreži elektroničke obrade podataka (čl. 391) i
6. Računarska sabotaža (čl. 392).

Katalozi krivičnih djela kompjuterskog kriminala iz KZ-a BD BiH i KZ-a FBiH praktično su identični kako po nazivima, tako i po zakonskim opisima ovih krivičnih djela za razliku od KZ-a RS, koji se od njih razlikuje kako po broju propisanih krivičnih djela, tako dijelom i po njihovom zakonskom opisu, odnosno radnji i objektu izvršenja. Ipak, kako detaljna analiza svih tih krivičnih djela nije od primarnog značaja za naše razmatranje, kao što je to zaštita djece i maloljetnika, to se u nju nećemo niti upuštati. Ovdje treba također istaknuti kako navedena

krivična djela nisu i jedina krivična djela kompjuterskog kriminala ili kriminala u vezi s njim, jer se u posebnim dijelovima krivičnih zakona susreću i druga krivična djela koja imaju obilježja visokotehnološkog kriminala, s obzirom na to da se npr. kao sredstvo izvršenja pojavljuje kompjuterski sistem, mreža ili komunikacija. Navodimo neke od tih primjera:

1. iskorištavanje kompjuterske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih djela seksualnog zlostavljanja ili iskorištavanja djeteta (čl. 178. KZ-a RS);
2. neovlašteno korištenje ličnih podataka (čl. 157. st. 2. KZ-a RS);
3. povreda privatnosti djeteta (čl. 189. st. 2. KZ-a RS);
4. povreda tajnosti pisama ili drugih pošiljki (čl. 186. st. 2. KZ-a FBiH);
5. neovlašteno prisluškivanje i zvučno snimanje (čl. 185. KZ-a BD BiH) i druga krivična djela.

U narednom poglavlju, a s obzirom i na prirodu samog vodiča, slijedi analiza krivičnih djela na štetu djece i maloljetnika iz odredbi entitetskih i Krivičnog zakona BD BiH s fokusom na seksualno iskorištavanje i zlostavljanje. Naglasit ćemo da KZ BiH ne poznaje grupu krivičnih djela protiv spolne slobode i morala, odnosno spolnog integriteta te seksualnog iskorištavanja i zlostavljanja djece. Iste međutim u potpunosti ili samo djelimično, a kada je riječ o seksualnom zlostavljanju ili iskorištavanju djece i maloljetnika propisuju ostali krivični zakoni koji su na snazi u Bosni i Hercegovini.

3. Zaštita djece od seksualnog zlostavljanja i iskorištavanja u Bosni i Hercegovini

3.1. Republika Srpska

Republika Srpska je jedina od tri zakonodavne razine u Bosni i Hercegovini, na kojima se osigurava krivičnopravna zaštita djece i maloljetnika, koja je u okvire svojih krivičnopravnih normi implementirala i odredbe Konvencije Vijeća Evrope o zaštiti djece od seksualnog iskorištavanja i seksualne zloupotrebe iz 2007. (Lanzarote konvencija), a koju je Bosna i Hercegovina, kako smo to već prethodno ustanovili, potvrdila još 2012. godine. To se posebno može uočiti po činu implementacije potpuno nove grupe krivičnih djela seksualnog iskorištavanja i zlostavljanja djece u Glavi XV Krivičnog zakonika iz 2017. godine. Novim rješenjima zaštita spolnog integriteta djece i maloljetnika te posebno zaštita djece od seksualnog zlostavljanja i iskorištavanja ostvarena je kroz dvije grupe krivičnih djela: onih iz Glave XIV „Krivična djela protiv spolnog integriteta“ i onih iz Glave XV „Krivična djela protiv spolnog zlostavljanja i iskorištavanja djece“. Upravo je potonja grupa rezultat nastojanja da se što adekvatnije provedu odredbe Lanzarote konvencije i time ostvare ciljevi sprečavanja i suzbijanja seksualnog iskorištavanja i zloupotrebe djece. No, moramo naglasiti i da zakonodavac u Republici Srpskoj svoje opredjeljenje za ostvarivanjem maksimalne zaštite djece od ovakvog vida zloupotrebe nije iskazao samo uvođenjem novih inkriminacija te unapređenjem postojećih već i implementacijom drugih krivičnopravnih solucija koje tome trebaju doprinijeti. Ovdje ćemo ukratko navesti neke od njih:

- zabrana ublažavanja kazne u slučajevima obljube nad djetetom mlađim od 15 godina (čl. 54. st. 3);
- mjera sigurnosti potpune zabrane vršenja poziva, djelatnosti ili dužnosti, pri čijem obavljanju se ostvaruje neposredan kontakt s djecom počiniocu krivičnog djela učinjenog na štetu spolnog integriteta djeteta (čl. 77. st. 2.);
- osuda za krivično djelo počinjeno na štetu spolnog integriteta djeteta neće se brisati iz kaznene evidencije (čl. 89. st. 5.);
- vođenje posebnog registra u okviru kaznene evidencije o osobama koje su pravomoćno osuđene za krivična djela na štetu spolnog integriteta djeteta (čl. 92. st. 2.);
- početak toka zastare krivičnog progona za krivična djela počinjena na štetu spolnog integriteta djeteta tek od dana punoljetstva žrtve (čl. 96. st. 3.) i dr.

Dodatnu posebnost rješenja u RS-u na području krivičnopravne zaštite djece i maloljetnika čini i postojanje Zakona o posebnom registru lica pravosnažno osuđenih za krivična djela seksualne zloupotrebe i iskorištavanja djece[44] čiji je cilj zaštita djece od seksualne zloupotrebe, zlostavljanja i iskorištavanja, te sprečavanje lica pravosnažno osuđenih za ta krivična djela da ponovo izvrše isto ili slično krivično djelo.

3.1.1. Krivično djelo iskorištavanje djece za pornografiju (čl. 175. KZ-a RS)

Krivično djelo "Iskorištavanje djece za pornografiju" propisano je u čl. 175. KZ-a RS i pripada katalogu krivičnih djela iz Glave XV "Krivična djela seksualnog zlostavljanja i iskorištavanja". Ovo djelo čini onaj:

- *(1) ko navodi dijete na učestvovanje u snimanju dječije pornografije ili ko organizuje ili omogući snimanje dječije pornografije;*
- *(2) ko neovlašteno snimi, proizvede, nudi, čini dostupnim, distribuiše, širi, uvozi, izvozi, pribavlja za sebe ili za drugoga, prodaje, daje, prikazuje ili posjeduje dječiju pornografiju ili joj svjesno pristupa putem računarske mreže i*
- *(3) ko upotrebom sile, prijetnje, obmane, prevare, zloupotrebom položaja ili teških prilika djeteta ili odnosa zavisnosti, prisili ili navede dijete na snimanje dječije pornografije.*

Za navedene oblike krivičnog djela iskorištavanja djece za pornografiju iz st. 1. i 2. propisane su zatvorske kazne u trajanju od šest mjeseci do pet godina, odnosno jedna do osam godina, a za kvalifikovani oblik iz st. 3. kazna zatvora u trajanju od dvije do deset godina.

U skladu sa st. 4. predmeti korišteni za izvršenje ovog djela se oduzimaju, a pornografski materijal koji je nastao izvršenjem djela se uništava. Važna je odredba st. 5., prema kojoj se dijete neće kazniti za proizvodnju i posjedovanje pornografskog materijala koji prikazuje njega lično ili njega i drugo dijete ako su oni sami taj materijal proizveli i posjeduju ga uz pristanak svakog od njih i isključivo za njihovu ličnu upotrebu. Odredbom st. 6. data je i definicija dječije

[44] „Službeni glasnik RS", br. 31/18

pornografije kao materijala koji vizuelno ili na drugi način prikazuje dijete ili je realno prikazano nepostojeće dijete ili osoba koja izgleda kao dijete, u pravom ili simuliranom (eksplicitnom) evidentnom seksualnom ponašanju ili koji prikazuje spolne organe djece u seksualne svrhe. Konačno, st. 7. propisuje da se materijali koji imaju umjetnički, medicinski ili naučni značaj ne smatraju pornografijom u smislu ovog člana.

3.1.2. Iskorištavanje djece za pornografske predstave (čl. 176. KZ-a RS)

Krivično djelo "Iskorištavanje djece za pornografske predstave" propisano je u čl. 176. KZ-a RS i također pripada katalogu krivičnih djela iz Glave XV. Radi se o krivičnom djelu koje je u okvirima ranijeg krivičnog zakonodavstva u RS-u bilo dijelom dviju inkriminacija "Iskorištavanja djece i maloljetnih osoba za pornografiju" iz čl. 199. i "Proizvodnja, posjedovanje i prikazivanje dječije pornografije" iz čl. 200. KZ-a RS[45], koji više nije na snazi. Novim rješenjima postaje posebnim krivičnim djelom uz inkriminisanje i onih koji pod određenim okolnostima gledaju pornografsku predstavu u kojoj učestvuje dijete. Ovo djelo čini onaj

- *(1) ko navodi dijete na učestvovanje u pornografskim predstavama.*

Propisana kazna za ovo krivično djelo je kazna zatvora u trajanju od šest mjeseci do pet godina. Kvalifikovani oblik djela propisan je u st. 2. i njega čini onaj:

- *(2) ko upotrebom sile, prijetnje, obmane, prevare, zloupotrebom položaja ili teških prilika djeteta ili odnosa zavisnosti, prisili ili navede dijete da učestvuje u pornografskoj predstavi. Kaznit će se kaznom zatvora od dvije do deset godina.*

Za ovaj oblik djela propisana je kazna zatvora u trajanju od dvije do deset godina. Konačno, u st. 3. istog člana inkriminisano je i samo gledanje pornografske predstave u kojoj učestvuje dijete.

- *(3) ko gleda pornografsku predstavu uživo ili putem komunikacijskih sredstava ako je znao ili je trebalo i moglo da zna da u njoj učestvuje dijete.*

Propisana kazna je kao i za osnovni oblik odjela. Konačno u st. 4. posebno se propisuje da će se predmeti korišteni za izvršenje djela oduzeti, a pornografski materijal koji je nastao izvršenjem djela uništiti.

3.1.3. Upoznavanje djece s pornografijom (čl. 177. KZ-a RS)

Krivično djelo "Upoznavanja djece s pornografijom" propisano je u čl. 177. KZ-a RS i kao i prethodna djela pripada katalogu krivičnih djela iz Glave XV. Ovo djelo čini onaj:

- *(1) ko djetetu mlađem od 15 godina proda, pokloni, prikaže ili javnim izlaganjem, posredstvom kompjuterske mreže ili drugih vidova komunikacije ili na drugi način učini dostupnim spise, slike, audio-vizuelni materijal ili druge predmete pornografske sadržine ili mu prikaže pornografsku predstavu.*

[45] „Službeni glasnik RS" br. 49/2003, 108/2004, 37/2006, 70/2006, 73/2010, 1/2012 i 67/2013

Za ovo krivično djelo propisana je kazna zatvora u trajanju od šest mjeseci do tri godine. Kao i u slučaju ostalih krivičnih djela na štetu djece u skladu sa st. 2. predmeti korišteni za izvršenje ovog djela se oduzimaju, a pornografski se materijal uništava.

U st. 3. definiše se pornografija pod kojom se podrazumijeva materijal koji vizuelno ili na drugi način prikazuje osobu u pravom ili simuliranom evidentnom seksualnom ponašanju ili koji prikazuje spolne organe ljudi u seksualne svrhe.

Konačno, odredbom st. 4, a kada je u pitanju ovo krivično djelo iz okvira pornografije, isključuju se materijali koji imaju umjetnički, medicinski ili naučni značaj.

3.1.4. Iskorištavanje kompjuterske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih djela seksualnog zlostavljanja ili iskorištavanja djeteta (čl. 178. KZ-a RS)

I krivično djelo "Iskorištavanje kompjuterske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih djela seksualnog zlostavljanja ili iskorištavanja djeteta" iz čl. 178. KZ-a RS pripada katalogu krivičnih djela iz Glave XV. Ovo djelo nije poznavalo ranije krivično zakonodavstvo RS-a i u potpunosti je rezultat implementacije Lanzarote konvencije. Ovo djelo čini onaj:

- *(1) ko s djetetom starijim od 15 godina, koristeći kompjutersku mrežu ili komunikaciju drugim tehničkim sredstvima, dogovori sastanak radi vršenja obljube ili s njom izjednačene spolne radnje, ili radi proizvodnje pornografskog materijala, ili radi drugih oblika seksualnog iskorištavanja i pojavi se na dogovorenom mjestu radi sastanka.*

Propisana kazna za osnovni oblik ovog djela je jedna do pet godina zatvora. Kvalifikovani oblik djela propisan je u st. 2.:

- *(2) ako je djelo iz stava 1. izvršeno prema djetetu mlađem od 15 godina.*

Za ovaj oblik djela propisana kazna je od dvije do osam godina.

3.2. Federacija Bosne i Hercegovine

U Federaciji BiH zaštita djece od seksualnog zlostavljanja i iskorištavanja još se zasniva na odredbama koje nisu usklađene sa zahtjevima Lanzarote konvencije i koje stoga teško da mogu u savremenim uvjetima odgovoriti zahtjevima suzbijanja ovakvog vida kriminalnog ponašanja.

3.2.1. Iskorištavanje djeteta ili maloljetnika radi pornografije (čl. 211. KZ-a FBiH)

„Iskorištavanje djeteta ili maloljetnika radi pornografije" propisano je čl. 211. KZ-a FBiH i dijelom je kataloga krivičnih djela iz Glave XIX „Krivična djela protiv spolne slobode i morala". Ovo krivično djelo čini onaj:

- *(1) ko dijete ili maloljetnika snimi radi izrade fotografija, audio-vizuelnog materijala ili drugih predmeta pornografskog sadržaja, ili posjeduje ili uvozi ili prodaje ili raspačava ili prikazuje takav materijal, ili te osobe navede na učestvovanje u pornografskoj predstavi.*

Propisana kazna jeste jedna do pet godina zatvora. U st. 2. propisuje se obaveza oduzimanja predmeta koji su bili namijenjeni ili upotrijebljeni za učinjenje ovog krivičnog djela kao i uništenje onih predmeta koji su nastali učinjenjem krivičnog djela.

3.2.2. Upoznavanje djeteta s pornografijom (čl. 212. KZ-a FBiH)

Krivično djelo „Upoznavanje djeteta s pornografijom" iz čl. 212. KZ-a FBiH također pripada katalogu krivičnih djela iz Glave XIX istog Zakona. Ovo krivično djelo čini onaj:

- *(1) ko djetetu proda, prikaže ili javnim izlaganjem ili na drugi način učini pristupačnim spise, slike, audio-vizuelne i druge predmete pornografskog sadržaja ili mu prikaže pornografsku predstavu.*

Propisana kazna jeste novčana ili kazna zatvora do jedne godine. U st. 2. propisuje se oduzimanje predmeta pornografskog sadržaja.

3.2.3. Neovlašteno optičko snimanje (čl. 189. st. 3. KZ-a FBiH)

Krivično djelo "Neovlašteno optičko snimanje" propisano je čl. 189. KZ-a FBiH i pripada katalogu krivičnih djela iz Glave XVII "Krivična djela protiv prava i sloboda čovjeka i građanina", a za potrebe ovog Vodiča je predstavljeno iz razloga što jedan od kvalifikovanih oblika ovog djela čini i okolnost da je počinjeno prema djetetu ili maloljetniku. Ovo krivično djelo čini onaj:

- *(1) ko fotografski, filmski ili na drugi način snimi drugu osobu bez njezinog pristanka u njezinim prostorijama ili ko takav snimak direktno prenese trećem ili ko mu takav snimak pokaže ili mu na koji drugi način omogući da se s njim direktno upozna.*

Propisana kazna za osnovni oblik djela jeste novčana kazna ili kazna zatvora do tri godine.

Kvalifikovani oblici djela postoje u slučaju da:

- *(2) ovo krivično djelo počini službena osoba u vršenju službe s propisanom kaznom zatvora u trajanju od šest mjeseci do pet godina kao i*

- *(3) ko dijete ili maloljetnika snimi radi izrade fotografija, audio-vizualnog materijala ili drugih predmeta pornografskog sadržaja, ili posjeduje ili uvozi ili prodaje ili rasparčava ili prikazuje takav materijal, s propisanom kaznom zatvora u trajanju od jedne do pet godina.*

Konačno, u st. 4. propisano je oduzimanje predmeta koji su bili namijenjeni ili upotrijebljeni za učinjenje ovog krivičnog djela, odnosno uništenje onih predmeta koji su počinjenjem ovog djela nastali.

3.3. Brčko distrikt Bosne i Hercegovine

Rješenja koja susrećemo u Brčko distriktu BiH, a kada je u pitanju zaštita djece i maloljetnika od seksualnog zlostavljanja i iskorištavanja u potpunosti odgovaraju rješenjima u Federaciji BiH osim različite enumeracije krivičnih djela. Tako je krivično djelo „Iskorištavanja djeteta ili maloljetnika radi pornografije" propisano u čl. 208, a djelo „Upoznavanje djeteta s pornografijom" u čl. 209. KZ-a BDBiH. Krivično djelo „Neovlašteno optičko snimanje" propisano je u čl. 186. KZ-a BD BiH. Kao i u Federaciji BiH ova su djela katalogizirana u okviru Glave XIX „Krivična djela protiv spolne slobode i morala", odnosno Glave XVII „Krivična djela protiv prava i sloboda čovjeka i građanina".

3.4. Seksualno, odnosno spolno uznemiravanje

Na kraju da damo i kratak osvrt na krivična djela spolnog uznemiravanja, koja, iako nisu prvenstveno usmjerena na zaštitu djece i maloljetnika, u moderno vrijeme zauzimaju značajno mjesto u okvirima suprotstavljanja protupravnom ponašanju koje smjera povredi ili ugrožavanju spolnog integriteta pojedinca. Nerijetko, upravo je spolno uznemiravanje prva inicijalna forma nedozvoljenog ponašanja koja kasnije prerasta u najteže oblike krivičnih djela protiv spolnog integriteta, odnosno spolne slobode, kao što su silovanje i druga slična krivična djela.

Krivično djelo spolnog nasilja, uznemiravanja i seksualnog uznemiravanja u Bosni i Hercegovini propisano je Zakonom o ravnopravnosti spolova u BiH.[46] Prema čl. 29. navedenog Zakona ovo krivično djelo čini onaj:

- *ko na osnovu spola vrši nasilje, uznemiravanje ili seksualno uznemiravanje kojim se ugrozi mir, duševno zdravlje i tjelesni integritet.*

Kazna propisana za ovo krivično djelo je kazna zatvora od šest mjeseci do pet godina. Pod nasiljem na osnovu spola navedeni zakon podrazumijeva svako djelovanje kojim se nanosi ili može biti nanesena fizička, psihička, seksualna ili ekonomska šteta ili patnja, kao i prijetnja takvim djelovanjem koje sputavaju osobu ili grupu osoba da uživa u svojim ljudskim pravima i slobodama u javnoj i privatnoj sferi života. Također, nasilje po osnovu spola uključuje, ali se ne ograničava na: a) nasilje koje se dešava u porodici ili domaćinstvu; b) nasilje koje se dešava u široj zajednici; c) nasilje koje počine ili tolerišu organi vlasti i drugi ovlašteni organi i pojedinci; d) nasilje po osnovu spola u slučaju oružanih sukoba (čl. 6.). Čl. 5. Zakona sadrži definicije uznemiravanja i seksualnog uznemiravanja. Tako uznemiravanje predstavlja svako neželjeno ponašanje po osnovu spola kojim se želi povrijediti dostojanstvo osobe ili grupe osoba i stvoriti zastrašujuće, neprijateljsko, degradirajuće, ponižavajuće ili uvredljivo okruženje ili kojim se postiže takav učinak. Seksualno uznemiravanje, s druge strane, jeste svaki neželjeni oblik verbalnog, neverbalnog ili fizičkog ponašanja spolne prirode kojim se želi povrijediti dostojanstvo osobe ili grupe osoba, ili kojim se postiže takav učinak, naročito kad to ponašanje stvara zastrašujuće, neprijateljsko, degradirajuće, ponižavajuće ili uvredljivo okruženje. Od krivičnih zakona u Bosni i Hercegovini jedino KZ-a RS propisuje krivično djelo slične prirode i to u čl. 170. pod nazivom „Spolno uznemiravanje". Za razliku od onog

[46] Prečišćeni tekst – "Službeni glasnik BiH", br. 32/10

propisanog Zakonom o ravnopravnosti spolova u BiH, koje se goni po službenoj dužnosti, krivično djelo spolnog uznemiravanja iz KZ-a RS goni se po prijedlogu oštećenog i za njega je predviđena kazna zatvora u trajanju do dvije godine.

Na kraju da kažemo i to da u Bosni i Hercegovini još nema posebnog zakona koji bi ustanovio registar počinilaca krivičnih djela na štetu spolnog integriteta djece i maloljetnika odnosno njihovog seksualnog zlostavljanja i iskorištavanja. U KZ-u RS, istina, implementirane su odredbe o vođenju posebnog registra u okviru kaznene evidencije za počinioce ove vrste krivičnih djela, no nema sumnje da bi donošenje jednog takvog zakona za prostor cijele Bosne i Hercegovine i unifikacijom pravnih rješenja unaprijedilo suzbijanje ovog vida kriminala. Smatra se da iako donošenje jednog takvog zakona temeljem kojeg bi se prikupljali i čuvali podaci o počiniocima krivičnih djela seksualnog zlostavljanja i iskorištavanja djece ne bi riješilo problem seksualnog zlostavljanja djece, ipak bi doprinijelo njihovoj boljoj zaštiti, prije svega stalnim nadzorom nad osobama koje su već osuđene za ova krivična djela.[47]

4. Grooming – poglavlje prilagođeno rješenjima u Bosni i Hercegovini

Uobičajeni način izvršenja je da izvršilac nastoji najprije da dođe do „prijateljskog“ zbližavanja porukama koje će kod djeteta učvrstiti uvjerenje da komunicira s osobom koja ima razumijevanja za djetetova razmišljanja, dijeli interesovanja za iste društvene mreže i onlajn igre i sl. Poseban aspekt te problematike se vezuje upravo za djelovanje u kibernetičkom svijetu, naročito u vidu nesposobnosti djece da shvate značaj prosljeđivanja različitih informacija različitim putevima na internetu pa tako se navodi gdje rade tata ili mama, kako se roditelji zovu, koliko godina imaju, kakvo im je radno vrijeme, kada su i koliko odsutni od kuće, što može biti od koristi izvršiocu.

Potom se izvršilac okreće nenametljivom uvođenju djeteta u razgovore o intimnim stvarima, postepenom izlaganju djetetu seksualno eksplicitnih materijala. Zatim se neagresivno predlaže *screen-to-screen* ćaskanje ili komuniciranje preko web-kamere, što obično vodi dalje u dobrovoljno slanje vlastitih kompromitujućih fotografija djeteta. Konačno, izvršilac dogovara mjesto i vrijeme sastanka. Izvršioci se pri svemu tome lažno predstavljaju ili upotrebljavaju podatke drugih maloljetnih osoba kao i njihove fotografije da bi se lažno predstavili žrtvama kao vršnjaci. Dešava se da se lažni identitet upotrijebi više puta za vršenje istih ili različitih kriminalnih radnji.

Onlajn podvođenje maloljetnika je veoma frustrirajuće za mnoge optužene jer ne zahtijeva završni “akt” s maloljetnom osobom, a naime da je izvršeno neko od pobrojanih krivičnih djela. 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 s maloljetnom osobom.

Za traženje na internetu ili onlajn podvođenje maloljetnika način kontakta mora uključivati neku vrstu komunikacije elektronskim putem. Dokle god je metod elektronski i razgovor

[47] V. *Zaštita djece od seksualnog zlostavljanja i iskorištavanja: Registar počinilaca krivičnih djela seksualnog zlostavljanja djece, potrebe i obaveza* (2016). World Vision International u Bosni i Hercegovini, Banja Luka

istovremeno uključuje zahtjev za susret s djetetom kako bi se izvršilo neko od navedenih djela, onda optuženi može biti optužen za *grooming*.

Kada se sagledaju iskazi oštećenih osoba, može se vidjeti da su pretežno ženskog spola, a što se tiče posljedica, različito se izjašnjavaju. Neke žrtve navode da su imale noćne more, da se plaše da upoznaju nove ljude, da ne smiju više noću da se kreću same, zatvorile su profile i nakon dosta vremena još osjećaju sramotu jer je npr. cijela škola vidjela golišave slike ili da i dalje ima osjećaj 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 djece, što je za njih bila još dodatna frustracija.

U situaciji ne baš bogate domaće sudske prakse ukazat ćemo na neka iskustva država koje se odavno u velikom broju i već duže vrijeme suočavaju s ovim krivičnim djelom. Između ostalog, postavilo se i pitanje je li optužba neodrživa ukoliko je optuženi imao komunikaciju s pripadnikom policije koji se samo predstavljao kao dijete? U nekim slučajevima okrivljeni su se branili da su ih policajci agresivno ciljali da ih uvjere da počine krivično djelo koje oni inače nisu imali predispoziciju da počine. Namještaljka, klopka, podstrekivanje, provocirano krivično djelo je bila teza odbrana. Mnoge države u SAD su baš zato promijenile svoje zakone kako bi omogućile osudu zasnovanu na vjerovanju okrivljenog da razgovora s maloljetnom osobom. Još jedan odbrambeni ugao je pokušaj da se dokaže da optuženi nije znao da je osoba s druge strane maloljetna. Većina država ima zakone po kojima država nije dužna da dokaže da je optuženi znao koliko je dijete bilo staro, već samo da je znao da je u pitanju maloljetna osoba. Optuženi se brane i pozivanjem da su mu prekršena prava na slobodu govora, ali takva odbrana nije uspješna. Primjer sljedećeg navoda odbrane je da je razgovor bio samo onlajn fantazija ili dokazivanje da okrivljeni nikada nije ni namjeravao da zaista susretne maloljetnika. Imajući u vidu ga je izvršenje ovog krivičnog djela po našem zakonodavstvu neophodno da se izvršilac pojavi na mjestu sastanka, slučajno zaticanje na istom mjestu bi bilo teško prihvatljivo.

Posljednjih godina uočena je pojava *sekstinga* (kovanica od riječi seks i teksting) veoma zastupljena među tinejdžerima, koja podrazumijeva razmjenu tekstualnih poruka eksplicitnog sadržaja i fotografija na kojima se vide nagi dijelovi tijela i/ili seksualni čin. Poruke i fotografije se prije svega razmjenjuju između vršnjaka, s tim što jedanput poslata poruka lako stiže do onih kojima nije bila namijenjena. Visok procent adolescenata praktikuje danas seksting, a sve više se sada govori o posljedicama koje takvo ponašanje može izazvati u tinejdžerskim godinama. Greška mladog čovjeka može dovesti do odbacivanja ili ismijavanja od vršnjaka, ali i posljedica koju seksting može imati i na društveni ugled pa čak i kasniju mogućnost zaposlenja. Izlaganje fotografija i ličnih podataka može rezultovati negativnim posljedicama i onda kada nije riječ o fotografijama koje prikazuju nagost. Fotografije se mogu smjestiti u negativan kontekst, popraćene negativnim komentarima, što može pogubno utjecati na samopouzdanje djeteta.

Ovdje će se prikazati zanimljiv primjer iz američke države Ilinois, gdje osoba vrši krivično djelo dječije pornografije ako snimi ili fotografiše osobu za koju zna je mlađa od 18 godina i koja je angažovana 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 treba znati da je mlađa od 18 godina da se pojavi na takvoj slici ili na videozapisu se sancioniše kao dječija pornografija, ali i prosljeđivanje seksting poruka drugima ili širenje takvih slika drugima. Djelo vrši i osoba koja, znajući sadržaj ili prirodu, posjeduje fotografiju ili film koji prikazuje nekoga za koga treba znati da je maloljetan.

Posjedovanje se smatra voljnim, kad osoba "svjesno nabavi ili dobije" nezakoniti materijal "s dovoljno vremena da okonča posjedovanje."

Sljedeći primjer stavlja prethodno navedena djela u perspektivu: 16-godišnja djevojka koja snima seksualnu sliku sebe polugole i pošalje je kao telefonsku poruku svom dečku izvršila je najmanje tri krivična djela: stvaranje, širenje i posjedovanje dječije pornografije. Ako joj je njen dečko tražio da mu pošalje takvu poruku, on će odgovarati za najmanje dva krivična djela: navođenje i dobrovoljno posjedovanje seksting poruke. Tako jedna ne baš mudra mladalačka nesmotrenost može rezultovati u pet krivičnih djela i nekoliko tinejdžera je spreman za upisivanje u registar "seksualnih prijestupnika."[48]

5. Virtuelno zlostavljanje (Cyberbullying)

Bullying – vršnjačko nasilje je neželjeno, agresivno ponašanje među djecom školskog uzrasta koje uključuje stvarnu ili percipiranu neravnotežu moći. Cyberbullying je takvo ponašanje koje se javlja na internetu upotrebom prijetećeg ili zlog jezika u namjeri uznemiravanja ili emocionalnog povređivanja jedne osobe ili grupe ljudi, slanjem tekstualnih poruka, elektronske pošte u onlajn igricama, sobama za čatovanje, na diskusionim grupama ili web-stranicama i dr.

Ponašanje se ponavlja ili ima potencijal da se ponovi tokom vremena. Djeca koja su maltretirana, ali i ona koja maltretiraju druge mogu imati ozbiljne trajne probleme. Potreba da se drugi maltretira obično potječe iz nasilnog ponašanja negdje drugdje u životu djece koja u školama ili na drugim mjestima ponavljaju ona ponašanja koja su iskusila, vidjela ili naučila kod kuće.

Kao jedan od početnih koraka za izvršenje krivičnog djela je i krađa identiteta. Informacije od značaja za izvršioce krivičnih djela koji se bave krađom identiteta širom svijeta obuhvataju imena i prezimena, adrese, zdravstvene podatke i sve drugo što kasnije mogu zloupotrijebiti. 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 internetskog saobraćaja, ubacivanje "trojanaca" u sistem, krađa ličnih i drugih podataka korisnika i njemu bliskih osoba. Do ličnih podataka može se doći i bez korištenja 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 cyberbullynga govori se i o krađi ili pogađanju lozinke djeteta, pa se zatim ta lozinka mijenja ili se blokira, zaključava, tako da dijete više ne može pristupiti svom nalogu. Poslije krađe obično slijedi zloupotreba identiteta, koja podrazumijeva upotrebu ličnih podataka neke osobe koji su prethodno pribavljeni bez njenog znanja i odobrenja za izvršenje krivičnih djela pod njenim identitetom.

Kada se govori o nasilju preko interneta, ono između ostalog podrazumijeva:

- slanje uznemirujuće poruke e-mailom ili na čatu,
- slanje poruka neprimjerenog sadržaja,

[48] https://www.isba.org/ibj/2010/04/sextingitsnojokeitsacrime

- slanje neželjene pošte, spamova i virusa putem elektronske pošte ili na bilo koji drugi način na internetskoj mreži,
- slanje fotografija koje vrijeđaju dostojanstvo, integritet, slobodu i sigurnost,
- krađu ili promjenu lozinke za e-mail ili nadimak na čatu,
- objavljivanje privatnih podataka ili neistine na čatu, blogu ili internetskoj stranici,
- postavljanje internetske ankete o žrtvi,
- poticanje govora mržnje i mržnje uopće na internetu,
- poticanje komunikacije uvreda i nipodaštavanja,
- proslјeđivanje tuđih fotografija i traženje komentara ili bilo kakvog sadržaja o drugom sa zahtjevom za komentarisanje,
- povređivanje privatnosti upadanjem u tuđi kompjuter i čitanjem tuđih sadržaja komunikacije na internetu,
- lažno predstavljanje i upotrebu lažnog identiteta,
- proizvodnju i distribuciju dječije pornografije[49].

Osim navedenih, primjeri onlajn nasilja podrazumijevaju i slanje prijetnji, provokativnih uvreda ili rasne ili etničke uvrede, seksualno pogrdno obraćanje, dijeljenje primljenih e-mailova bez dozvole onog koji ga je napisao, zastrašivanje i prijetnje ili stvarno nasilje ili drugi oblici diskriminacije usmjereni na osobe koje su (ili za koje izvršilac smatra da su) pripadnici LGBT populacije, zatrpavanje e-mail inboxa nasilnim porukama, dijeljenje slika snimljenih u neprijatnim situacijama, bez dozvole osoba na fotografiji, uvjeravanje drugih da isključe nekog iz zajednice (*online* ili *offline*), postavljanje ili širenje lažnih informacija o osobi s ciljem da se povrijedi ta osoba ili njena reputacija, slanje u više navrata neprijatnih, zlih poruka, ruganje, spletkarenje.

Ovdje treba ukazati na to da je Protokolom postupanja u ustanovi u odgovoru na nasilje, zlostavljanje i zanemarivanje[50] navedeno da se nasilje i zlostavljanje može javiti kao fizičko, psihičko (emocionalno) i socijalno. Osim navedenih oblika, nasilje i zlostavljanje prepoznaje se i kroz: zloupotrebu, seksualno nasilje, eksploataciju djeteta i učenika, elektronsko nasilje i dr. Elektronsko nasilje i zlostavljanje je zloupotreba informacionih tehnologija koja može imati za posljedicu povredu druge ličnosti i ugrožavanje dostojanstva i ostvaruje se slanjem poruka elektronskom poštom, SMS-om, MMS-om, putem web-stranice, čatovanjem, uključivanjem u forume, socijalne mreže i sl.

Oblici psihičkog nasilja i zlostavljanja su naročito: omalovažavanje, ogovaranje, vrijeđanje, ruganje, nazivanje pogrdnim imenima, psovanje, etiketiranje, imitiranje, "prozivanje", ucjenjivanje, prijetnje, nepravedno kažnjavanje, zabrana komuniciranja, isključivanje, manipulisanje, zastrašivanje. Oblici socijalnog nasilja i zlostavljanja su naročito: dobacivanje, podsmjehivanje, isključivanje iz grupe ili zajedničkih aktivnosti, favorizovanje na osnovu

[49] http://internetbezbednost.weebly.com/10531072108910801113107 7-10851072-10801085109010771088108510771090109 1.html
[50] "Službeni glasnik RS", br. 30/2010

različitosti, širenje glasina, spletkarenje, uskraćivanje pažnje od grupe (ignorisanje), neuključivanje, neprihvatanje, manipulisanje, iskorištavanje, prijetnje, izolacija, maltretiranje grupe prema pojedincu ili grupi, organizovanje zatvorenih grupa (klanova), što za posljedicu ima povređivanje drugih. Oblici seksualnog nasilja i zlostavljanja su naročito neumjesno sa seksualnom porukom: lascivni komentari, širenje priča, etiketiranje, pokazivanje pornografskog materijala, pokazivanje intimnih dijelova tijela, 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 videozapisa, zloupotreba blogova, foruma i čatovanja, snimanje kamerom pojedinaca protiv njihove volje, snimanje nasilnih scena kamerom, distribuisanje snimaka i slika, dječija pornografija. Sve navedeno, iako se tiče prosvjete, 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 ocjene da li se u konkretnom slučaju može nesumnjivo (u)tvrditi da se radi o protivpravnom ponašanju.

Cyberbullyng se uglavnom posmatra kao situacija kada jedno dijete odabere kao cilj drugo dijete, koristeći interaktivnu tehnologiju. Vršnjačko nasilje može trajati mnogo duže nego što traje školovanje i prati žrtve svuda gdje god koriste svoje mobilne telefone ili gdje se loguju na internet, može se događati 24 sata dnevno, sedam dana u nedjelji, u bilo koje doba dana ili noći, može doći do djeteta čak i kada je samo. Poruke i slike mogu se objaviti anonimno i brzo se distribuisati širokoj publici. Može biti veoma teško, a ponekad i nemoguće pratiti izvor dok je brisanje neprimjerenih ili uznemirujućih poruka, tekstova i slika gotovo nemoguće nakon objavljivanja ili slanja.

Postoje dva načina cyberbullynga, a to su direktni napadi, tj. poruke koje su poslate djetetu direktno ili one koje su poslate preko drugih, koji im u tome trebaju pomoći, bez obzira na to jesu li oni toga svjesni. To je cyberbullyng pomoću *proxyja*, koji često obuhvati i odrasle koji su uključeni u to i samim tim je zbog toga i opasniji za više osoba.

Direktni napadi se izvršavaju putem tekstualne poruke, ponekad i hiljade tekstualnih poruka na mobilni telefon, kada djeca šalju poruke mržnje ili prijeteće poruke drugoj djeci, a da ponekad nisu da svjesni da su, iako nisu izrečene u stvarnom životu, takve poruke veoma podobne da povrede i umiju biti veoma ozbiljne. Ovi napadi mogu biti i na blogovima ili na web-stranicama. Naime, danas su djeca toliko tehnološki opismenjena da znaju kreirati internetsku stranicu specifično dizajniranu kako bi se neko vrijeđao. Dalje, djeca 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 djeca koja šalju viruse ili *spyware* i koji na taj način prosto špijuniraju svoju žrtvu. "Trojanci" također omogućuju cyberbullyng i to na taj način da kontrolišu s daljine računar žrtve ili koriste svoja umijeća kako bi se izbrisao hard disk žrtve.

Internet polling predstavlja neku vrstu ankete kojoj se postavljaju pitanja i pozivaju drugi da glasaju ko je od ponuđenih vršnjaka najdeblji, najružniji itd. Također, mogu se postaviti pitanja tipa ko je 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 ono što je najstrašnije jeste da su ih kreirala djeca ili tinejdžeri. Što se tiče *gaminga*, ogroman broj djece igra interaktivno igrice bilo na *sony playstationu*, *xbox liveu* ili računaru. Igra se često onlajn i pruža se mogućnost međusobne komunikacije putem čatovanja ili *live internet* veze s bilo kim ko

istovremeno igra. Tada ponekad djeca verbalno maltretiraju drugu djecu, koriste prijetnje ili neki ružan rječnik, a ponekad čak idu i korak dalje, isključujući ih iz igara ili šire nekakve lažne vesti o njima.

Cyberbullyng pomoću proxyja je jedan od najozbiljnijih i najopasnijih vrsta, jer vrlo često uključuje odrasle osobe. To se najčešće čini tako što se maltretiranje ustvari sprovodi preko nekoga ko obavlja "prljav posao", vrlo često bez svoje volje i bez znanja da se to čini uopće. *Warning* ili *notify words* su primjeri ovakvog cyberbullynga putem proxyja. Djeca, naime kliknu na dugme za upozorenje ili za obavještenje na svom ekranu, ili čatu ili na e-mail stranici i na taj način upozoravaju pružaoca interneta da je žrtva učinila nešto što krši njihova pravila. Pružaoci usluga su upoznati s ovom vrstom zloupotrebe, često provjeravaju da bi vidjeli da li je upozorenje zaista opravdano. Ali sve što izvršilac treba učiniti 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 pružalac internetskog servisa je ustvari jedan nedužni saučesnik u ovom procesu virtuelnog nasilja. Ponekad su ti neželjeni saučesnici i roditelji same žrtve. Ukoliko izvršilac može učiniti da izgleda kao da žrtva radi nešto pogrešno, loše i o tome obavijesti žrtvine roditelje, velika je vjerovatnoća da će roditelji kazniti žrtvu.

Vrlo često će se desiti da izvršioci zlonamjerno registruju žrtvu za "e-mailing" ili za instant poruke na pornografskim stranicama. Tada se desi da žrtva primi stotine e-mailova od takvog sajta. Osim ovoga, može biti i mnogo ozbiljnije, a to je u situacijama kada izvršioci postavljaju informacije o žrtvi u sobama za čatovanje zlostavljača djece i čak reklamišući žrtvu za seks. Onda oni prosto samo sjede i čekaju da članovi te *hate* grupe ili grupe za zlostavljače djece napadaju ili kontaktiraju žrtvu bilo onlajn, a ponekad čak i offline. Zamjenom ličnosti, odnosno predstavljajući se kao žrtva, izvršilac može načiniti značajnu štetu. Oni mogu postaviti provokativnu poruku u sobi za čatanje 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 ustvari žrtve, govoreći neke prijeteće stvari ili govor mržnje. Takođe, oni mogu izmijeniti poruku koja dolazi od žrtve, tako da zamijene uloge u tekstu, predstavljajući da je žrtva ustvari rekla ružne stvari o nekom drugom.

Cyberbullyng je situacija kada su u cijelu priču uključeni samo maloljetnici i to s obje strane, bilo kao izvršilac bilo kao žrtva ili makar treba biti inicirano od maloljetnika prema drugom maloljetniku. Izvršioci uvijek kod vršnjačkog nasilja pokušavaju uključiti što više drugih u cijelu ovu priču. Odrasli se mogu uključiti u ovu priču najčešće kada se upravo na ove sajtove za zlostavljače djece 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. Posljedice mogu biti od onih koje nisu tako ugrožavajuće, do ubistva počinjena ili do samoubistava počinjenih nakon što je neko bio uključen u cyberbullyng.

Kad je riječ o motivima izvršioca, vrlo često se radi o nekom bijesu, osveti ili prosto frustraciji. Nekada to čine radi svoje "zabave" ili zato što im je dosadno, ili imaju previše vremena i previše *gadgeta*, odnosno previše tehnoloških "igrački" koje su im dostupne. Mnogi to čine prosto radi stjecanja 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 razumijevanje. Otkucana riječ prosto ne može iskazati kakav ton bi pratio izgovorenu riječ i svakako se značajno razlikuje od informacije koju bismo dobili kada bismo čuli glas osobe koja se obraća ili vidjeli govor tijela. Treba, dakle, razmišljati i o objektivnom kriteriju dobijenih informacija prilikom procjene ili ocjene, a ne da se one baziraju samo na tome kako su se te riječi učinile žrtvi, vodeći svakako računa o uzrastu, s obzirom da ta ocjena može biti pogrešna i ponekad se teško može izbjeći da se riječi protumače izvan konteksta. Te riječi, 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 povrijeđenim osjećanjima, u ljutnji i bijesu, u frustraciji ili u osjećaju straha ili prosto osjećaju da neko prijeti.

Pregled sudske prakse

Rješenjem Vijeća za maloljetnike prema maloljetnoj osobi je izrečena mjera upozorenja sudskog ukora i to zbog krivičnog djela ugrožavanja sigurnosti iz člana 138 stav 1. Naime, maloljetna osoba je ugrozila sigurnost oštećene maloljetne osobe 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 s 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 s navedenom sadržinom. Oštećeni je u svom iskazu naveo da se uplašio za svoju ličnu sigurnost, jer su riječi "crno ti se piše" bile napisane velikim slovima, a poruku je primio s nepoznatog broja. Sud je u toku dokaznog postupka izvršio uvid u kriminilastičko-tehničku dokumentaciju, utvrdio tekst poruke, datum slanja i broj s kojeg je poslata, a potom je izvršen uvid i u listing odlaznih poruka s mobilnog telefona maloljetne. Sud je zaključio da se u radnjama maloljetne stiču svi zakonski elementi krivičnog djela iz člana 138. stav 1. nalazeći da poruka s navedenom sadržinom predstavlja ozbiljnu prijetnju s obzirom na to da je objektivno podobna da kod onoga kome se prijeti odnosno oštećenog izazove osjećaj straha ili nesigurnosti, što je oštećeni potvrdio.

Drugi primjer za isto krivično djelo je presuda kojom je okrivljeni proglašen krivim što je ugrozio sigurnost oštećenog prijetnjom da će napasti na život i tijelo te osobe na taj način što je na mreži Facebook sa svog korisničkog profila poslao oštećenom prijeteće poruke između ostalog i sadržine "Mrtav si, majmune, odrobijat ću 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".

Primjer za krivično djelo iz člana 138. stav 2. je presuda kojom je okrivljena proglašena krivom što je sa svog kućnog računara ugrozila sigurnost više osoba – dvije oštećene, prijetnjom da će napasti na njihov život i tijelo tako što je na internetskoj prezentaciji društvene mreže Facebook s korisničkog profila, koji je kreirala pod lažnim imenom, na korisnički profil maloljetne oštećene uputila prijetnje: "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 posljednja opomena, doći ću i razvalit ću je od batina".

Pred Višim sudom u Beogradu donesena je presuda kojom je prihvaćen sporazum o priznanju krivičnog djela iskorištavanja računarske mreže ili komunikacija drugim tehničkim sredstvima za izvršenje krivičnih djela protiv spolne slobode prema maloljetnoj osobi iz člana 185 b. stav 1. KZ-a u vezi s članom 184. stav 2. u vezi sa stavom KZ-a u vezi s članom 30 KZ-a i to koje je okrivljenom stavljeno na teret. Okrivljeni je proglašen krivim što je u stanju uračunljivosti svjestan svog djela da je zabranjeno, pri čemu je htio njegovo izvršenje, u namjeri da izvrši krivično djelo posredovanja u vršenju prostitucije iz člana 184. stav 2. u vezi sa stavom 1., koristeći računarsku mrežu s umišljajem pokušao da dogovori sastanak s maloljetnom oštećenom osobom starom 13 godina na taj način što je sa svog mobilnog telefona elektronskim putem koristeći svoj profil na Facebooku stupio u kontakt s oštećenom, kojoj je najprije poslao zahtjev za prijateljstvo da bi nakon što ga je oštećena prihvatila i saopćila mu da ima 14 godina, počeo da joj šalje poruke seksualne sadržine kao i poruke kojima je navodi i potiče na prostituciju : "Ćao mačkice, ajde da ti dam 500 eura mjesečno za povremeno viđanje u tajnosti", "Važi mačkice moja ..... ako budeš dobra u krevetu, onda i više ćeš da dobiješ, jesi već vodila ljubav s nekim" i slično, nakon čega je tražio broj telefona oštećene, a nakon čega je oštećena prekinula komunikaciju s njim. Osuđen je na kaznu zatvora u trajanju od jedne godine, koja će se izvršiti u kućnim uvjetima uz elektronski nadzor i izrečena je novčana kazna u iznosu od 50.000,00 dinara kao i mjera sigurnosti oduzimanja predmeta, računara, mobilnih telefona. Prema okrivljenom je na osnovu člana 89a KZ-a izrečena mjera sigurnosti zabrane približavanja i komunikacije s oštećenom i to na udaljenosti manjoj od 200 metara, stanu u kojem oštećena živi i osnovnoj školi koju pohađa maloljetna oštećena, a zatim je na osnovu člana 7. stav 1. tačka 2. i 3. Zakona o posebnim mjerama za sprečavanje vršenja krivičnih djela protiv spolne slobode prema maloljetnicima (tzv. Marijin zakon) prema okrivljenom izrečena mjera zabrane posjećivanja mjesta na kojima se okupljaju maloljetne osobe (vrtići, škole i slično) i obavezno posjećivanje profesionalnih savjetovališta i ustanova. Određeno je da će se mjere sprovoditi poslije izdržane kazne zatvora, najduže 20 godina poslije izvršene kazne zatvora, s tim što će sud po službenoj dužnosti po isteku svake četiri godine od početka primjene ovih mjera odlučiti o potrebi njihovog daljeg sprovođenja.

Primjer za 185b KZ-a je još jedan prihvaćen sporazum o priznanju krivičnog djela kojim je okrivljeni proglašen krivim što je u namjeri da izvrši obljubu nad djetetom koristeći računarsku mrežu s umišljajem pokušao da dogovori sastanak s oštećenim djetetom starim 11 godina na taj način što je sa svog mobilnog telefona elektronskim putem preko interneta na društvenoj mreži Facebook, na kojem se lažno predstavljao kao 12-godišnji dječak, stupio u kontakt s oštećenim dječakom, predstavljajući se kao dječak koji ga zna s fudbala da bi nakon toga počeo da mu šalje poruke seksualne sadržine naprimjer "Kad bi te uhvatio, oborio bi te u krevet, onda bi ti noge raširio i onda znaš", "Znaš gdje bi te jebao, stavio bi ti moju kitu i jako te udarao, dal da budem jako grub ili malo prema tebi, oćeš da ti kažem kako bi te rasturio, znaš šta volim da radim dječacima posle utakmice", da bi mu poslao poruke u kojima navodi da želi da dođe na trening određenog datuma, upozna se s maloljetnim oštećenim te da će doći u svlačionicu nakon treninga, nakon čega je oštećeni prekinuo komunikaciju s njim. Osuđen je na kaznu zatvora u trajanju od jedne godine i to u prostorijama u kojima stanuje, izrečena je mjera sigurnosti oduzimanja mobilnog telefona i SIM-kartica, a primijenjena je odredba člana 89a KZ-a izrečena mjera sigurnosti zabrana približavanja i komunikacije s oštećenim i to na udaljenosti od 200 metara, zabranjen je pristup u prostor oko mjesta stanovanja oko škole koju maloljetni pohađa i 200 metara od škole fudbala te sportske sale, zabranjeno mu je uznemiravanje oštećenog odnosno dalja komunikacija s oštećenim i ta mjera prema izreci presude može trajati najduže tri godine. Primijenjena je i odredba člana 7. stav 1.

tačka 2. i 3. Zakona o posebnim mjerama za sprečavanje vršenja krivičnih djela protiv spolne slobode prema maloljetnicima i to zabrana posjećivanja mjesta na kojima se okupljaju maloljetne obaveze i obavezno posjećivanje profesionalnih savjetovališta i ustanova.

Primjer je i presuda kojom je okrivljeni proglašen krivim zbog izvršenja krivičnog djela iz člana 185. stav 2. u vezi sa stavom 1. u vezi s članom 180. stav 1. i zbog izvršenja krivičnog djela iz člana 185. stav 4. KZ-a i to zato što je u namjeri da izvrši obljubu s djetetom, koristeći računarsku mrežu i komunikaciju drugim tehničkim sredstvom – mobilnim telefonom, s umišljajem dogovorio sastanak s maloljetnom oštećenom osobom starom 12 godina i pojavio se na dogovorenom mjestu radi sastanka, tako što je elektronskim putem, preko interneta, na društvenoj mreži Facebook, koristeći svoj korisnički profil, stupio u kontakt s oštećenom osobom, uputio joj poruku: "Lijep pozdrav za tebe, hvala ti za dodavanje... vrlo si lijepa i posebna... volio bih da se više upoznamo... ako si malo više znatiželjna, imam neke jako lijepe priče za tebe, intrigantne... posebne... vrlo si slatka... ženstvena i vrlo seksi", nakon čega je maloljetna oštećena prijavila poruku svojoj majci, koja je promijenila lozinku navedenog profila, nastavila komunicirati s okrivljenim, predstavljajući se kao dijete, 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 volio 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 12... one dvije 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 vrijeme u uvjerenju da komunicira s djetetom, nakon čega je dogovorio da se s djetetom sastane u Beogradu, pri čemu se pojavio na zakazanom sastanku kako bi se upoznao s djetetom, u namjeri da izvrši krivično djelo obljuba s djetetom iz člana 180. stav 1. KZ-a, nakon čega je lišen slobode, kao i što je posjedovao 606 slika pornografske sadržine, nastalih iskorištavanjem maloljetnih osoba, a što je pronađeno prilikom pretresa stana u kojem stanuje. Prema okrivljenom je izrečena mjera sigurnosti oduzimanja predmeta – laptopa, dvije fleš memorije, jedan mobilni telefon i primijenjena odredba člana 7. u vezi s članom 9. i 10. Zakona o posebnim mjerama za sprečavanje... i to zabrana posjećivanja mjesta na kojima se okupljaju maloljetne osobe, kao što su školske zgrade, školska dvorišta, vrtići, igrališta, dječije manifestacije i sl., kao i obavezno posjećivanje profesionalnih savjetovališta i ustanova prema programu koji će mu biti određen od organizacione jedinice Uprave za izvršenje krivičnih sankcija, nadležne za tretman i alternativne sankcije. Navedene mjere 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 postojanje komunikacije između dva profila na društvenoj mreži Facebook djeteta 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, potvrdom o privremeno oduzetim predmetima, izvještajem o prikupljanju podataka iz mobilnih telefona, vještačenjem CD-medija (pregled uređaja) kao i izvještajem MUP Direkcije policije UKP. Optuženi se branio da nije zainteresovan za djecu i djevojčice mlađeg uzrasta kao i za dječiju pornografiju, ali i da nije komunicirao s djetetom, već da je sve vrijeme znao da se dopisuje s majkom. Međutim, takva odbrana osnovana od prvostepenog suda nije prihvaćena kao vjerodostojna. Nesumnjivo je utvrđeno da je okrivljeni i ranije tokom 2013., 2014. i 2016. godine koristeći računarsku mrežu kontaktirao s maloljetnim djevojčicama drugih korisničkih profila, sadržina

tih poruka također je seksualne konotacije, što je prvostepeni sud nesumnjivo utvrdio iz vještačenja CD-medija. Na laptop-računaru koji je od okrivljenog oduzet kao i na dvije USB fleš memorije pronađeno je i oduzeto ukupno 606 fotografija s dječijom pornografijom, a posjedovanje takvog materijala okrivljeni nije sporio, a potvrdili su ga i pisani dokazi u spisima. Da je okrivljeni sve vrijeme komunikacije tokom koje je dogovorio sastanak s maloljetnom oštećenom bio uvjeren da ih šalje djetetu, da je to i htio upravo u namjeri da izvrši obljubu s djetetom, prvostepeni sud je nesumnjivo utvrdio kako iz sadržine poslatih poruka koje se u većini odnose na seksualne odnose s djecom, tako i ocjenom ostalih pisanih dokaza u spisima, ali i iskaza majke maloljetne, svjedoka koji je u svemu saglasan s materijalnim dokazima. Dalje je sud utvrdio da je okrivljeni došao na dogovoreni sastanak, da je mijenjao mjesto gdje će se naći insistirajući da to bude na autobuskoj stanici, da će on stajati u bočnoj ulici i biti u parkiranom vozilu s uključenim žmigavcima, da maloljetna dođe do kola, a u telefonskom razgovoru je i ponovio da joj je ponio mobilni telefon koji joj je prethodno obećao.

Primjer za krivično djelo prikazivanje, pribavljanje i posjedovanje pornografskog materijala i iskorištavanje maloljetne osobe za pornografiju iz člana 185. stav 3. u vezi sa stavovima 1. i 2. i stavom 4. KZ-a i krivično djelo iskorištavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih djela protiv spolne slobode prema maloljetnoj osobi iz člana 185b. stav 2. u vezi sa stavom 1. KZ-a u vezi s članom 180. stav 1. KZ-a u vezi s članom 30. KZ-a je i postupak u kojem je okrivljenom stavljeno na teret da je učinio dostupnim slike i audio-vizuelni materijal pornografske sadržine djetetu starom osam godina i u više navrata iskoristio dijete za proizvodnju slika pornografske sadržine na taj način što je preko interneta putem društvene mreže Facebook preko svog korisničkog profila stupio u kontakt s oštećenom osobom i u više navrata slao slike svog spolnog organa u erekciji i prilikom ejakulacije i videosnimak na kojem se samozadovoljava te od oštećene osobe zahtijevao da mu šalje svoje slike na kojima je ona naga i pri tom davao uputstva na koji način i koje dijelove da slika, što je ona učinila i poslala mu ukupno osam slika te je na elektronski način učinio dostupnim navedene slike pornografske sadržine nastale iskorištavanjem maloljetne osobe tako što je preko Facebooka poslao tri fotografije na kojoj je maloljetna oštećena naga korisnicima drugih profila. Osim toga, okrivljenom je dalje stavljeno na teret da je u periodu od nedjelju dana u namjeri da izvrši obljubu s djetetom koristeći računarsku mrežu Facebook s umišljajem pokušao dogovoriti sastanak s oštećenom na taj način što je uputio više poruka sljedeće sadržine "A znaš da mi je veliki, ja mislim da ti ne bi cio mogao stati, hoćemo probati jednom to, mislim da vidimo da li bi ti mogao stati, pa jedino da ti dođeš kod mene, jer bi htjela da jednu noć spavamo zajedno", ali s umišljajem započeto djelo nije dovršio jer je oštećena prekinula kontakt s njim. Predloženi su dokazi: zapisnik o pretresanju stana i drugih prostorija, potvrda o privremeno oduzetim predmetima, izvještaji službe za specijalne istražne metode o vještačenju hard diska oduzetog od okrivljenog, dio komunikacije izdvojen u fotodokumentaciji, komunikacija između okrivljenog i korisnika profila na koje je slao fotografije. Predloženo je da se izvrši uvid u sadržaj medija koji je dostavljen uz izvještaj vještačenja elektronske opreme oduzete od okrivljenog i to slika kao i videoklipa koji se nalaze u označenom folderu kao i sadržaja CD-medija dostavljenog spisima.

Sljedeći primjer je krivično djelo iz člana 185. stav 3. u vezi sa stavom 2. u sticaju s krivičnim djelom prinude iz člana 135. stav 1. i osuđujuća presuda kojom je okrivljeni proglašen krivim da je iskoristio dijete staro 13 godina za proizvodnju slika i videoklipova pornografske sadržine. Ozbiljnom prijetnjom da će fotografije oštećene na kojima se nalazi bez odjeće i videosnimak na kojem je prikazana oštećena bez gornjeg dijela odjeće postaviti na internet

prinudio je oštećenu da nešto učini na taj način što je koristeći društvenu mrežu Facebook kreirao više lažnih profila, zatim od maloljetne zahtijevao da se fotografiše i svlači pred web-kamerom koja je instalirana na njenom računaru, da prikazuje svoje gole grudi, svoj spolni organ – vaginu, pri čemu je sve to snimao i čuvao na svom računaru. Navedeni materijal je koristio da bi prijetio oštećenom djetetu 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 web-kamerom te kada je maloljetna htjela da prekine kontakt, prijetnje je ostvario postavivši navedene slike na "zid" naloga na Facebooku oštećene i potom ih poslao njenim prijateljima iz osnovne škole. Za navedena krivična djela utvrđene su mu pojedinačne kazne i to uz primjenu ublažavanja, najprije za član 185. stav 3. u vezi sa stavom 2. kazna zatvora u trajanju od deset mjeseci, a za krivično djelo prinuda iz člana 135. stav 1. kazna zatvora od tri meseca te je osuđen na jedinstvenu kaznu zatvora u trajanju od jedne godine, koja se ima izvršiti u prostorijama u kojima osuđeni stanuje. Izrečena je i mjera sigurnosti oduzimanja telefona, kućišta desktop-računara i SIM-kartica.

Primjer za krivično djelo prikazivanje, pribavljanje i posjedovanje pornografskog materijala i iskorištavanje maloljetne osobe za pornografiju iz člana 185. stav 2. u vezi s članom 33. KZ-a je i primjer presude kojom su okrivljeni proglašeni krivim što su iskoristili maloljetnog oštećenog za proizvodnju audio-vizuelnog predmeta pornografske sadržine i pornografsku predstavu tako što su ga nagovorili da ima seksualni odnos s kobilom, za koje vrijeme je jedan okrivljeni držao kobilu za uzde sprečavajući je da se udalji s lica mjesta, a drugi okrivljeni držao rep kako bi omogućio maloljetnom oštećenom da ima spolni odnos s kobilom potičući ga na to, a za to vrijeme je treći okrivljeni snimio spolni odnos telefonom i snimak postavio na Youtubeu. Za navedeno krivično djelo izrečene su im uvjetne osude.

Sljedeći primjer je primjer ukinute presude za krivično djelo iz člana 185b KZ-a kojom je okrivljeni, student, neosuđivan, proglašen krivim što je u namjeri da izvrši nedozvoljenu spolnu radnju nad maloljetnikom, koristeći računarsku mrežu i komunikaciju, putem mobilnog telefona dogovorio sastanak s oštećenom maloljetnom osobom i pojavio se na dogovorenom mjestu radi sastanka, preko interneta, elektronskim putem, na društvenoj mreži Facebook, koristeći lažni profil, lažno se predstavljao kao djevojka koja se bavi manekenstvom, stupio u kontakt s oštećenom osobom koja je imala 14 godina, uputio joj poruku da je lijepa i zgodna, pitanje "da li bi željela da se bavi fotomodelingom", da će uvijek imati šta poželi, šminku, garderobu, upitao koje je godište, a oštećena je sve ovo prijavila svom ocu, koji je s njom nastavio komunicirati s okrivljenim, da bi nakon toga okrivljeni u porukama počeo upućivati 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 fotomodel, 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 s njegovim sinom, nakon čega je tražio broj mobilnog telefona, pa pošto mu ga je ona poslala, oštećenoj je poslao poruku da će broj telefona proslijediti šefovom sinu, koji će s njom komunicirati putem mobilnog telefona, potom ju je kontaktirao, dogovorio se da se s njom sastane u restoranu, pojavio se na sastanku, rekao joj da ga sačeka da uđe u muški toalet, da će je pozvati odatle i da ga oralno zadovolji, da bi nakon ulaska u toalet pozvao telefonom oštećenu i rekao joj: "Ajde, gdje si više, čekam te". Prvostepenom presudom je proglašen krivim i osuđen na kaznu zatvora u trajanju od šest mjeseci i novčanu kaznu u iznosu od 50.000,00 dinara, oduzet mu je mobilni telefon i kućište za kompjuter i izrečena mjera u smislu člana 89a KZ-a i primijenjena odredba člana 7. stav 1. tačka 2. i 3. Zakona o posebnim mjerama za sprečavanje. Okrivljeni se u ovom postupku branio šutnjom. Nije priznao izvršenje krivičnog djela.

Navedena presuda je ukinuta, s obzirom na to da je sadržavala bitne povrede odredbi krivičnog postupka jer je izreka presude nerazumljiva i proturiječna sama sebi, a razlozi nejasni i nerazumljivi. Ovo stoga što prvostepeni sud nije opredijelio krivično djelo za koje je vezao odredbu člana 185-b KZ. Naime, odredbom člana 185. KZ-a propisano je da je izvršilac ovog krivičnog djela onaj ko u namjeri izvršenja krivičnog djela silovanje iz stava 4. (dijete), obljuba nad nemoćnom osobom, obljuba s djetetom, obljuba zloupotrebom položaja, nedozvoljene spolne radnje, podvođenje i omogućavanje vršenja spolnog odnosa, posredovanje u vršenju prostitucije, iskorištavanje maloljetne osobe za proizvodnju... i navođenje maloljetne osobe na prisustvo spolnim radnjama, iskoristi računarsku mrežu ili komunikaciju drugim tehničkim sredstvima, dogovori s maloljetnikom sastanak i pojavi se na dogovorenom mjestu radi sastanka, što znači da se u konkretnom slučaju radi o složenom krivičnom djelu, a prvostepeni sud nije odredio radnje za koje je vezao odredbu člana 185-b stav 1 KZ-a. U izreci je navedeno da je okrivljeni imao namjeru da izvrši nedozvoljenu spolnu radnju nad maloljetnikom. Dakle, iz izreke ožalbene presude proizlazi da se protivpravno postupanje okrivljenog sastoji u namjeri vršenja nedozvoljene spolne radnje nad maloljetnikom, što bi upućivalo na odredbu člana 182 stav 1 KZ-a, međutim, tom odredbom propisano je da je izvršilac krivičnog djela onaj ko pod uslovima iz citiranih članova izvrši neku drugu spolnu radnju, što dalje govori da je odredba upućuje na uvjete, a to su: da je potrebno postojanje prinude, odnosno sile ili prijetnje ili da je oštećeni nemoćna osoba ili da je u odnosu podređenosti ili zavisnosti u odnosu na okrivljenog, pa kako iz činjeničnog opisa krivičnog djela za koje je okrivljeni oglašen krivim ne proizlazi postojanje sile ili prijetnje, niti odnos podređenosti ili zavisnosti, to je izreka presude nerazumljiva i proturiječna sama sebi.

Opće mjere zaštite i iskaz djeteta u krivičnom postupku

1. Uvod

U posljednjih nekoliko decenija naročita pažnja na međunarodnom planu posvećena je uspostavljanju djelotvorne zaštite djece žrtava savremenih oblika kriminaliteta, posebno imajući u vidu neophodnost poduzimanja zakonodavnih i drugih mjera za sprečavanje svih vidova seksualne eksploatacije i seksualnog zlostavljanja djece, kao i potrebu njihove zaštite, uvažavajući da najbolji interesi djeteta i pravo djeteta da se njegovo mišljenje čuje i uzme u razmatranje predstavljaju jedan od osnovnih principa u ostvarivanju, poštovanju i zaštiti njihovih prava. Države ugovornice, svjesne obima i karaktera ovih pojava, posebno povećane međunarodne trgovine djecom, iskorištavanja djece u prostituciji i pornografiji, odnosno sve izražene zloupotrebe računarskih sistema i mreža u cilju regrutovanja djece u spomenute 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 djela na nivou materijalnog krivičnog prava, od izuzetne važnosti su i jasno definisane odredbe koje se odnose na specifičnosti procesnog položaja djece žrtava seksualne eksploatacije i seksualnog zlostavljanja.

2. Opće mjere zaštite djeteta oštećenog/svjedoka u krivičnom postupku

Zakon o ratifikaciji Fakultativnog protokola uz Konvenciju o pravima djeteta o prodaji djece, dječijoj prostituciji i dječijoj pornografiji, između ostalog, obavezuje države ugovornice da usvoje odgovarajuće mjere za zaštitu prava djeteta[51] u svim fazama krivičnog postupka (član 8. *Protokola*), a naročito:

- priznavanjem ugroženosti djece žrtava i prilagođavanjem postupaka da bi se uvažile njihove posebne potrebe, uključujući njihove posebne potrebe kao svjedoka;
- obavještavanjem djece 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 prezentuju i razmotre gledišta, potrebe i preokupacije djece žrtava, na način koji je u skladu s pravilima nacionalnog procesnog prava;

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

- osiguranjem odgovarajućih službi podrške djeci žrtvama tokom čitavog pravnog procesa;
- zaštitom, kada je to odgovarajuće, privatnosti i identiteta djece žrtava i poduzimanjem mjera u skladu s nacionalnim pravom kako bi se izbjeglo nepodesno širenje informacija koje bi mogle dovesti do identifikovanja djece žrtava;
- osiguranjem, u odgovarajućim slučajevima, sigurnosti djece žrtava, kao i sigurnosti njihovih porodica i svjedoka koji svjedoče u njihovo ime, od zastrašivanja i odmazde;
- izbjegavanjem nepotrebnog odgađanja razmatranja slučajeva i izvršavanja naloga ili uredbi o davanju obeštećenja djeci žrtvama.

Također, u smislu *Protokola*: "Države ugovornice će osigurati da neizvjesnost u pogledu stvarne starosne dobi žrtve ne spriječi pokretanje krivičnog postupka, uključujući istražne radnje usmjerene na utvrđivanje starosne dobi žrtve. Da u postupanju od sistema krivičnog pravosuđa, s djecom žrtvama nezakonitih radnji opisanih u ovom protokolu najbolji interes djeteta bude priotitet". Države ugovornice poduzet će također mjere kako bi osigurale odgovarajuću obuku, posebno pravnu i psihološku, za osobe koje rade sa žrtvama nezakonitih radnji zabranjenih prema ovom *Protokolu* i usvojiti mjere kako bi zaštitile sigurnost i integritet osoba i/ili organizacija uključenih u sprečavanje i/ili zaštitu i rehabilitaciju žrtava takvih nezakonitih radnji.

Zakon o potvrđivanju Konvencije Vijeća Evrope o zaštiti djece od seksualne eksploatacije i seksualnog zlostavljanja izuzetno detaljno reguliše opće mjere zaštite djeteta žrtve u krivičnom postupku, ali i sam način razgovora s njim. U tom smislu države ugovornice ove *konvencije* se obavezuju na poduzimanje neophodnih zakonodavnih i drugih mjera za zaštitu prava žrtava kao i njihovih posebnih potreba u ulozi svjedoka u svim fazama krivičnog postupka, a posebno:

a. upoznavajući ih, osim 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 općem toku postupaka, optužbama kao i ishodu njihovog predmeta;

b. staranjem da barem u slučajevima gdje eventualno postoji opasnost za žrtvu ili njenu porodicu oni mogu biti obaviješteni, ako je neophodno, kada je gonjena ili osuđena osoba privremeno ili konačno puštena na slobodu;

c. omogućavanjem da na način koji je u skladu s 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 se njihova prava i interesi mogu blagovremeno predočiti i uzeti u obzir;

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

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

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

Organizacija postupka, okruženje po mjeri djeteta i jezik prilagođen djetetu

Metode rada koje su koncipirane tako da budu po mjeri djeteta trebaju omogućiti djeci da se osjećaju sigurno. Ako djecu prati osoba u koju oni mogu imati povjerenja, osjećaju se sigurnije i lagodnije tokom postupka.

U zgradama u kojima se nalaze sudovi mogu, kad god je to moguće, biti određene posebne prostorije za razgovore s djecom i saslušanje djece, tako što će se uvijek voditi računa o najboljim interesima djeteta.

Pravosuđe u krivičnom postupku primjereno djetetu podrazumijeva i da djeca zaista shvate prirodu i obim odluka koje se donose kao i posljedice tih odluka.

Razgovor s djetetom

Zakon o potvrđivanju Konvencije Vijeća Evrope o zaštiti djece od seksualne eksploatacije i seksualnog zlostavljanja posebno ustanovljava i obavezu da u situacijama kada se radi o djetetu žrtvi seksualnog zlostavljanja, odnosno seksualne ekspoloatacije, države ugovornice poduzmu neophodne zakonodavne i druge mjere kojima se osigurava:

- da se razgovori s djetetom održe bez neopravdanog odgađanja po prijavljivanju činjenica nadležnim organima;
- da se razgovori s djetetom obave, kada je neophodno, u prostorijama za to projektovanim ili adaptiranim;
- da razgovore s djetetom vodi stručnjak za to osposobljen i po mogućnosti ista osoba;
- da broj razgovora bude što manji i to samo onoliko koliko je potrebno za potrebe krivičnog postupka;
- odnosno da dijete 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 s maloljetnom osobom (pogotovo mlađe starosne dobi) važno je...

1. "Spustiti se na nivo" maloljetne osobe (sjesti pored nje, ali ne suviše blizu da ne ugrozite njen prostor)
2. Započeti razgovor tako da probudite interesovanje maloljetne osobe (počnite razgovor jednostavnim pitanjima, obratite pažnju na neverbalnu komunikaciju – vodite računa i o svom neverbalnom izražavanju...)
3. Objasniti maloljetnoj osobi zašto ste tu i šta namjeravate uraditi:

- *Postavit ću ti mnogo pitanja...*
- *Ja ću ponavljati ono što si mi rekao-la, ako pogriješim, reci mi da sam pogrešno razumio-la;*
- *Ukoliko ti treba pauza, reci mi i prekinut ćemo razgovor na nekoliko minuta;*
- *Kada završim s pitanjima, ako imaš neka pitanja za mene, ja ću pokušati odgovoriti na njih...*

Također, važno je imati na umu da djeca predškolskog uzrasta imaju kapacitet pamćenja kao i odrasli, ali oni ne obraćaju uvijek pažnju na detalje koje odrasli smatraju relevantnim – problemi vezani za sugestibilnost: maloljetne osobe (pogotovo mlađeg uzrasta) manje su sugestibilne u pogledu činjenica, nego u pogledu intrepretacije tih činjenica.

Maloljetne osobe ne lažu više od odraslih (već s pet godina djeca razumiju potrebu da govore istinu, dok djeca školskog uzrasta već razumiju samu potrebu utvrđivanja činjenica).

Djeca već u uzrastu od dvije do tri godine mogu jednostavnim jezikom da opišu opaženi događaj.

S pet godina djeca su u stanju da koriste složenije rečenice.

S deset godina djeca su u stanju da opišu vrijeme, procijene trajanje, odrede sukcesiju ili broj događaja.

Mlađa djeca bolje komuniciraju neverbalno.

S mlađom djecom treba upotrebljavati jednostavni jezik i izbjegavati upotrebu zamjenica.

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

Najbolji interes djeteta predstavlja jedan od osnovnih principa u ostvarivanju, poštovanju i zaštiti prava djeteta. Obaveza države, svih relevantnih institucija, pa i suda jeste da u svim postupcima koji se tiču djeteta vode računa o njegovim najboljim interesima. Ujedno najbolji interes djeteta predstavlja pravni standard koji se cijeni prema okolnostima svakog pojedinačnog slučaja. To znači da se prilikom donošenja svake odluke moraju sagledati okolnosti svakog pojedinačnog slučaja i odluka donijeti u najboljem interesu djeteta o čijim se pravima odlučuje.

Obaveza postupanja u skladu s najboljim interesom djeteta sadržana je u članu 3. stav 1. *Konvencije o pravima djeteta*[52], u kojem je propisana obaveza svih javnih ili privatnih institucija socijalnog staranja, sudova, administrativnih organa ili zakonodavnih tijela da u svim aktivnostima koje se tiču djeteta vode računa o njegovim najboljim interesima.[53] U tačkama 8. i

[52] *Konvencija o pravima djeteta*, "Službeni list SFRJ - Međunarodni ugovori", br. 15/90.
[53] Vučković Šahović, N., Doek, J., Zermatten, J. (2012) *The Rights of the Child in International Law, Berne: Stampfli Publications Ltd.*, str. 303-309.

9. *Zakona o potvrđivanju Fakultativnog protokola uz Konvenciju o pravima djeteta o prodaji djece, dječijoj prostituciji i dječijoj pornografiji se* posebno ukazuje na to da je država dužna osigurati zaštitu najboljeg interesa djeteta žrtve u svim fazama krivičnog postupka uz prvenstveno priznavanje principa pravičnosti i nepristranosti.

Obaveza poštovanja principa najboljeg interesa djeteta sadržana je i u drugim međunarodnim dokumentima, posebno od Bosne i Hercegove ratifikovanoj *Konvenciji Vijeća Evrope o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja* i *Smjernicama* Komiteta *ministara Vijeća* Evrope o *pravosuđu po mjeri djeteta*, a u kojima je jasno ukazano na obavezu postupanja u skladu s najboljim interesom djeteta u krivičnim postupcima, na obavezu zaštite maloljetnog oštećenog (djeteta svjedoka/žrtve) u krivičnom postupku, kao i uspostavljanja sistema pravosuđa po mjeri djeteta.

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

Prilikom procjene najboljih interesa djece koja su u uključena u krivični postupak kao žrtve ili svjedoci, važno je uzeti u obzir:

a) *njihove stavove i mišljenja;*

b) *sva druga prava djeteta, kao što je pravo na dostojanstvo, slobodu i ravnopravno postupanje trebaju u svakom trenutku da se poštuju;*

c) *svi nadležni organi vlasti trebaju usvojiti 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 djeteta.*

Pravo djeteta na participaciju je jedan od osnovnih principa prava djeteta. Član 12. *Konvencije o pravima djeteta* sadrži obavezu države da osigura djetetu koje je sposobno da formira mišljenje pravo na slobodu izražavanja mišljenja o svim pitanjima koja se tiču djeteta i da posebno pruži mogućnost djetetu 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 s nacionalnim pravilima procesnog zakonodavstva. Participacija djeteta je u skladu sa shvatanjem djeteta kao subjekta prava koje aktivno participira u ostvarivanju svojih prava. Ovo pravo je usko vezano s pravom djeteta na informisanje i pravom djeteta na slobodu izražavanja, a što podrazumijeva obavezu postupajućih organa da prije izražavanja mišljenja djeteta osiguraju da dijete bude informisano o svim činjenicama koje su od značaja za donošenje odluke i to na jeziku koji je prilagođen djetetu, kao i da mu omoguće da svoje mišljenje izrazi slobodno.

Pravo je svakog djeteta da bude obaviješteno o svojim pravima, da mu se ukaže na odgovarajuće puteve koji su mu osigurani radi pristupa pravosuđu i da bude konsultovano i saslušano u postupcima u kojima učestvuje ili koji utječu na njega. Djecu treba smatrati punim nosiocima prava i tako treba postupati prema njima.

3.1. Krivičnopravni sistem i uvažavanje principa najboljeg interesa djeteta i prava na participaciju u krivičnim postupcima u Bosni i Hercegovini

Smatra se kako je pojava zloupotrebe i zanemarivanja djece egzistirala tokom čitave historije ljudskog roda, ali do priznavanja i uvažavanja ove pojave dolazi tek šezdesetih godina XX stoljeća, nakon što je američki pedijatar Henry Kempe prvi upotrijebio emocionalno nabijen termin „sindrom pretučenog djeteta" opisujući i dokumentujući drastične slučajeve fizičkog zlostavljanja djece s fatalnim ishodom.[54] Zaštita djece i maloljetnika u domenu savremenog krivičnog prava predstavlja jedan od njegovih najvećih izazova. Iako krivično pravo nije jedino pravno područje u okviru kojeg se pruža zaštita djeci i maloljetnicima kao kategoriji osoba od posebnog interesa za jedno društvo, upravo će manjkava, ali isto tako i napredna rješenja na području ove grane u najvećoj mjeri odražavati stepen ukupne zainteresovanosti društva za zdravo i slobodno odrastanje onih koji će činiti to društvo u doglednoj budućnosti. Interes djeteta, odnosno najbolji interes djeteta ustanovljen je Konvencijom o pravima djeteta UN iz 1989. godine[55] iako je zaštita djece i prije toga bila predmetom međunarodnih dokumenata kao što su Deklaracija o pravima djeteta Lige naroda iz 1924. godine[56], Deklaracija o pravima djeteta Opće skupštine UN-a iz 1959 godine[57] i drugi. Čl. 3. st. 1. Konvencije UN ustanovio je obavezu prema kojoj u svim akcijama koje u vezi s djecom poduzimaju javne ili privatne ustanove socijalne skrbi, sudovi, državna uprava ili zakonodavna tijela, prvenstveno se ima voditi računa o interesima djeteta. Kao elementi relevantni za najveći broj situacija u kojima se dijete ili grupa djece može naći, a sa stajališta procjene i utvrđivanja standarda najboljeg interesa djeteta smatraju se:

1. *Mišljenje djeteta: bez obzira na to ko i u kojoj situaciji odlučuje o pitanju koje se tiče djeteta, stav djeteta o tom pitanju je osnovni element, a u isto vrijeme i sredstvo za procjenu i utvrđivanje njegovog najboljeg interesa. U skladu s njegovim uzrastom i zrelošću, djetetu se mora uvijek dati mogućnost da utječe na određenje svog najboljeg interesa.*
2. *Identitet djeteta: svako dijete je drugačije od drugog pa se pri procjeni najboljeg interesa djeteta mora uzeti u obzir njegov identitet, odnosno karakteristike koje su uključene u njega, kao što su spol, spolna orijentacija, nacionalno porijeklo, religija, kulturni identitet.*
3. *Očuvanje porodične sredine i održavanje odnosa djeteta s roditeljima i članovima porodice: dijete se intervencijom nadležnih organa i tijela, odnosno izricanjem mjera može odvojiti od porodice samo ako se na drugi način ne može zaštititi. Onda kada se odvoji od jednog ili oba roditelja, odnosno od drugih članova porodice, mora mu se osigurati održavanje redovnih i kvalitetnih ličnih odnosa i neposrednih kontakata s njima.*
4. *Staranje, zaštita i sigurnost djeteta: djetetu se u svim situacijama i donošenjem odluke o svim pitanjima koja ga se tiču treba osigurati dobrobit, odnosno zadovoljenje osnovnih primarnih, materijalnih, obrazovnih i emotivnih potreba te potrebe za ljubavlju i sigurnošću.*
5. *Stanje ranjivosti djeteta (dijete s poteškoćama u razvoju, pripadnik nacionalne manjine, žrtva nasilja, migrant, izbjeglica itd.): najbolji interes djeteta se ne može procjenjivati na isti način za ovu i ostalu djecu, kao ni za svu djecu iz istog stanja ranjivosti.*

[54] Salkić, S. (2013). *Krivična djela nasilja and djecom: Stanje i problemi*, Sarajevo, str. 1.
[55] „Službeni list RBiH", broj: 25/93 – Međunarodni ugovori
[56] Ženevska deklaracija o pravima djeteta iz 1924. (*Geneva Declaration of the Rights of the Child*), Liga nacija O.J. Spec. Supp. 21, 43 (1924)
[57] Odluka Generalne skupštine iz 1386. (XIV) od 20. novembra 1959.

6. *Pravo djeteta na zdravlje i njegovo zdravstveno stanje: djetetu se mora pružiti bezuvjetna i adekvatna zdravstvena zaštita, koja uključuje preventivnu i medicinsku njegu, bez obzira na njegov status osiguranja.*
7. *Pravo djeteta na obrazovanje: obrazovanje je osnovno ljudsko pravo svakog djeteta koje je sadržano u brojnim međunarodnim dokumentima i zakonima u Bosni i Hercegovini. Ovo pravo je povezano s ostvarivanjem drugih prava, čime se utječe na kvalitet života svakog pojedinca.*[58]

U Bosni i Hercegovini danas, što posebno dolazi do izražaja u Federaciji BiH, kao i Distriktu Brčko BiH, krivičnopravna zaštita djece i maloljetnika, premda postoji, ipak kako smo to imali prilike konstatovati u dijelu Vodiča koji se odnosi na krivičnopravna rješenja u vezi s inkriminisanjem seksualnog zlostavljanja i iskorištavanja djece, u potpunosti ne odražava ni zahtjeve preuzete potvrđivanjem međunarodnih dokumenata, ni stvarne potrebe bosanskohercegovačkog društva za adekvatnim uređenjem ovog pravnog područja. Jedini izuzetak čine zakonodavna rješenja u Republici Srpskoj, koja u značajnom kapacitetu slijede obaveze preuzete potvrđivanjem Lanzarote ali i Istanbulske konvencije.

Pored dijela inkriminacija usmjerenih na zaštitu djece i maloljetnika kada je u pitanju visokotehnološki kriminal, krivičnopravna zaštita obuhvata i druga krivična djela iz krivičnih zakona čiji je cilj također zaštititi djecu i maloljetnike, bilo kroz zasebne inkriminacije npr. Obljuba s djetetom mlađim od 15 godina ili kroz propisivanje kvalifikovanih oblika drugih krivičnih djela ukoliko su počinjeni na štetu djece ili maloljetnika, npr. silovanje.

Osim odredbi materijalnog krivičnog prava, zaštita djece odnosno maloljetnika osigurava se i odredbama procesnog krivičnog prava. Tako zakoni o krivičnom postupku koji su na snazi u Bosni i Hercegovini propisuju posebne odredbe u okolnostima kada se u nekom procesnom statusu pojavljuje dijete, odnosno maloljetnik. Navodimo neke od njih iz ZKP FBiH uz napomenu kako slične odredbe propisuju i drugi zakoni o krivičnom postupku koji su na snazi u Bosni i Hercegovini:

- *Zdravstveni radnici, nastavnici, vaspitači, roditelji, staratelji, usvojitelji i druge osobe koje su ovlaštene ili dužne da pružaju zaštitu i pomoć maloljetnim osobama, da vrše nadzor, odgajanje i vaspitavanje maloljetnika, a koji saznaju ili ocijene da postoji sumnja da je maloljetna osoba žrtva seksualnog, fizičkog ili nekog drugog zlostavljanja, dužni su o toj sumnji odmah obavijestiti ovlaštenu službenu osobu ili tužioca (čl. 228. st. 2.).*
- *Pozivanje kao svjedoka maloljetne osobe koja nije navršila 16 godina života vrši se preko roditelja, odnosno zakonskog zastupnika, osim ako to nije moguće zbog potrebe da se hitno postupa ili drugih okolnosti (čl. 95. st. 2.).*
- *Maloljetna osoba koja s obzirom na uzrast i duševnu razvijenost nije sposobna shvatiti značaj prava da ne mora svjedočiti ne može se saslušati kao svjedok u krivičnom postupku (čl. 96. st. 1. d).*
- *Prilikom saslušanja maloljetne osobe, naročito ako je ona oštećena krivičnim djelom, postupit će se obazrivo da saslušanje ne bi štetno utjecalo na psihičko stanje maloljetnika. Saslušanje maloljetne osobe izvršit će se uz pomoć pedagoga ili druge stručne osobe (čl. 100. st. 4.)*
- *Zaštita interesa maloljetnika je jedan od razloga za isključenje javnosti s glavne rasprave (čl. 250.).*

[58] *Smjernice za procjenu i utvrđivanje najboljeg interesa djeteta: Vodič za profesionalce*, (2018). Bosna i Hercegovina, Ministarstvo za ljudska prava i izbjeglice, Sarajevo

Osim krivičnih zakona i zakona o krivičnom postupku u entitetima i Brčko distriktu BiH na snazi su i zakoni o zaštiti i postupanju s djecom i maloljetnicima u krivičnom postupku. Iako navedeni zakoni u najvećem obimu propisuju odredbe materijalnog, procesnog i izvršnog krivičnog prava u okolnostima kada se u ulozi počinioca krivičnog djela pojavljuje maloljetna osoba, jedan, istina, mali dio normi usmjeren je i na zaštitu djece i maloljetnika na čiju je štetu krivično djelo i počinjeno. Uz napomenu kako u odredbama navedenih zakona postoje stanovita odstupanja između Federacije BiH, Republike Srpske i Distrikta Brčko BiH predstavit ćemo neke od odredbi propisane Zakonom o zaštiti i postupanju s djecom i maloljetnicima u krivičnom postupku Republike Srpske, koji je i prvi zakonski propis takve prirode koji je stupio na snagu i počeo se primjenjivati u Bosni i Hercegovini.

- *Sudija za maloljetnike ili sudija koji ima posebna znanja sudi i punoljetnim počiniocima za krivična djela propisana Krivičnim zakonom kada se u krivičnom postupku kao oštećeni pojavljuje dijete i maloljetna osoba, kao što su krivična djela: a) ubistvo, b) teško ubistvo; c) ubistvo djeteta pri porođaju, d) navođenje na samoubistvo i pomaganje u samoubistvu, e) teška tjelesna ozljeda, f) otmica… (čl. 184. st. 1.).*
- *Istragu vodi tužilac koji je stekao posebna znanja iz oblasti prava djeteta i krivičnopravne zaštite maloljetnih osoba (čl. 185. st. 2.).*
- *U istražnim radnjama postupaju specijalizovana ovlaštena službene osobe koje su stekle posebna znanja iz oblasti prava djeteta i krivičnopravne zaštite maloljetnih osoba (čl. 185. st. 3.).*
- *Kod postupanja u krivičnim predmetima protiv počinilaca krivičnih djela na štetu djece, pri sprovođenju procesnih radnji posebno obazrivo se odnosi prema djetetu na čiju štetu je učinjeno krivično djelo, imajući u vidu njegov uzrast, osobine njegove ličnosti, obrazovanje i prilike u kojima živi, kako bi se izbjegle moguće štetne posljedice na njegov budući život, vaspitanje i razvoj. Saslušanje djeteta se obavlja uz pomoć stručnog savjetnika ili druge stručne osobe (čl. 186. st. 1.).*
- *Stručno lice je stručni radnik organa starateljstva - psiholog, pedagog, socijalni pedagog - defektolog, specijalni pedagog - defektolog, socijalni radnik koji posjeduje certifikat o stručnoj osposobljenosti za obavljanje poslova iz oblasti prestupništva mladih i krivičnopravne zaštite djece, iskustvo na poslovima zaštite i brige o djeci i profesionalne vještine u komunikaciji sa djecom, a uz čiju pomoć se obavlja saslušanje djeteta kao svjedoka oštećenog krivičnim djelom iz člana 184 (čl. 186a st. 1.).*
- *Ako se kao svjedok saslušava dijetem oštećeno krivičnim djelom iz člana 184. Zakona (teška krivična djela), saslušanje se može sprovesti najviše dva puta (čl. 186. st. 2.).*
- *Ako se kao svjedok saslušava dijete ili maloljetnik koji je ozbiljno fizički ili psihički traumatizovan okolnostima pod kojima je izvršeno krivično djelo ili pati od ozbiljnih psihičkih poremećaja koji ga čine posebno osjetljivim, zabranjeno je vršiti njegovo suočenje s osumnjičenim, odnosno optuženim (čl. 187).*
- *Ako prepoznavanje osumnjičenog, odnosno optuženog vrši maloljetnik oštećen krivičnim djelom ili je očevidac učinjenog krivičnog djela, takvo prepoznavanje u svim fazama postupka vrši se na način koji u potpunosti onemogućava da osumnjičeni, odnosno optuženi, vidi maloljetnu osobu (čl. 188.) i dr.*

[56] „Službene novine FBiH“, br. 36/03.

Dalje, zaštita djece i maloljetnika osigurana je i zakonima o zaštiti svjedoka pod prijetnjom i ugroženih svjedoka na svim razinama u Bosni i Hercegovini. Tako Zakon o zaštiti svjedoka pod prijetnjom i ugroženih svjedoka Federacije BiH[59] u čl. 3. st. 3. pod ugroženim svjedokom pored svjedoka koji je ozbiljno fizički ili psihički traumatizovan okolnostima pod kojima je izvršeno krivično djelo ili koji pati od ozbiljnih psihičkih poremećaja koji ga čine izuzetno osjetljivim, tretira i dijete odnosno maloljetnika sa svim procesnim učincima kojima takav status rezultira.

Konačno, poseban vid zaštite djece i maloljetnika osiguran je i nekim podzakonskim propisima u okolnostima kada se oni pojave kao žrtve trgovine ljudima. To su Pravila o zaštiti žrtava i svjedoka žrtava trgovine ljudima državljana Bosne i Hercegovine[60] te Pravilnik o zaštiti stranaca žrtava trgovine ljudima.[61] Navodimo nekoliko odredbi potonjeg dokumenta:

- *dijete koje nije državljanin Bosne i Hercegovine uživa ista prava na brigu i zaštitu kao i djeca koja su državljani Bosne i Hercegovine (čl. 20. st. 2.);*
- *ukoliko se dob stranca ne može utvrditi sa sigurnošću, a postoje razlozi za vjerovanje da se radi o djetetu, on se tretira kao dijete sve do potvrđivanja njegove starosne dobi. Prema toj osobi se poduzimaju sve posebne propisane mjere u cilju zaštite najboljeg interesa djeteta, te se obavještava mjesno nadležni općinski organ uprave za poslove socijalne zaštite u cilju osiguranja privremenog staratelja (čl. 10. st. 5);*
- *dijete koje ima odobren privremeni boravak kao žrtva trgovine pored ostalih prava kao što su: pravo na adekvatan i siguran smještaj, pristup hitnoj medicinskoj zaštiti, pravo na psihološku pomoć… ima i pristup obrazovanju (čl. 15. st. 2.);*
- *tokom provođenja postupka smještaja djeteta u sklonište nadležna organizaciona jedinica Službe obavještava organ uprave nadležan za poslove socijalne zaštite, u mjestu gdje se sklonište nalazi o potrebi imenovanja staratelja koji je u obavezi zastupati interese djeteta u postupku do nalaženja trajnog rješenja (čl. 20. st. 3.);*
- *dijete žrtva trgovine koje nije državljanin Bosne i Hercegovine ima pravo na povratak u državu porijekla ili uobičajenog boravka ili u državu koja ga prihvata (čl. 22. st. 1.);*
- *dijete žrtva trgovine neće biti vraćeno u državu porijekla ili uobičajenog boravka ili u državu koja ga prihvata ako postoji opravdana sumnja, a nakon procjene rizika i sigurnosti, da postoje razlozi da povratak djeteta ugrožava njegovu sigurnost ili sigurnost članova njegove porodice (čl. 22. st. 4.) i dr.*

Na kraju, da kažemo još i to da unatoč tome što na planu suzbijanja ove vrste kriminala u Bosni i Hercegovini postoji mnoštvo zapreka, kao što je to slučaj i s drugim oblicima kriminala, zakonodavac, ali i tijela, odnosno subjekti koji provode propise, moraju biti opredijeljeni za boljitak djece i mladih kao kategorije od posebnog interesa za društvo u cjelini. Ovo posebno na polju njihove krivičnopravne zaštite. Samo na taj način može se garantovati i zdrava budućnost Bosne i Hercegovine.

[59] „Službene novine FBiH“, br. 36/03.
[60] „Službeni glasnik BiH“, br. 66/07
[61] „Službeni glasnik BiH“, br. 90/08

Preporučena literatura

1. Bajramović, M. (2013) Pravna analiza usklađenosti nacionalnog zakonodavstva s Konvencijom o zaštiti djece od seksualnog iskorištavanja i seksualne zloupotrebe (Lanzarote konvencija). Banja Luka i Tuzla: Organizacija "Zdravo da ste" i Udruženje "Zemlja djece" Tuzla
2. Bajramović, M. (2014). Zaštita djece od seksualnog nasilja i iskorištavanja. Banja Luka: "Zdravo da ste" Banja Luka.
3. Budimlić, M. i Puharić, P. (2009) *Kompjuterski kriminalitet: kriminološki, krivičnopravni, kriminalistički i sigurnosni aspekti, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije*, Sarajevo
4. Marković, I. (2012) Usklađivanje nacionalnog zakonodavstva sa međunarodnim standardima u oblasti krivičnopravne zaštite polnog integriteta djece, objavljen u zborniku Relevantna pitanja primene međunarodnog krivičnog prava u nacionalnom pravu, Tara, jun 2012. godine, u izdanju Udruženja za međunarodno krivično pravo, str. 245-25;
5. Marković, I. (2012) Krivičnopravna zaštita polnog integriteta djece i maloljetnih lica u krivičnom zakonodavstvu Republike Srpske, Zbornik radova IX tradicionalnog međunarodnog naučnog skupa „Pravnički dani Prof. dr Slavko Carić", na temu Savremene tendencije razvoja pravnih sistema država u reogionu, Novi Sad, 2012. izdavač Pravni fakultet za privredu i pravosuđe, Univerzitet Privredna akademija, str. 450-462.;
6. Marković, I. (2010) Polno nasilje nad djetetom, Pravni život, časopis za pravnu teoriju i praksu, tematski broj Pravo i prostor, broj 10/2010. godina LIX, tom II, Beograd, s. 167-177 .
7. Marković, I. (2018) Seksualno zlostavljanje i iskorištavanje djece (novine u krivičnom zakoniku Republike Srpske) , Godišnjak Pravnog fakulteta, s. 27-45, Godišnjak časopis za pravnu teoriju i praksu, broj 40, Banja Luka
8. Muratbegović , E. Kobajica, S. i Vujović, S. (2016). Analiza u oblasti borbe protiv seksualnog nasilja i drugih oblika zlostavljanja djece na internetu u Bosni i Hercegovini, Save the Children, Sarajevo
9. Muratbegović, E. Kobajica, S. i Vujović, S. (2016). *Nasilje nad djecom putem informaciono-komunikaijskih tehnologija u Bosni i Hercegovini*, CPRC, Save the Children, Sarajevo
10. Salkić, S. *Krivična djela nasilja and djecom: Stanje i problem*, Sarajevo
11. *Smjernice za procjenu i utvrđivanje najboljeg interesa djeteta: Vodič za profesionalce*, (2018). Bosna i Hercegovina, Ministarstvo za ljudska prava i izbjeglice, Sarajevo
12. *Zaštita djece od seksualnog zlostavljanja i iskorištavanja: Registar počinilaca krivičnih djela seksualnog zlostavljanja djece, potrebe i obaveza* (2016). World Vision International u Bosni i Hercegovini, Banja Luka

13. 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.

14. Milosavljević-Đukić, I. Tankosić, B., Petković, J., Marković, M. (2017) "Jedinice za podršku deci žrtavama i svedocima u krivičnom postupku – Domaće pravo i praksa", *Temida*, br. 1, str. 45-64.

15. *Posebni protokol o postupanju pravosudnih organa u zaštiti maloljetnih lica od zlostavljanja i zanemarivanja,* 2009, Beograd: Ministarstvo pravde Republike Srbije.

16. *Posebnim protokolom o postupanju policijskih službenika u zaštiti maloljetnih lica od zlostavljanja i zanemarivanja,* 2012, Beograd: Ministarstvo unutrašnjih poslova Republike Srbije, dostupno na sjtu: www.mup.gov.rs

17. Stevanović, I.(a) (2014) „Krivičnopravni sistem i zaštita maloljetnih lica (nacionalni normativni aspekt)", u: Vučković Šahović, N. i dr. *Zaštita dece žrtava i svedoka krivičnih dela*, Beograd: International Management Group, str. 30-42.

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

19. 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.

20. 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*.

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

22. Škulić, M. (2014) "Zaštita dece/maloljetnih 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. 43-70.

23. Škulić, M. (2016) "Položaj žrtve/oštećenog u krivičnopravnom sistemu Srbije uopšte i u odnosu na Direktivu EU 2012-29", *Kaznena reakcija u Srbiji VI deo*, (ur. Đ. Ignjatović), *edicija Crimen*, Beograd: Pravni fakultet Univerziteta u Beogradu

Preporučeni internetski resursi

www.osintframework.com

Okvir OSINT je fokusiran na onlajn prikupljanje informacija od besplatnih alata i resursa na internetskoj mreži. Namjera je da se pomogne istražiocima da pronađu besplatne OSINT resurse radi identifikovanja izvršilaca i žrtvi visokotehnološkog kriminala. Neki od sajtova mogu zahtijevati registraciju ili nude više podataka za novčanu nadoknadu, ali je većina alata za onlajn istrage u kibernetičkom 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 Centra za sigurni internet koji je osnovan u svrhu prijema i obrade prijava o nelegalnim ili štetnim sadržajima na internetu.

www.GetSafeOnline.org

- Internet Safety Advice (savjeti o sigurnosti na internetu)
- Crime Prevention Advice (savjeti o sprečavanju kriminala)

www.ThinkUKnow.co.uk

- Child Protection Online Advice (savjeti o zaštiti djece onlajn)
- Public Portal to report suspected child abuse online (javni portal za prijavu sumnje na zlostavljanje djeteta onlajn)
- Crime Prevention Advice (Children & Parents) (savjeti o sprečavanju kriminala; djeca i roditelji)

www.InternetWatchFoundation.org.uk

- Public Hotline for reporting child abuse images, video"s or Text observed online (for anywhere in the world). (javna telefonska linija za prijavu slika, videa ili tekstova zlostavljanje djeteta onlajn – za bilo gdje u svijetu)

www.ActionFraud.org.uk

- Public Hotline for reporting fraud (javna telefonska linija za prijavu prevare)

- Support and advice about fraud (podrška za savjete o prevari)
- Crime Prevention Advice (savjeti za sprečavanje kriminala)

www.APWG.org

- Anti-Phishing Working Group (radna grupa za sprečavanje lažnog predstavljanja)
- Public Hotline for reporting phishing emails and websites (javna telefonska linija za prijavu e-mailova i web-stranica lažnog predstavljanja)
- Crime Prevention Advice (savjeti o sprečavanju kriminala)

www.ic3.gov

IC3 je sajt za onlajn prijave internetskog kriminala koji za posljedicu prevare ima materijalnu štetu. U zahtjevu je potrebno da pružite sljedeće informacije prilikom podnošenja prijave:

- ime oštećenog, adresu, telefon i e-mail,
- informacije o finansijskim transakcijama (npr. informacije o nalogu, datum transakcije i iznos, i dr.),
- ime subjekta kojem je doznačen novac, adresu, telefon, e-mail, web, i IP-adresu,
- detalje o tome kako ste bili žrtva prevare,
- e-mail zaglavlja (i),
- sve druge relevantne informacije koje smatrate važnim.

Save the Children za sjeverozapadni Balkan
Ljubljanska 16, Sarajevo, Bosna i Hercegovina

Tel +387 (0) 33 290 671, Fax +387 (0) 33 290 675 |
info.nwbalkans@savethechildren.org

https://nwb.savethechildren.net

savethechildrennwb

savethechildrennwb

scnwb

SavethechildrenNWB

Zajedno možemo učiniti više. Šta misliš o našem radu?
reci-nam@savethechildren.org