VISOKOTEHNOLOŠKI KRIMINAL

PRAKTIČNI VODIČ KROZ SAVREMENO KRIVIČNO PRAVO I PRIMJERE IZ PRAKSE

CENTAR ZA EDUKACIJU NOSILACA PRAVOSUDNE FUNKCIJE CRNE GORE

OSCE
Organization for Security and Co-operation in Europe
Mission to Montenegro

VISOKOTEHNOLOŠKI KRIMINAL

PRAKTIČNI VODIČ KROZ SAVREMENO KRIVIČNO PRAVO I PRIMJERE IZ PRAKSE

Podgorica, mart 2014. godine

Izdavač

OEBS MISIJA U CRNOJ GORI

Autori

Branko Stamenković

Doc. dr. Adis Balota

Valentina Pavličić

Bojana Paunović

Jakša Backović

Tiraž

500 primjeraka

Priprema

Miloš Otašević

Štampa

Artgrafika Podgorica

CIP - Katalogizacija u publikaciji
Centralna narodna biblioteka Crne Gore, Cetinje
ISBN 978-9940-500-15-3
COBISS.CG-ID 24604176

9 789940 500153

This publication was made possible thanks to funding from the United States Embassy in Podgorica - Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL).

Izrada ove publikacije omogućena je uz podršku Američke Ambasade u Podgorici - Biroa Stejt Dipartmenta za borbu protiv međunarodne trgovine drogom i sprovođenje zakona (INL).

SADRŽAJ

Poštovani čitaoci,

drage kolege,

U nedjeljama kada je sudbina leta malezijske avio-kompanije MH 370 još uvijek neizvjesna, mada uz rastuću bojazan da ishod sveobuhvatnih potraga nad nekoliko okeana i mora neće biti pozitivan, pitanja o mogućnostima i moći zloupotrebe računara i računarskih mreža, kao i uredjaja koji su povezani ili zavisni od istih, prosto sama naviru i upućuju na razmišljanja o istinskim razmjerama i posljedicama post-informatičkog društva i njegovih tehnologija.

Komentari odredjenih stručnih krugova da je sasvim moguć scenario u kome je neko, bio to pojedinac ili grupa, putem računara ili „pametnog" telefona velike procesorske moći, uspio da neovlašćeno pristupi sistemima navigacije i upravljanja letom MH 370, i da svojim radnjama utiče na njegov let, posadu i putnike, čak i ako se zaista graniči sa djelima najboljih pisaca naučne fantastike, nije nezamisliv i nemoguć.

Iako su računarski sistemi u savremenim avionima povezani u tzv. „trostruke bajpasove" tj., pratkično tri nezavisna računarska sistema u svakom momentu mogu da reaguju u avionu na zadatu komandu, postavlja se pitanje da li je i ovako visoko sofisticiranim i zatvorenim računarskim sistemima moguće pristupiti neovlašćeno, promijeniti njihov način funkcionisanja i time proizvesti odredjenu posljedicu u korist onoga ko ima namjeru da utiče ili postigne odredjenu namjeru ovim činom. Svakako, ta posljedica nikako ne mora da bude u skladu sa isčekivanjima svih drugih. Na žalost, može biti sasvim pogubna.

I u scenariju koji bi mogao biti sasvim običan, na žalost, opet sa negitivnim ishodom, računari i njihove periferije, bili to avionski transponderi i komunikacioni sistemi, mjerači brzine, zemaljski radari kako civilni tako i vojni, satelitski računari, brodski i podmorničarski sonari i sa njima povezani računari, kao i druga avionska, brodska i zemaljska računarska oprema, je takodje ili zakazala ili nije bila na visini zadatka.

Dakle, sa jedne strane postojanje mogućnosti da se računarskim putem utiče na nešto tako bitno kao što je avionski let ili centrala za proizvonju električne energije, nuklearna elektrana, sistem gradskog vodosnabdijevanja ili na neki drugi sličan strateški resurs ili infrastrukturu, a sa druge strane mogućnost nesavršenosti te opreme ili, još pogubnije, nedovoljna obučenost zaduženih ljudskih resursa da sa takvom tehnologijom upravljaju, radja osnovanu bojazan da je mogućnost ozbiljne zloupotrebe informacionih tehnologija ne samo moguća, već prisutna i narastajuća.

S tim u vezi, jasno je da organi otkrivanja, gonjenja, tj. pripadnici policije i ovlašćenih državnih službi za borbu protiv kriminala, nosioci državno-tužilačkih funkcija i njihovi saradnici, kao i sudovi i sudije današnjice, moraju biti svjesni da informatički kriminal nije nešto što će se desiti za generaciju ili dve, ili da je

informatički kriminal nešto što je rijetka pojava koju mogu da prate samo posebno zainteresovani i obučeni pripadnici navedenih organa.

Naprotiv, informatički kriminal je kriminal današnjice i njegov obuhvat nije lokalan već globalan.

Imajući navedeno u vidu, Misija OEBS u Crnog Gori, ambasada Sjedinjenih Američkih Država i Centar za edukaciju nosilaca pravosudne funkcije Crne Gore su pravilno prepoznali potrebu, da se za što veći broj državnih tužilaca i sudija, ali i pripadnika kriminalističkih službi policije, izradi jedan kratak vodič kroz osnove savremenog krivičnog prava i krivično-pravnu praksu visokotehnološkog kriminala.

Pred Vama se nalazi plod rada više policijskih, tužilačkih i sudskih stručnjaka, uz podršku članova nadležnih sektorskih ministarstava, čiji je cilj bio izrada prve knjige u mogućoj ediciji stručnih naslova na temu visokotehnološkog i računarskog kriminala, u kojoj će, na jedan prilagodjen i prijemčiv način, biti izloženi osnovi medjunarodnog i domaćeg krivičnopravnog okvira, kako materijlnog tako i procesnog i organizacionog, uz primjere iz prakse policije, državnih tužilaštava i sudova, koji trebaju da posluže kao pomoćni alat u radu ovih organa prilikom postupanja u predmetima iz oblasti takozvanog „cyber" kriminala.

Nadamo se da ćete sadržinu ovog Vodiča naći korisnom i da će Vam isti uspjeti da u odredjenim momentima nedoumica korisno ukaže na puteve kojima su neke Vaše kolege već išle i postupale, te da ćete na osnovu njihovih iskustava, kako pozitivnih, ali i negativnih, biti u mogućnosti da zauzmete stav i donesete odluku koja će biti pravilna i zakonski zasnovana prilikom postupanja u ovoj krivično-pravnoj oblasti koja može nositi razne epitete, ali one koji označavaju lakoću ili manju važnost, nikako.

S poštovanjem,

Posebni tužilac za visokotehnološki kriminal
Branko Stamenković i grupa autora

I UVOD

1.1. Informatička revolucija

Informatička revolucija donijela je 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. Sa druge strane, ovakav eksplozivan razvoj je neumitno proizveo i određene prateće posljedice negativnog karaktera. Neprestane su naučne i strukovne rasprave da li kriminalitet u oblasti informacionih tehnologija predstavlja samo logičan nastavak svakodnevnog kriminaliteta sa kojim se susreće svaka ljudska zajednica, ili samo jedan od oblika tog istog kriminaliteta ili pak potpuno nov i poseban oblik kriminogenog ponašanja koji zahtijeva posebno definisanje i tretiranje.

Ono što je *differentia specifica* kompjuterskog kriminala u odnosu na dobro poznate i proučene forme kriminala jesu činjenice da je potrebno relativno kratko vrijeme za sticanje znanja neophodnog za izvršavanje krivičnih djela iz ove oblasti, potrebni su mali materijalni i ljudski resursi u odnosu na štetu ili protivpravnu dobit koja se može ostvariti i bez fizičkog prisustva na mjestu izvršenja djela; zatim, nije uvijek jasno da li se radi o krivičnom djelu ili ne, zahvaljujući nedostacima pravnog sistema, i, konačno, teško se otkriva i još teže dokazuje.

Svi klasični elementi su primjenjivi i na krivična djela i njihove počinioce koji za medijum koriste Internet. Počinioci, izdajući specifične naredbe na kompjuterskim sistemima, čine određena krivična djela, što ispunjava zahtjev da krivično djelo mora biti djelo čovjeka. Dakle, kompjuteri i Internet su samo oruđe u rukama umješnog kriminalca.

Društvena opasnost se ogleda kako u najmanjim štetama kod lica koja u udobnosti svojih domova koriste Internet, tako i u sprječavanju protoka informacija na Nacionalnoj Internet okosnici koja je u toku izvršenja jednog krivičnog djela bila van upotrebe određeni broj dana, što je prouzrokovalo znatnu direktnu i indirektnu štetu. Protivpravnost i određenost u zakonu su predmet diskusije mnogih foruma, no primjeri koji nam dolaze iz tužilačke i sudske prakse pokazuju da se i primjenom postojećih pravnih normi mogu postići određeni rezultati u cilju specijalne i generalne krivičnopravne prevencije. I pored toga, neophodno je aktivno praćenje razvoja računarskog kriminaliteta radi pravilnog i pravovremenog odgovora države

kroz donošenje zakonskih i podzakonskih akata koji će na konkretan način sankcionisati ispoljeno društveno-opasno ponašanje.

Na kraju, vinost počinioca ovih krivičnih djela se može posmatrati, na osnovu dosadašnjih iskustava, kroz direktni i eventualni umišljaj, s obzirom da je za izvršenje ovakvih krivičnih djela potrebno specifično znanje visokog stepena koje se u datim okolnostima svjesno upotrebljava u cilju postizanja određenog protivpravnog cilja.

Efikasna prevencija, otkrivanje i pokretanje postupaka protiv izvršilaca krivičnih djela dodatno je otežana njegovim transnacionalnim karakterom. Pojavom Interneta, kao Globalne kompjuterske komunikacione mreže, i njegovog snažnog uticaja na razvoj modernog društva, pojavila se i nova kasta kriminalaca – hakeri. Hakeri, kao izvršioci krivičnih djela koje za svoj subjekat i objekat imaju Internet okruženje, primjenjujući svoje stečeno znanje koje je po pravilu znatno iznad znanja kojeg imaju organi otkrivanja i gonjenja, potpuno su svjesni ovakvog stanja stvari.

Internet kriminalitet možemo definisati na sljedeći način: *"Internet kriminalitet predstavlja izvršenje krivičnih djela koje za svoj subjekat i objekat imaju Internet kao Globalnu računarsku mrežu i koja čine informatički obučena lica u cilju izazivanja štetnih posljedica ili pribavljanja protivpravne imovinske koristi."*

Demokratske i ekonomski razvijene zemlje ulažu ogromna sredstva u pravcu suzbijanja Internet kriminaliteta. Činjenica je da su zemlje članice Evropske Unije, kao i Sjedinjene Američke Države preduzele korake da se, prije svega na tehničkom nivou, a zatim i na pravnom polju, suprotstave kompjuterskom kriminalu. Ono što mora biti nesporno u zemljama u tranziciji, jeste da bez stvaranja bezbjednog cyber prostora neće biti ni značajnijih ulaganja stranih kompanija, niti će biti moguće ostvariti efikasnu saradnju između zemalja regiona. Naravno, ove zemlje i onako imaju veliki broj problema, a premalo finansijskih i ljudskih resursa da bi se koncentrisale isključivo ili pretežno na stvaranje odbrambenog sistema protiv kompjuterskog kriminala; takođe je činjenica da u tim zemljama veoma mali broj građana uopšte ima pristup kompjuteru. Ovo, međutim, ne znači da kompjuterski kriminal ne predstavlja nešto što bi moglo u bliskoj budućnosti u značajnijoj mjeri ugroziti društvo; stoga se ovom problemu mora posvetiti dužna pažnja.

Osnovne karakteristike kompjuterskog kriminaliteta su da sam kompjuter može biti objekt napada - i to obje osnovne komponente kompjutera – hardver i softver. Oštećenje, uništenje ili zloupotreba te dvije komponente ostvaruje se pomoću dva osnovna sredstva, a to su posebno stvoreni računarski programi za zloupotrebu drugih računara, računarskih sistema i programa, kao i posebno napravljeni uređaji sa istom svrhom. Posebno opasni i štetni mogu biti računarski programi, tzv."malware" raznih pojavnih oblika, koji pošiljaocu omogućava da pristupi "zaraženom"

kompjuteru i tako stekne pristup i kontrolu nad podacima u kompjuteru, te tako i mogućnost korišćenja tog kompjutera po svojoj volji, po pravilu i bez znanja vlasnika samog računara.

Kompjuter kao subjekat napada, tj. kao sredstvo izvršenja krivičnog djela, kojim se omogućava ili pak olakšava realizacija određene kriminalne aktivnosti. Kompjuter se takođe može korisititi i kao sredstvo za planiranje, prikrivanje ili rukovođenje određenom kriminalnom aktivnošću. Ova karakteristika je od posebnog značaja, jer će ona u budućnosti upravo predstavljati tačku povezivanja organizovanog kriminala i kompjuterskog kriminala, kakav danas postoji.

Određena kriminalna aktivnost se može ostvariti i bez korišćenja kompjuterske tehnologije, ali joj ta tehnologija omogućava obradu izuzetno velikog broja informacija u kratkom vremenskom periodu, bolju povezanost i efikasnije rukovođenje, kao i komplikovanije identifikovanje i dokazivanje određenih radnji kao kriminalnih.

Profil kompjuterskog kriminalca - ukoliko se ranije moglo reći da se u najvećem broju slučajeva radi o mladim osobama, prosječne starosti dvadesetpet godina, koji u najvećem broju slučajeva nijesu ranije dolazili u sukob sa zakonom, danas to više nije pravilo. Naime, starosna granica izvršioca ovih krivičnih djela je značajno istovremeno i spuštena i podignuta, tako da je potpuno uobičajeno vođenje postupaka protiv izvršioca od najmlađih do najstarijih.

U pogledu formalnog obrazovanja ne postoji pravilo, obzirom da se znanje za rukovanje kompjuterom relativno lako stiče i bez pohađanja određenih škola ili fakulteta; u pogledu ličnih osobina, radi se o inteligentnim osobama, potpuno otvorenim za praćenje tehnološkog napretka, dok su na intimnom planu vrlo često neostvareni i kompjuter za njih predstavlja centar njihovog života.

Tamna brojka kompjuterskog kriminaliteta - broj neotkrivenih krivičnih djela iz oblasti kompjuterskog kriminala po svemu sudeći je izuzetno visok. Razloge za to treba prije svega tražiti u nedovoljnoj tehničkoj i kadrovskoj opremljenosti organa krivičnog gonjenja u regionu, neujednačenoj zakonskoj regulativi koja se bavi ovim problemom, te još uvijek široko rasprostranjenom shvatanju među građanima da je kompjuterski kriminal marginalna i bezopasna pojava.

1.1.1. Klasifikacija računarskog kriminala

Prema preporuci Savjeta Evrope o računarskom kriminalitetu No. R(89)9, kasnije konkretizovanoj u Konvenciji o kompjuterskom kriminalu, kao krivična djela navode se: kompjuterska prevara, kompjuterski falsifikat, kompjuterska sabotaža, neautorizovani pristup, neautorizovano unošenje,

neautorizovano reprodukovanje zaštićenog kompjuterskog programa i neautorizovano reprodukovanje zaštićene topografije, uz opcionu listu, u kojoj se navodi promjena kompjuterskih podataka ili kompjuterskih programa, kompjuterska špijunaža, neautorizovano korišćenje kompjutera i neautorizovano korišćenje zaštićenih kompjuterskih programa i topografije.

Međunarodni pravni izvori - od posebnog značaja za oblast računarskog kriminala su Konvencija UN protiv transnacionalnog organizovanog kriminala sa dopunskim protokolima, Palermo, 2000., kao i Konvencija Savjeta Evrope o kompjuterskom kriminalu (Cybercrime), usvojena u Budimpešti, 23. novembra 2001. godine. Palermo Konvencija predstavlja značajan napredak u globalnom određenju – definisanju transnacionalnog organizovanog kriminala i utvrđivanju promjena koje države treba da sprovedu u okviru svog krivičnog zakonodavstva, da bi suprostavljanje organizovanom kriminalu bilo efikasnije. Njeno donošenje posljedica je, prije svega, opšteg povezivanja država i regiona na ekonomsko–finansijskom planu, čime je organizovani kriminal dobio mnogo širi prostor za djelovanje.

Od naročitog značaja za vezu transnacionalnog organizovanog kriminala i kompjuterskog kriminala, kao i za suzbijanje te veze jeste čl.6 Konvencije (kriminalizacija pranja dobiti stečene kroz kriminal); imajući u vidu mogućnosti kompjuterske tehnologije, lako je zamisliti potencijalnu "korist" koja se može ostvariti angažovanjem lica osposobljenih za rukovanje kompjuterskim hardverom i softverom. Dalje, članom 7 (mjere za borbu protiv pranja novca), predviđena je obaveza država potpisnica da oforme sveobuhvatni nacionalni regulatorni i nadzorni režim za finansijske institucije i ostale organe, koji su posebno podložni pranju novca, te da se obezbijedi organima koji se bave borbom protiv pranja novca, mogućnost da sarađuju i razmjenjuju informacije na nacionalnom i međunarodnom nivou.

Navedeno je moguće ostvariti samo u slučaju podizanja nivoa tehničke i kadrovske opremljenosti na nivo koji u ovom trenutku postoji u razvijenim zemljama i formiranjem strategije i centara na nacionalnom nivou, koji bi koristeći kompjutersku tehnologiju ostvarivali obaveze predviđene ovim članom. Uzajamna pravna pomoć, koja je od posebnog značaja zbog specificnih karakteristika kompjuterskog kriminala, utrđena je članom 18 Konvencije; tačkom 13 države se obavezuju da imenuju centralni organ koji ima odgovornost i ovlašćenje da prima zahtjeve za uzajamnu pravnu pomoć i da ih ili izvršava ili prenosi nadležnim organima radi izvršenja. Zbog prirode kompjuterskog kriminala (prije svega kritični faktor vrijeme), takav organ bi morao imati ovlašćenje da izvršava zahtjeve za uzajamnu pravnu pomoć.

Cyber kriminalitet nije pojam vezan samo za uskostručnu javnost i izvršenje krivičnih djela. Svakim danom sve je više krivičnih prijava protiv nepoznatih izvršilaca krivičnih djela koja su na neki način vezana za Internet. Pri takvom stanju stvari, kada Internet kriminalci imaju znanje, sposobnosti i

opremu, ponekad savremeniju od organa koji bi trebalo da ih gone i kažnjavaju, perspektiva može biti zaista zabrinjavajuća.

Sigurno je da takvo stanje ne može potrajati dugo i da se odlučni koraci moraju preduzeti koliko sjutra. U regionu Zapadnog Balkana danas postoji jako jezgro odličnih poznavalaca Interneta i računara, pretežno među mlađom populacijom. Dio tog jezgra posjeduje takvo znanje koje se može mjeriti sa najvišim svjetskim dostignućima.

Obzirom da im se vrlo malo toga nalazi na putu, postoji velika vjerovatnoća da će postati svjesni mogućnosti da bez pretjerano velikog rizika krenu putem pribavljanja protivpravne imovinske koristi vršenjem krivičnih djela putem računara i računarskih sistema. Nije teško zamisliti pripadnike tog jezgra kako za dobre honorare nanose štetu konkurentskim firmama na tržištima u zemljama regiona. Praktično, svi sistemi koji budu priključeni na Internet neće biti do kraja sigurni. Širenjem Internet korisničke baze u regionu, pored tvrdokornih veterana, javiće se i nova klasa Internet kriminalaca, koji možda neće imati takvo znanje, ali će u svakom slučaju barem jednom doći u iskušenje da učine neko krivično djelo. Tvrdo hakersko jezgro će nastaviti svoje akcije više uperene u pravcu pribavljanja imovinske koristi kroz razne osnove.

Rast populacije Internet korisnika će dovesti do talasa izvršenja sitnih krivičnih djela putem Interneta; elektronska trgovina i industrijska špijunaža i sabotaža u zemljama regiona će predstavljati najinteresantiju oblast za Internet i računarski kriminal; preduzeća koja se bave pružanjem Internet usluga će i dalje trpjeti znatne štete zbog nesakcionisanih DoS napada; policija neće uspjeti na pravi način da se izbori sa novom vrstom kriminaliteta; tužilaštva neće uspijevati da uspješno vode postupke protiv kriminalaca iz ove oblasti; sudovi će zbog nedostatka dokaznog materijala donositi oslobađajuće presude.

1.1.2. Ovako optimistično viđenje budućnosti ove vrste kriminaliteta po njegove izvršioce, a sumorne za sve ostale, bazirano je na pretpostavci da će zakonska regulativa ostati ista i da će izostati postupak edukacije pripadnika policije, tužilaca i sudija, te organizacione promjene u navedenim organima. Da bi se to spriječilo, pored preduzimanja koraka neophodnih za borbu protiv Internet kriminaliteta, neophodno je da naše društvo posveti mnogo više pažnje, na pravi način, dobu u kome živimo kroz prihvatanje činjenice da je to doba informacija i informacionih tehnologija.

Informatička revolucija i sa njom Internet revolucija, već su među nama. Nijesu u pitanju tehnologije budućnosti, već tehnologije sadašnjosti. Samo ako na ovaj način pristupimo problemu ove vrste kriminaliteta onda ćemo zaista imati šansu da postignemo uspjeh u suzbijanju istog i na najbolji mogući način promovišemo društvo koje je moderno i zasnovano na teme-

ljima vladavine prava. U tom svijetlu treba posmatrati i Internet kriminalitet u našoj zemlji. Do juče, Internet kriminalitet nebitan i tolerisan, danas prima svoje prve značajne udarce. Obzirom da se proklamovani osnov politike nove vlasti zasniva na ekonomskom prosperitetu i zaštiti tih interesa, vrlo brzo će potencijali elektronske trgovine i poslovanja postati jedna od značajnijih privrednih grana naše zemlje.

Ako znamo da je samo u prošloj godini obrt neto profita u svijetu putem e-commerc-a iznosio nekoliko stotina milijardi dolara, onda sa pravom možemo očekivati da i u ovoj novoj privrednoj grani dio kolača pripadne i nama. No, da bi smo tako nešto zaista i dočekali, neophodno je postići osnovni uslov poslovanja, a to je sigurnost investicija i zarade. Da bi takav zahtjev bio ispunjen, moramo prilagoditi naše zakonodavstvo modernim tokovima. Naravno, nakon modernizacije zakonodavstva, moramo imati i obrazovane ljudske resurse koji će umjeti na pravi način da primijene nove trendove. Internet kriminalitet sa svojim destruktivnim dejstvom nalazi se na putu ovakvoj ideji. Zbog toga, iako potpuno moderan i za naše shvatanje možda ekstravagantan, Cyber crime predstavlja zlo, sa kojim se moramo obračunati.

1. 2. Crna Gora

1.2.1. Danas je Sajber prostor prepoznat kao realno okruženje sa najbržim rastom stepena kriminala.

Sajber kriminal, sa trenutno poznatim njegovim oblicima pojavljivanja, predstavlja globalni problem kako za razvijene države, tako i za srednje razvijene i nerazvijene države. Danas ne postoji ni jedan vid organizovane kriminalne aktivnosti a koji u nekoj formi ili fazi njegove realizacije ne koristi sajber prostor, kao što su: šverc droge, pranje novca, organizovani kriminal i korupcija, šverc oružja, finasijske prevare, dječija pornografija i dr.

Da bi se uspješno borili sa kriminalom iz ove oblasti, potrebno je razviti kapacitete, kako za prevenciju i istraživanje, tako i za fazu dokazivanja.

Samo kontinuiranom edukacijom kadrova, kao i jasnom podjelom aktivnosti između institucija sistema, moguće je pratiti na andekvatan način ovu problematiku.

Ovaj vodič treba da pruži osnovne informacije za sudije i tužioce. Vodič predstavlja samo preteču jasno definisanim serijalom edukativnih skupova koji moraju da uslijede u narednom periodu.

Jasnim sagledavanjem ove problematike od što većeg kruga zaposlenih iz sudske i izvršne vlasti, moguće je definisati i pristup budućim promjenama zakonodavnog okvira, a sve u cilju pravovremene reakcije.

1.2.2. Internet, kao i informaciono komunikacione tehnologije na kojima je baziran, predstavljaju vitalni resurs za socio-ekonomski rast i razvoj jedne države. Kako se sve više usluga nudi putem interneta, sve je veći broj prijavljenih sajber bezbjednosnih incidenata, od napada poznatih kao distribuirani napadi uskraćivanja usluga – DDoS napadi, pa do napada na *web* sajtove sa ciljem neovlašćene izmjene njihovog sadržaja. Poseban vid opasnosti predstavlja i neautorizovan pristup razvijenim informacionim sistemima državnih organa, kao i njihovim bazama podataka. Internet servis provajderi (ISP) takođe trpe sajber napade na njihovoj infrastrukturi, ali ne postoji koordinisan odgovor koji bi se odvijao bezbjednim komunikacionim kanalima na nacionalnom nivou u cilju rješavanja ovakvih situacija.

Koordinisana izgradnja organizacionih, insitucionalnih i upravljačkih kapaciteta, unapređenje zakonskih i podzakonskih propisa bitne su stavke postojanja informacione bezbjednosti u Crnoj Gori.

U sajber prostoru, današnjicu obilježavaju i *"zlonamjerni programi u službi država"*, i u narednom periodu predstavljaće jednu od glavnih opasnosti po nacionalnu bezbjednost jedne države.

Gore navedeno govori u prilog činjenici da su Internet i sa njim povezane globalne mreže značajno uvećali svjetsku zavisnost od ICT i ujedno povećali nivo potencijalne štete koju je moguće prouzrokovati kada je infrastruktura pod napadom.

Analizom strategija sajber bezbjednosti velikog broja država utvrđeno je da ne postoji usaglašena definicija pojmova kao što su: *informaciona bezbjednost*, *sajber prostor*, *sajber bezbjednost*, *sajber kriminal* i sl.

Dok neke strategije definišu pomenute pojmove precizno i konkretno, npr. usko vezujući ih za računare i računarske sisteme, druge imaju opštiji pristup i definicije sadrže ne samo stvari koje se odnose na računare i računarske sisteme, već i na bilo koji drugi faktor koji može doći u interakciju sa njima, kao npr. ljudski faktor. U ovom dijelu Priručnika, biće prikazane definicije određenih termina, koje su zastupljene u Crnoj Gori, a koje su takođe usaglašene sa osnovnim značenjima termina u zemljama EU.

Definicije osnovnih pojmova, koje navodimo u nastavku teksta, su navedene u okviru važeće Strategije o sajber bezbjednosti Crne Gore 2013-2017.

1.2.3. „Sajber" se definiše kao: „sve što se odnosi na, ili uključuje, računare ili računarske mreže (kao što je Internet)". **Sajber prostor** je više nego Internet, uključuje ne samo hardver, softver i informacione sisteme, već i ljude, društvenu interakciju u okviru ovih mreža. Međunarodna unija za telekomunikacije (ITU) koristi termin da opiše „sisteme i servise povezane bilo direktno ili indirektno na Internet, telekomunikacione sisteme ili kompjuterske mreže". Međunarodna organizacija za standardizaciju (ISO) koristi nešto drugačiji termin pri definisanju, te „sajber" vidi kao „kompleksno

okruženje koje rezultira iz interakcije ljudi, softvera i servisa na internetu i to posredstvom tehnoloških uređaja i mreža sa njima povezanim koji ne postoji u bilo kom fizičkom obliku.“ Odvojeno, svaka država pri formulisanju nacionalne strategije koristi svoje termine i definicije. Primjer: Velika Britanija (UK) definiše sajber prostor kao „sve forme rada na mreži, digitalne aktivnosti; ovo uključuje sadržaj i akcije sprovedene kroz digitalne mreže“.

Informaciona bezbjednost podrazumijeva stanje povjerljivosti, cjelovitosti i dostupnosti podataka. Informaciona bezbjednost se fokusira na podatke bez obzira na njihovu formu: elektronski, štampani ili drugi oblici podataka.

Računarska bezbjednost obično teži da obezbijedi dostupnost i ispravno funkcionisanje računara i računarskog sistema.

Često dolazi do naizmjeničnog korišćenja navedenih termina, iako se odnose na malo drugačije aspekte u oblasti sajber bezbjednosti.

Internet bezbjednost u tehničkom kontekstu se odnosi na zaštitu Internet servisa i odnosnih ICT sistema i mreža kao produžetka mrežne bezbjednosti u organizacijama i domovima, a kako bi se obezbijedila svrha bezbjednosti. Internet bezbjednost takođe obezbjeđuje dostupnost i pouzdanost Internet servisa. Ipak, u političkom kontekstu, Internet bezbjednost se često izjednačava sa onim što je takođe poznato kao bezbjedno korišćenje Interneta. Prema nekim definicijama, Internet bezbjednost podrazumijeva globalni režim koji se nosi sa stabilnošću Internet koda i hardvera, kao i sporazume o procesuiranju nelegalnog sadržaja. **Mrežna bezbjednost** je takođe važna za kritične infrastrukture koje često nijesu direktno povezane na Internet.

Sajber bezbjednost - Međunarodna organizacija za standardizaciju (ISO) definiše sajber bezbjednost kao „očuvanje povjerljivosti, integriteta i dostupnosti informacija u sajber prostoru“. Holandija je ponudila nešto širu definiciju: „sloboda od opasnosti ili štete prozrokovane prekidom, kvarom ili zloupotrebom rada ICT-a. Opasnost ili šteta prouzrokovana prekidom, kvarom ili zloupotrebom može se sastojati od ograničenja dostupnosti ili pouzdanosti ICT-a, kršenja privatnosti informacija sačuvanih na ICT uređajima, ili šteta integritetu informacija. ITU takođe definiše široko sajber bezbjednost kao: „Kolekcija alata, pravilnika, sigurnosnih koncepata, zaštita, smjernica, pristupa u upravljanju rizicima, akcija, obuka, najboljih praksi, uvjerenja i tehnologija koje se mogu koristiti radi zaštite sajber okruženja i organizacija i korisničke imovine. Sajber bezbjednost pretenduje da obezbijedi postizanje i održavanje bezbjednosti imovine organizacije i korisnika protiv relevantnih sigurnosnih rizika u sajber okruženju. Generalni bezbjednosni ciljevi se sastoje od sljedećeg: dostupnosti; integriteta, koji može uključiti autentičnost i neporječivost, i povjerljivosti.“

Sajber odbrana se uglavnom koristi u vojnom kontekstu, ali može se odnositi i na kriminalne i špijunske aktivnosti.

NATO koristi sljedeću definiciju kada je riječ o sajber odbrani: „sposobnost da se osigura dostava i upravljanje servisima u operativnim komunikacionim i informacionim sistemima kao odgovor na potencijalne, neposredne kao i stvarne, maliciozne akcije koje potiču iz sajber prostora".

Sajber kriminal - ili e-kriminal, ili VTK obuhvata kriminalne aktivnosti u kojima su kompjuteri i slični informatički uređaji i kompjuterska mreža predmet, sredstvo, cilj ili mjesto krivičnog djela.

Sajber terorizam – predstavlja kriminalni akt u sajber prostoru koji ima za cilj da se zaplaši Vlada ili njeni građani, a sve u cilju ostvarivanja političkih ciljeva. NIPC (National Infrastructure Protection Center) definiše sajber terorizam kao „kriminalni akt izvršen putem računara, a koji za rezultat ima nasilje, smrt i/ili destrukciju, stvarajući teror radi ubjeđivanja Vlade da promijeni svoju politiku".

Sajber špijunaža je definisana kao, „korišćenje agenata u cilju dobijanja informacija u vezi sa planovima ili aktivnostima strane države ili konkurentske kompanije". Nije rijedak slučaj gdje su kompanije ili vlade suočene sa pokušajima neautorizovanih pristupa njihovim kompjuterskim sistemima putem Interneta. Mnoge države koriste sredstva špijunaže da bi podstakli svoj ekonomski razvoj baziran na naprednim tehnologijama drugih nacija. ICT predstavlja bazičnu osnovu u razvoju i implementaciji većine drugih tehnologija, kako u civilnom, tako i u vojnom sektoru, i usljed toga postale su primarni cilj špijunaže.

Sajber ratovanje je neodređen i kontraverzan termin za koji ne postoji zvanična ili generalno prihvaćena definicija. Više od 30 država je prihvatilo doktrinu i najavilo razvoj specijalnog programa ofanzivnih mehanizama sajber ratovanja.

1.2.4. Da bi sagledali moguće kriminalne aktivnosti u Sajber prostoru, prikazaćemo osnovne izazove i prijetnje, koji su elaborirani kroz nekoliko zvanično usvojenih dokumenata u Crnoj Gori:

a. Propusti u organizaciji sajber zaštite mogu predstavljati opasnost po nacionalnu bezbjednost Crne Gore;
b. Internet se u Evropi pa i u našem bliskom okruženju intenzivno koristi u kriminalne svrhe, za potrebe trgovine drogom, pranja novca i finansijskih prevara, pa ni Crna Gora nije i neće biti pošteđena ove opasnosti;
c. ICT infrastruktura, računarski sistemi i korisnici u Crnoj Gori izloženi su većini sajber opasnosti i napada koje pogađaju ostatak svijeta. Ovo uključuje maliciozne programe, elektronske prevare, izmjene naslo-

vnih web stranica (Web Defacement) i "hakovanje" elektronske pošte;

d. Nerazvijena saradnja između privatnog i javnog sektora u oblasti koordinacije sistema bezbjednosti kritične infrastrukture;
e. Nepostojanje procedura, evidencija incidentnih situacija u sajber prostoru Crne Gore
f. Nepostojanje nacionalnog Savjeta za sajber bezbjednost sa njegovim funkcijama:
    i. koordinacija informacione bezbjednosti u Crnoj Gori
    ii. definisanje kritične informatičke infrastrukture
    iii. razmatranje legislativnog okvira za razvoj operativne sajber bezbjednosti
g. Sajber prostor se sve više koristi za organizaciju i medijsku propagandu ekstremističkih i radikalnih grupa koje na taj način propagiraju svoje aktivnosti, vrbuju nove članove, organizuju terorističke akcije i tako predstavljaju opasnost po nacionalnu bezbjednost Crne Gore.
h. Piraterija doprinosi visokoj stopi zaraženosti računarskim virusima.
i. On-line manipulacije, koristeći socijalni inženjering putem e-mail poruka, kao što je *„Nigerian 419"* prevara, *phishing*, idu ruku pod ruku sa krađom identiteta (nezakonita saznanja o nalozima i lozinkama drugih korisnika). Ovakvo stanje u crnogorskom sajber-prostoru je zabrinjavajuće i problematično i ne samo za Crnu Goru već i šire. Crnogorski građani u prošlosti su bili mete prevara i u tim prevarama čak ostajali i bez veće sume novca;
j. U periodu od 2008.-2013. godine, napadači su izmijenili ili preuzeli kontrolu nad više naslovnih web stranica crnogorskih institucija;
k. U Crnoj Gori je u prošlom periodu bilo više napada na informatičku infrastrukturu, na servise provajdera interneta kao i na bankarski sektor;
l. Prethodnih godina je primijećen i značajan broj slučajeva u kojima su napadači preuzeli kontrolu nad korisničkim profilima crnogorskih državljana na društvenim mrežama i ostavljali u ime vlasnika neprimjereni sadržaj, sve u cilju kompromitovanja vlasnika profila.
m. Sa adresa, za koje se istragom utvrdilo da potiču iz Crne Gore, prijavljeno je maliciozno djelovanje, između ostalog širenja SPAM-a, napadi probijanja lozinke metodom sile (brute force), DDoS napadi, lažno predstavljanje i drugi;
n. U Crnoj Gori postoji vrlo mali broj kadrova koji posjeduju usko specijalizovana znanja iz oblasti sajber bezbjednosti, tj. da posjeduju određene licence ili sertifikate iz ove oblasti, koje zahtijevaju evropski i svjetski standardi. U okviru Univerziteta u Crnoj Gori ne postoje fakulteti ili smjerovi koji obrađuju sajber bezbjednost ili forenziku, tj. da proizvode kadrove sa usko specijalizovanim znanjem iz ove oblasti.

1.2.5. Pravni akti koji čine temelj funkcionisanja i osnov za dalju nadogradnju savremenog koncepta informacione bezbjednosti u Crnoj Gori su:

a. Zakon o potvrđivanju Konvencije o računarskom kriminalu
b. Krivični zakonik
c. Zakonik o krivičnom postupku
d. Zakon o informacionoj bezbjednosti
e. Zakon o Agenciji za nacionalnu bezbjednost
f. Zakon o tajnosti podataka
g. Zakon o elektronskom potpisu
h. Zakon o elektronskim komunikacijama
i. Zakon o elektronskoj trgovini
j. Stategija sajber bezbjednosti u Crnoj Gori 2013-2017

Ostali važni akti koje treba pomenuti u ovom poglavlju:

- Elaborat sa definisanim nadležnostima državnih organa u borbi protiv računarskog kriminala kojim je izvršena procjena stanja i spremnost države u oblasti sajber bezbjednosti,
- Uredba o bližim uslovima i načinu sprovođenja informatičkih mjera zaštite tajnih podataka (01.jul 2010. godine),
- Uredba o bližim uslovima i načinu sprovođenja mjera zaštite tajnih podataka (06.novembar 2008.godine),
- Uredba o bližim uslovima i načinu sprovođenja industrijskih mjera zaštite tajnih podataka (16.decembar 2010. godine),
- Uredba o načinu vršenja i sadržaju unutrašnje kontrole nad sprovođenjem mjera zaštite tajnih podataka (28.jul 2010. godine).

1. 3. Zakonska zaštita softvera pravima intelektualne svojine

1.3.1 Nekada smo uređaje razlikovali po njihovom spoljašnjem izgledu, koji se često naziva hardverom, riječ koja je već postala sastavni dio našeg svakodnevnog rječnika, iako nijesmo sigurni da je svi u potpunosti razumiju. Danas većina uređaja liči jedan na drugi iako obavljaju potpuno različite funkcije, zahvaljujući nečemu što stoji u pozadini svega i što se često naziva softverom, čiju riječ takođe često koristimo, sa podjednakim nivoom razumijevanja kao kada je u pitanju hardver. Ono što svi manje ili više zaključuju jeste da je softver jedna od najprofitabilnijih oblasti, koja je u posljednjoj deceniji u velikoj ekspanziji.

Nažalost, još manji broj osoba razlikuje sami pojam ”softver”, od pojma ”softverski projekat” ili od pojma ”informacioni/računarski sistem”. Da ne

pominjemo i pojmove koji čine sastavni dio mozaika priče o softverima, kao što su: *podatak, informacija, algoritam, Kod, Use case, Class dijagrami, Activity dijagrami, State dijagram, modeli ORG, BPM CPJ* itd. Još je veća opasnost kada ove pojmove ne razumiju osobe koje vrše analize i vještačenja iz ove oblasti. Zbog pogrešnog razumjevanja, donose se i pogrešni zaključci.

Da je stvar izuzetno složena i komplikovana govori i podatak iz 2011. godine (*Garnerovo istraživanje*) da se na svjetskom nivou 31% softverskih projekata nikada ne završi, a 53% završi se sa značajnim prekoračenjem planiranog vremena i resursa (značajnim, na nivou 189% od planiranih), dok uspješnost iznosi svega 16%. Ako se tome doda podatak da na takve projekte državne organizacije i ustanove, kompanije i druge organizacije troše nekoliko desetina milijardi dolara godišnje, onda je jasno u kojoj mjeri je profatibilnost ove oblasti praćena rizikom od neuspjeha.

1.3.2. Softver i pojmovi u oblasti informaciono-komunikacionih tehnologija

Kada se pomene softver, većina ljudi koji uopšte imaju neka saznanja o tom pojmu, pod tim podrazumjeva napisane programe koji se izvršavaju na nekom računaru. Međutim, stvar je drugačija. Prije svega, programi se ne mogu napisati ukoliko u njihovoj osnovi ne leže odgovarajuće procedure i pravila koja definišu na koji način se rješava problem koji je predmet programa. Samo pisanje programa stvar je tehnike koja realizuje korake koji su predviđeni u postupku za rješavanje posmatranog problema. Međutim, iste korake za rješavanje problema svako od nas bi realizovao na svoj način, čak i kada bi koristili isti programski jezik za pisanje programa. To znači da pisanje programa tj. izrada softvera sadrži u sebi određenu kreativnu komponentu od koje će svakako zavisiti i veličina i složenost napisanog programa.

Jedna od najčešće korišćenih definicija Softvera (ISO_2382) jeste: "Softver je intelektualna kreacija koja sadrži programe, procedure, pravila i odgovarajuću dokumentaciju koja se odnosi na rad nekog sistema za obradu podataka".

Takođe, ISO_12207 definiše i sljedeće pojmove:

- Pod **"softverskim proizvodom"** podrazumijeva se skup računarskih programa, procedura i odgovarajuća dokumentacija i podaci koji su namijenjeni za isporuku korisniku
- **"Kod"** je sistem pravila koji obezbjeđuje da isporuke budu kodovane u izvornom kodu (engl. Source Code) koji je razumljiv prevodiocima izvornog koda.

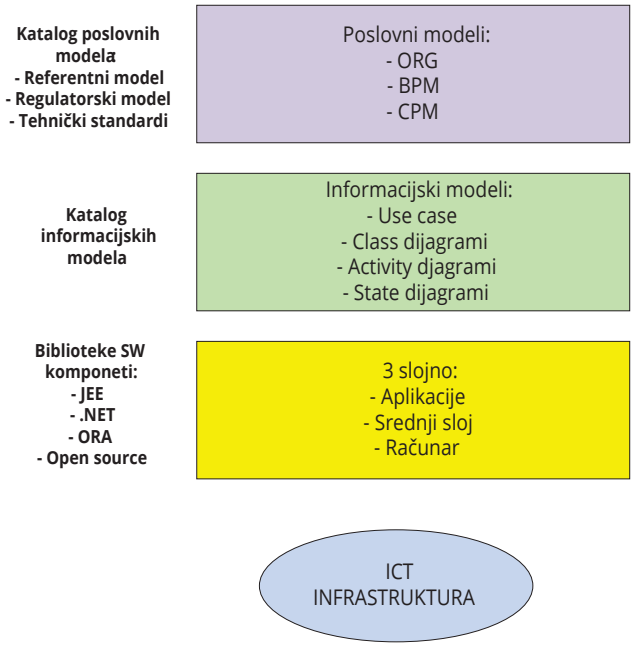
Dakle, da bi se instrukcije mogle izvršavati, potrebno je da se izvorni kod "prevede", a tu ulogu imaju specifični djelovi operativnog sistema.

Softveri se mogu podijeliti na sljedeće kategorije:

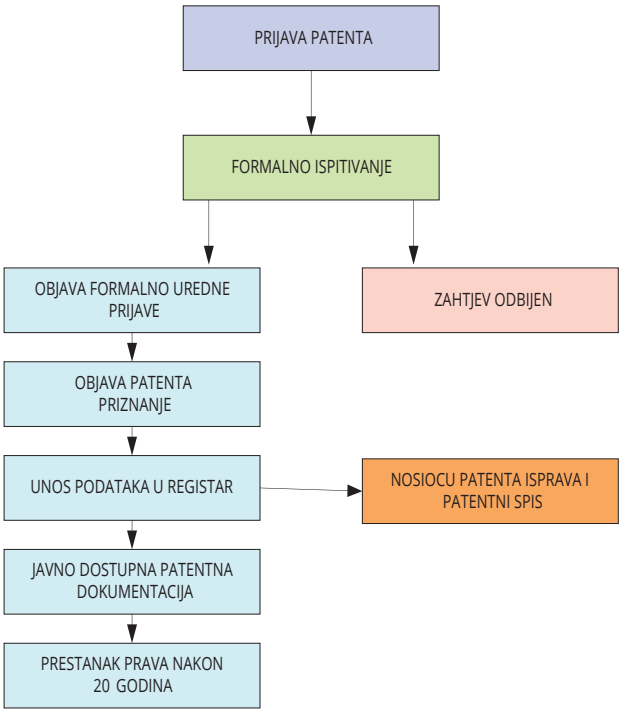
- **Public domain** je softver sa kojim korisnik može raditi šta želi. Dopušteno je korišćenje, umnožavanje, distribucija pa čak i prodavanje bez ikakve dozvole autora.
- **Open Source** je softver koji je besplatan za korišćenje, umnožavanje i distribuciju, a dozvoljeno je raditi promjene u izvornom kodu, te je takav softver moguće dalje distribuirati. Jedini uslov koji se obično nameće korisniku je da promijenjeni softver i dalje bude Open Source. Takav softver se distribuira zajedno s licencom u kojoj su definisana sva prava i obaveze korisnika. Ako korisnik distribuira takav softver, bilo u izvornom obliku, bilo izmijenjen, uvijek se mora distribuirati pod istim licenčnim sporazumom.
- **Freeware** je besplatan za korišćenje i distribuciju, ali se ne smije mijenjati. Taj softver se takođe izdaje pod posebnom licencom sa definisanim pravilima korišćenja. Autor zadržava autorsko pravo na ovakav softver.
- **Sharware** je sličan kao i Freeware, ali se u licenčnom sporazumu obično traži da korisnik pošalje autoru određenu svotu novca. Kod takvog softvera obično postoji definisano vrijeme u kojem korisnik može besplatno koristiti program, a ako ga želi koristiti i nakon tog razdoblja mora ga platiti. Novčane svote za takav softver su obično simbolične i to je zgodan način za distribuciju softvera koji inače ne bi opstao na tržištu komercijalnog softvera.
- **Komercijalni softver** je softver koji korisnik mora kupiti te ga smije samo koristiti, a ne kopirati, distribuirati ili mijenjati. Postoje dva tipa komercijalnog softvera:
    - ◊ Softver koji korisnik može kupiti
    - ◊ Licencirani softver

Ako korisnik kupi kopiju programa (ili namjenski urađen program), može ga koristiti na način definisan Zakonom o autorskim pravima.

Informacioni sistem se može predstaviti sa tri međusobno povezana modela, kao na slici 1.



Slika 1. Arhitektura informacionog sistema



Slika 2. Postupak za priznanje patenta

Znači, kada se posmatra ili opisuje razvijeni informacioni sistem, potrebno je poznaviti sve njegove nivoe. Jedino takvim pristupom može se imati kompletna slika jednog sistema.

Teorijski je nemoguće da postoje dva ista informaciona sistema, jer se i uslovi implementacije mijenjaju u zavisnosti od sistema do sistema.

1.3.3. Pravna regulativa u Crnoj Gori

Kada se govori o zaštiti softvera različitim pravima intelektualne svojine prvo treba dati njihovu definiciju. Crna Gora je usvojila dva važna zakona koja govore o ovoj problematici i to: Zakon o autorskim i srodnim pravima i Zakon o patentima.

Zakonom o autorskim i srodnim pravima utvrđuje se pravo autora književnih i umjetničkih djela (autorsko pravo), prava interpretatora, proizvođača fonograma, filmskih producenata, radiodifuznih organizacija, izdavača i proizvođača baza podataka, autorsko ugovoreno pravo, kolektivno ostvarivanje autorskog i srodnih prava i zaštita autorskog i srodnih prava.

Prema članu 4, odjeljka A pomenutog Zakona, **autorsko djelo** je individualna duhovna tvorevina iz oblasti književnosti, nauke i umjetnosti, koja je izražena na određeni način, ako ovim Zakonom nije drugačije određeno. Autorskim djelima smatraju se naročito, između ostalog, i pisana djela: romani, poezija, članci, priručnici, studije, monografije i računarski programi. U članu 19 se kaže: *"da autor ima isključivo pravo da dozvoli ili zabrani iskorišćavanje svojeg djela ili njegovih primjeraka*". Takođe isti član navodi *"Iskorišćavanje autorskog djela dozvoljeno je samo kada autor, pod uslovima koje odredi, ustupi odgovarajuće autorsko imovinsko pravo"*.

U odjeljku B - Računarski programi data je definicija računarskog programa koja glasi: **"Računarski program** u smislu ovog zakona, je pisano autorsko djelo izraženo u svakom obliku, uključujući i projektni materijal za njegovu izradu ako ispunjava uslove iz člana 4 stava 1 ovog Zakona". Ideje, principi i metode koji su osnov za izradu računarskog programa, kao i njegov interfejs, nijesu obuhvaćeni autorskom pravnom zaštitom, u smislu ovog Zakona.

U članu 112 definisano je da "smještanje, prikazivanje, djelovanje, prenos ili bilježenje u digitalnom obliku računarskog programa, koje zahtijeva njegovo umnožavanje, u smislu ovog Zakona predstavlja isključivo pravo autora na umnožavanje". Član 113 definiše da "Umnožavanje koda i prevod oblika računarskog programa može se vršiti samo ako je u skladu sa uobičajenim iskorišćavanjem djela i ako se time ne nanosi šteta zakonitim interesima autora".

Prema ***Zakonu o patentima*** (član 5) **"Patent"** je pravo koje se priznaje za pronalazak iz bilo koje oblasti tehnike, koji je nov, koji ima inventivni nivo

i koji je industrijski primjenjiv". Predmet pronalaska koji se štiti patentom može biti proizvod (kao npr. uređaj, supstanca, kompozicija) ili postupak. Na osnovu ovog zakona, ne smatraju se pronalascima: otkrića, naučne teorije i matematičke metode; estetske kreacije; planovi, pravila i postupci za obavljanje intelektualne djelatnosti, za igranje igara ili za obavljanje poslova; programi računara i prikazivanje informacija. Na gore navedenoj slici 2 je prikazan postupak za priznanje patenta.

1.3.4. Kršenje autorskih prava softvera

Kršenje autorskih prava, u kontekstu softvera, je, u suštini, pokretanje, kopiranje, mijenjanje ili distribuiranje računarskih programa, osim u slučajevima:

- kada to radi sam vlasik tog programa
- kada se posjeduje licenca (dozvola) vlasnika prava na program.

Ugovor o licenciranju mora da sadrži šta je dozvoljeno, a šta ne.

Postoje razne vrste zloupotrebe softvera. Najčešće vrste povreda su sljedeće:

- potpuna nelicencirana upotreba, npr: kopiranje softvera od prijatelja ili preko interneta, gdje licenca za softver ekspilcitno ne dozvoljava ovo;
- prekomjerna upotreba, npr: kupovina softvera koji je licenciran za jedan računar, a instaliranje na dva;
- ako se posjeduje već dodijeljena licenca softveru, npr: ako se kupuje polovan hardver, on ne mora da prenese sve licencirane softvere i potrebno je da se preuzmu sve mjere da se osigura da je upotreba zakonita;
- zloupotreba šerovanja: gde je softver lincenciran "za određene svrhe" i sl, to je kršenje autorskih prava koja prevazilaze ove uslove;
- pribavljanje softvera na prevaru, npr. kupovina softvera za sniženu cijnu pretvarajući se da radite u obrazovnoj instituciji;
- "warez" kršenje autorskih prava: "warez" je sajt na Internetu koji omogućava ljudima da preuzmu ilegalne kopije softvera. Softver će obično imati svoja "oštećena" digitalna prava, pa se ona nazivaju "warez kopijama" ili "hakovanim kopijama". Ljudi koji prave „warez" kopije, ljudi koji vode "warez" sajtove i ljudi koji preuzimaju te kopije i koriste ih su prekršioci autorskih prava.
- nezakonite "specijalne ponude" od hardverskog prodavca: hardver prodavac prodaje kompjuter sa instaliranim softverom, ali to je softver bez licence.
- pravljenje nezakonite kopije softvera na CD-ovima, ili nečemu sličnom, radi davanja nekom drugom.

- falsifikovanje: pravljenje nazakonite kopije softvera na CD-ovima, ili nečemu sličnom, za komercijalnu svrhu, i prodavanje istih pod izgovorom da su to zakonite kopije. Ako se softver prodaje po znatnoj nižoj cijeni, moguće je da je falsifikovan. [5]

1.3.5. Međunarodna zaštita softvera pravima intelektualne svojine

Jedno od najstarih prava intelektualne svojine je autorsko pravo. Međunarodna zaštita autorskog prava regulisana je **Bernskom konvencijom** koja je donijeta još 1886. godine i više puta revidirana. Ovom Konvencijom se štite literalna i umjetnička djela, uz uslov da su originalna. Mada djela, koja se mogu štititi autorskim pravom, ne sadrže eksplicitno programe računara, došlo se do generalnog stava da su programi računara proizvodi intelektualne kreativnosti i da se kao takvi smatraju djelima u smislu ove Konvencije.

Osim toga i prema **TRIPS**-u (Agreement on Trade-Related Aspects of Intellectual Property – Sporazum o trgovinskim aspektima prava intelektualne svojine) predviđeno je da se programi računara, bilo da su u izvornom ili izvršnom kodu, štite kao literalna djela prema pomenutoj Bernskoj konvenciji po reviziji od 1971. godine.

Autorsko pravo ne zahtijeva otkrivanje djela, odnosno u ovom slučaju ne zahtijeva otkrivanje programa u izvornom kodu. Na taj način, za razliku od programa u izvršnom kodu koji se plasira na tržištu, izvorni kod programa ostaje poslovna tajna što takođe predstavlja još jedan oblik intelektualne svojine.

Prema Bernskoj konvenciji djela su zaštićena samim činom svog stvaranja, odnosno nije potrebno vršiti njihovu registraciju kod nekog nadležnog organa, što važi i za softver. Zaštita softvera autorskim pravom traje za život autora i još 50 godina poslije njegove smrti, dok je TRIPS-om sada produžen period zaštite na 70 godina.

U slučaju patentnog sistema stvari stoje sasvim drugačije. Naime, patentna prava se ne stiču automatski, samim nastankom pronalaska ili obavještavanjem javnosti o tome. Ova prava se stiču tek poslije sprovedenog upravnog postupka za priznanje patenta koji se pokreće podnošenjem prijave patenta. Patent je ograničen vremenski, jer može da traje najviše 20 godina od dana podnošenja prijave, zatim on je ograničen teritorijalno, odnosno važi samo na teritoriji zemlje čijem nadležnom organu je podnijeta prijava patenta. U slučaju softvera, patentiranje znači i otvaranje izvornog koda, što je u najmanju ruku problematično sa aspekta autora softvera.

Trenutno stanje je takvo da patenti još uvijek nijesu preovlađujući oblik zaštite softvera. Prema istraživanjima koje je finansirala Evropska Unija za

sada prioritet imaju:

- autorsko pravo
- tehnički sistemi zaštite
- licenciranje

Ovo je posebno uočljivo u slučaju malih i srednjih preduzeća, dok velike kompanije pokazuju veći afinitet prema patentnom sistemu.

II MEĐUNARODNO-PRAVNI OKVIR BORBE PROTIV SAJBER KRIMINALA

2. 1. Konvencija o Sajber kriminalu (CETS br. 195)

Konvencija o Sajber kriminalu Savjeta Evrope je prvi međunarodni sporazum koji reguliše materijalno pravni, procesno pravni, organizacioni i međunarodni okvi rkrivičnih djela koja su izvršena putem interneta i drugih računarskih mreža.

Konvencija postavlja osnovne postulate pravnih normi koje se tiču kršenja prava intelektualne svojine, računarski izvršenih prevara, zloupotreba maloljetnika u pornografske svrhe itd. Ovom Konvencijom su propisane i radnje i mjere, kako materijalno, tako i procesno pravne prirode, koje su usmjerene ka regulisanju društveno štetnog ponašanja u ovoj oblasti i koje primjenjuju savremene istražne metode prilikom otkrivanja i gonjenja izvršioca krivičnih djela, kao što su pretraga računarskih mreža i presretanje računarskih podataka, čiji je glavni cilj gonjenje izvršioca krivičnih djela i uspostavljanje zajedničke krivično-pravne politike, koja je usmjerena ka zaštiti društva od svih oblika visokotehnološkog, tj. „sajber kriminala", posebno kroz usvajanje odgovarajućih pravnih normi i uspostavljanje operativne međunarodne saradnje u ovoj oblasti.

Konvencija o Sajber kriminalu Savjeta Evrope je nakon višegodišnjeg perioda usaglašavanja izvornog teksta otvorena za potpisivanje od strane članica Savjeta Evrope, kao i za potpisivanje od strane zemalja koje nije-su članice Savjeta Evrope, a koje su učestvovale u izradi izvornog teksta u Budimpešti, 23.novembra 2011. godine.

Činjenica je da ova Konvencija trenutno predstavlja jedini međunarodno pravno priznat i kontinentalno raširen pravni instrument u oblasti visokotehnološkog kriminala, koji u svom tekstu objedinjuje precizno određene, i što je još bitnije, upotrebljive i savremene metode postupanja nadležnih 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 uspostavljenu planetarnu mrežu za prvo kao i rano reagovanje, te vođenje daljih pretkrivičnih i krivičnih postupaka, imaju mogućnost da na odgovarajući način, u skladu sa svojim tehničkim mogućnostima, odgovore na izazove visokotehnološkog, tj. „sajber kriminala", koje pred njih stavljaju izvršioci ovih krivičnih djela.

Do 23.decembra 2013. godine, ukupno 52 zemlje su ratifikovale, zatražile pristupanje ovoj Konvenciji ili potpisale istu. Osam zemalja nijesu članice Savjeta Evrope. U te zemlje spadaju Australija, Kanada, Dominikanska Republika, Japan, Mauricijus, Južnoafrička Republika, Tonga i Sjedinjene Američke Države.

Od zemalja članica Evropske Unije, kojih je ukupno 28 u ovom momentu, samo Grčka, Lihtenštajn i Poljska nijesu i ratifikovale ovu Konvenciju, ali je jesu potpisale, dok su sve ostale zemlje članice Evropske Unije Konvenciju i ratifikovale, te se ista u skladu sa unutrašnjim pravnim poretcima zemalja potpisnica aktivno primjenjuje kroz unutrašnje materijalno, procesno i međunarnodno pravne odredbe.

Revolucija u informacionim tehnologijama je suštinski promijenila društvo i nastavljaće da ga mijenja i u buduće. Mnogi poslovi su postali jednostavniji za obavljanje. Do skoro, i u samo određenim djelovima društva, radi racionalizacije radnih procedura, korišćene su informacione tehnologije u svakodnevnom radu. Danas je teško zamisliti bilo koji dio društva bez uticaja primjene računara i računarskih sistema. Informacione tehnologije su na sveobuhvatan način danas umiješane i iskorišćene u svakom aspektu ljudske aktivnosti.

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

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

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

Ipak, domaći zakonodavni okvir je generalno ograničen. Iz tih razloga, problemi u ovoj oblasti su morali da budu riješeni na međunarodnom nivou kroz međunarodno pravni okvir, koji je iznjedrio usvajanje adekvatnih

međunarodnih pravnih instrumenata. Danas takav instrument predstavlja Konvencija o Sajber kriminalu Savjeta Evrope CETS 185, čiji je cilj da se suprotstavi ovoj vrsti izazova, uz dužno poštovanje ljudskih prava, u novom informatičkom i post informatičkom društvu.

Konvencija za svoj cilj ima na prvom mjestu harmonizaciju domaćih materijalno krivično pravnih odredbi u oblasti „sajber" kriminala, omogućavanje domaćem krivičnom procesno-pravnom okviru da nadležnim državnim organima pruži ovlašćenja koja su neophodna za 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:

- Upotreba termina (I)
- Mjere koje trebaju da budu preduzete na domaćem nivou – materijalno i procesno pravo (II)
- Međunarodna saradnja (III)
- Završne odredbe (IV)

Prvi odjeljak druge glave predviđa odredbe o sankcionisanju kriminala koji je izvršen pomoću računara i računarskih mreža i koji određuje 9 opštih krivičnih djela koja su podijeljena u 4 različite kategorije.

Krivična djela koja su određena Konvencijom su:

1. neovlašćeni (protiv pravni) pristup
2. neovlašćeno (protiv pravno) presretanje
3. ometanje toka podataka
4. ometanje računarskog sistema
5. zloupotreba uređaja
6. falsifikovanje počinjeno pomoću računara
7. prevara izvršena pomoću računara
8. krivična djela dječije pornografije
9. krivična djela autorskih i srodnih prava.

U odjeljku 2, druge glave, kada govorimo o procesnim odredbama isti predviđaju:

1. hitno čuvanje pohranjenih podataka
2. hitno čuvanje i djelimično otkrivanje podataka o saobraćaju
3. naredbu za dostavljanje
4. pretragu i zaplenu računarskih podataka
5. prikupljanje podataka o saobraćaju u realnom vremenu
6. presretanje podataka o saobraćaju

U trećoj glavi 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 kom slučaju se primjenjuju odredbe same Konvencije, kao i u slučajevima kada takva osnova postoji;
- kada se primjenjuju odredbe tih pravnih okvira uz pomoć primjene same Konvencije.

Takođe, 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.

U okviru poglavlja 1, Konvencija na opšti način definiše pojmove kao što su računarski sistem, računarski podaci, pružalac usluga, podaci o saobraćaju, itd.

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

Pod automatskom obradom podataka se smatra 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 strane računara radi postizanja određenih tj. željenih rezultata. Računari mogu koristiti različite programe.

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

satelitskog emitovanja) ili korišćenjem 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, takođe, mogu biti međusobno povezane na opisane načine.

Internet predstavlja globalnu mrežu koja se sastoji od mnoštva međusobno povezanih mreža koje sve koriste isti komunikacioni protokol, tj. način komunikacije. Drugi tipovi mreža takođe postoje, bez obzira da li su ili nijesu 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 esecijalno 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 takozvanom „ISO" standardima. Ova definicija sadrži izraze koji su pogodni za procesuiranje, tj. korišćenje. Ovo znači da su podaci, da bi imali i kvalitet , sastavljeni u takvoj formi da mogu biti direktno obrađeni – procesuirani od strane računarskog sistema.

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

Na osnovu ove definicije, računarski podaci su oni podaci koji su, u smislu krivično-pravnog 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 predviđene ovom Konvencijom.

2. 2. Pružalac usluga

Termin pružalac usluga, tj. „*Internet service provider*", obuhvata široku kategoriju fizičkih i pravnih lica koja imaju određene uloge u odnosu na komunikaciju ili procesuiranje podataka u računarskim sistemima. Pod ovom definicijom je jasno navedeno da kako javni, tako i privatni subjekti koji pružaju ovakvu vrstu usluga, jesu i moraju biti uključeni u krivično-pravni 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 preduzeća kojima je ovakva vrsta komunikacije omogućena od strane kompanijske mreže.

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

Na primjer, 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 npr. osoba koja sklopi ugovor sa kompanijom za takozvano „web hostovanje" radi „hostovanja", tj. čuvanja i prikazivanja njegovog/njenog web sajta – prezentacije, nije obuhvaćan ovom definicijom, ukoliko entitet kod koga se navedeni sadržaj nalazi takođe ne pruža komunikacione ili obrađivačke usluge podataka.

2. 3. Podaci o saobraćaju

Pojam podataka o saobraćaju je definisan u članu 1. Konvencije, u okviru stava D, i predstavlja kategoriju računarskih podataka koji su predmet posebnog pravnog režima. Ova vrsta podataka je generisana - stvorena od strane računara (kompjutera) 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 sa 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 krivično-pravne odgovornosti njegovog izvršioca. Zbog svoje prirode, koja se ogleda u vrlo kratkom trajanju, podaci o saobraćaju zahtevaju da budu sačuvani – obezbijeđeni 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 strane nadležnog organa, otkrivanja ili

gonjenja bivaju preduzete radi utvrđivanja postojanja krivičnog djela i eventualne krivične pravne odgovornosti njegovog izvršioca, mogu se u ovom slučaju pokazati kao nedovoljne. Šta više, 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 okvir, koji prati primjenu standardnih istražnih metoda mogu predstavljati jednu od ključnih prepreka za uspješno gonjenje u ovoj krivično- pravnoj 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 pomenuti da neće sve ove kategorije biti uvijek tehnički dostupne, posebno kada imamo u vidu raznolikost tehničke opremljenosti i obučenost zaposlenih u raznim preduzećima koja se bave uslugom pružanja pristupa internetu ili omogućavanju korišćenja određenih kategorija usluga koje su vezane za korišćenje računarskih mreža, kako međunarodnih, tako i lokalnih, javnih i privatnih.

Porijeklo komunikacije se odnosi na broj telefona, internet protokol, adresu ili sličnu identifikaciju komunikacione opreme kojoj internet servis provajder pruža usluge.

Odredište predstavlja uporedivu indikaciju o uređajima koji služe za komunikaciju, kako je sama komunikacija, tj. podaci usmjereni, transmitovani ili isporučeni.

Pojam vrste servisa se odnosi na vrstu usluge koja se koristi unutar same mreže i može biti ostvarena 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 sa njihovom osjetljivišću. U ovom smislu, u članu 15 Konvencije, postoji obaveza da strana potpisnica pruži uslove i garancije radi adekvatne zaštite ljudskih prava i sloboda.

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

2. 4. Krivična djela

Konvencija Savjeta Evrope CETS 185 o računarskom kriminalu, tzv. „Sajber krajm Konvencija“, u svojoj II glavi u okviru 3. djela reguliše materijalno-pravni okvir i to u članovima od 2 do 13, procesno pravni okvir od članova 14 do 21, kao i nadležnost u članu 22.

Cilj propisivanja materijalno pravnog okvira Konvencijom, u svakom slučaju, leži u unapređenju sredstava radi sprječavanja, kao i gonjenja svake vrste kriminala, tj. kriminaliteta, a u ovom slučaju specifičnog oblika, tj. vrste kriminaliteta koji se izvršava pomoću računara i u računarskom okruženju uz korišćenje računarskih mreža.

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

U koliko bi ovakva harmonizacija materijalno pravnih krivičnih odredbi izostala, primjena drugih međunarodno pravnih instrumenata, kao što je na primjer, Palermo Konvencija ili Konvencija o pružanju međunarodne pravne pomoći u krivičnim stvarima iz 1959. godine, bila bi dovedena u pitanje, u smislu da ne bi bilo moguće da se odredbe tih drugih konvencija primjenjuju jedinstveno na teritoriji i u okviru pravnih poredaka zemalja koje su ratifikovale navedene konvencije, 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 krivično pravnom smislu određenog ljudskog ponašanja, koje mora biti propisano kako materijalno pravnim odredbama krivičnog zakonodavstva zemlje molilje, kao izamoljene zemlje. U slučaju nedostatka harmonizacije materijalno pravnih propisa u ovoj oblasti, kao i u svakoj drugoj oblasti krivično pravog progona, neumitno bi dovelo do neželjenog ishoda u vidu nemogućnosti preduzimanja 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 „Sajber krajm Konvencijom" Savjeta Evrope predstavljaju minimum regulisanja i propisivanja krivično pravne norme u domaćim zakonodavstvima zemalja koje su ratifikovale i koji u svakom slučaju, ne isključuje njihovu dodatnu razradu u okviru krivičnih zakonika tih zemalja.

Komitet navedene Konvencije, koji je sastavljen od nacionalnih predstavnika zemalja koje su ratifikovale Konvenciju, kao i Biro navedenog Komiteta (T-SY), u periodu koji je danas već duži od jedne dekade, je aktivno radio i radi na osavremenjavanju tumačenja i metoda primjene osnovnih odredbi

same Konvencije kroz tzv. „uputstva" (guidelines), koja bi trebalo da detaljnije pojasne mogućnost primjene određenih instituta Konvencije u savremenom životu, kao i u savremenom otkrivanju i gonjenju krivičnih djela iz ove oblasti.

Ipak, može se odati priznanje tvorcima teksta ovog međunarodno-pravnog akta, koji su u drugoj polovini 90-tih godina XX vijeka uspjeli da skoro u potpunosti definišu, propišu i predvide preovlađujuće oblike tzv. Sajber kriminaliteta, te da iste utkaju u tkivo Konvencije koja i posle više od 15 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, korišćenjem tih tehnologija, da odgovori na izazove koji se nalaze pred onim pripadnicima društva kojima je data ustavna i zakonska nadležnost da isto štite od štetnih društvenih pojava.

Kriminalizacija tih ponašanja u vidu protiv pravnog pristupa, protiv pravnog presrijetanja, ometanja podataka, ometanja sistema i zloupotrebe uređaja, 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 krivično pravne odgovornosti pravnih lica u ovoj oblasti, ukazuje na to, da i pored proteka već navedenog vremenskog perioda i brze promjene navedenih tehnologija, u svojoj biti izvršenje krivičnih djela, uključujući i njihove nove oblike i nove načine izvršenja u tzv. „sajber svijetu", mogu biti uspješno predviđeni, definisani i sankcionisani.

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

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

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

2. 5. 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 internet protokola i internet tehnologija, su međusobno povezane kroz podjelu zajedničkih resursa na lokalnom i na globalnom nivou, čime iste neminovno dolaze u kontakt i sa kriminogenim sredinama, često bivajući otvorene ili ranjive za zloupotrebu od strane društvenih elemenata koji nijesu 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 sa ovakvim razvojem društvene stvarnosti i zloupotrebama iste, već i procesno pravo, zajedno sa istražnim tehnikama koje su propisane i neophodne za uspješno postupanje u ovoj oblasti, takođe mora biti, čak i više nego materijalno pravo, u skladu sa IKT (informaciono komunikacionim 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 ovlašćenja državnih institucija takođe moraju biti u korak sa razvojem tehnologije i krivično-pravnog, materijalnog i procesnog okvira.

Jedan od najvećih izazova u borbi protiv visoko tehnološkog kriminala u mrežnom okruženju je teškoća 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. Na primjer, 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, su vrlo često od vitalnog značaja za uspeh istraga u ovoj specifičnoj oblasti kriminala.

U tom smislu, Konvencija o Sajber kriminalu Savjeta Evrope prilagođava tradicionalne procesne mjere kao što su pretresanje stana i prostorija u novom tehničkom okruženju. S tim u vezi, mogu biti kreirane i upotrijebljene 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 osetljivom tehnološkom okruženju.

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

Neke od ovih mjera navedene su u preporuci Savjeta Evrope broj R (95) 13 u vezi problema krivično procesnog prava koji su u vezi sa informacionim tehnologijama.

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

1. podatke o saobraćaju
2. podatke o sadržini komunikacije
3. podatke o pretplatniku

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

- pohranjenom obliku
- u obliku korišćenja u realnom vremenu u toku komunikacije.

Konvencija predviđa definicije ovih izraza u svojim članovima 1 i 18 primjenljivost 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 procesno pravne 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 korišćenje novih i više tehnološko orjentisanih računarskih termina kao što je „pristup“ i „kopiranje“, koji su danas već standardno uključeni u tekstove međunarodnog okruženja u vezi ovih pitanja.

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

Takođe, pojam nadležnih organa, je posebno u zemljama okruženja, u posljednih 10 godina značajno promijenjen, u smislu da su ovlašćenja

u istražnom postupku značajno ili u potpunosti prenijeta na državna tužilaštva, u kom smislu je kao *sui generis* ovlašćenje sudske vlasti ostalo staranje o institutima kojima se ograničavaju ljudska prava i slobode, tj. institutima, čije je određivanje neophodno radi 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. „Sajber krajm Konvenciji" Savjeta Evrope, podrazumijeva da će sve zemlje koje su ratifikovale ovu Konvenciju usvojiti takav normativni okvir koji će dalje dati ovlašćenja 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 krivičnih djela.

S druge strane, uspostavljanje i primjena ovakve vrste ovlašćenja kroz procesne odredbe, treba biti pažljivo posmatrana i usmjerena ka mogućnosti uslovljavanja i kontrole koje su predviđene u okviru domaćeg zakonodavstva. Drugačije rečeno, zemlje koje su ratifikovale Konvenciju su u obavezi da donesu određene procesno pravne norme, kao i njihove modalitete, radi uspostavljanja i primjene ovih ovlašćenja kako u opštim, tako i u posebnim slučajevima, čije će propisivanje biti u skladu sa domaćim pravnim okvirom. Ove odredbe mogu uključivati i takvu vrstu zaštitnih odredbi koje su na domaćem nacionalnom nivou predviđene u okviru Ustava, pravnog poretka, sudskog i javno-tužilačkog 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 bezbjedonosnih agencija da postupaju u skladu sa odredbama Konvencije i drugih međunarodnih i pravnih akata, kojima se obezbjeđuje određena zaštita ljudskih prava i sloboda.

U tom smislu, Konvencija izričito navodi i time uvažava da države koje su ratifikovale istu potiču iz različitih pravnih sistema i kultura, te da nije moguće taksativno navesti, kao i konkretno odrediti jasno primjenjive uslove i zaštitne odredbe za svako moguće ovlašćenje ili proceduru u svakoj pojedinačnoj zemlji. S tim u vezi, ipak postoji zajednički minimum standarda koje Konvencija predviđa. Ovaj minimum standarda proističe iz obaveza svake zemlje koja ju je ratifikovala da primijeni međunarodne instrumente koji su donijeti 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 djelovima 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 uslove za uspostavljanje ovih mehanizama, Konvencija specifično zahtijeva da se takvi uslovi koji se smatraju odgovarajućim u smislu odredaba procesnih zakonodavstava odnose na pravosudne ili druge nezavisne organe nadzora koji u okvirima svojih ovlašćenja mogu odobriti na određeni način krivično-pravne procesne alate, u smislu vođenja krivičnih postupaka, kao i njihovo eventualno ograničavanje radi obezbjeđivanja i poštovanja ljudskih prava i sloboda.

2.5.1. Imajući u vidu ranije navedeno 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, koji se odnose na podatke koji su već prikupljeni i sačuvani od strane držaoca podataka, kao što su na primjer Internet servis provajderi. Ove odredbe se ne odnose na prikupljanje podataka u realnom vremenu, prikupljanje podataka o budućem saobraćaju ili pristup komunikacijama u realnom vremenu. Mjere koje su opisane u ovom članu se odnose samo na podatke koji već postoje i koji su pohranjeni.

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

„**Prezervacija-očuvanje podataka**" označava čuvanje podataka koji već postoje u pohranjenoj formi, koji su zaštićeni od bilo čega što može uticati na njihov kvalitet ili uslove u kojima bi 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 čuvanje istih za buduće i u budućem vremenskom periodu. Retencija podataka je ustvari postupak odlaganja podataka, dok je prezervacija podataka aktivnost koja označava čuvanje podataka na sigurnom i obezbijeđenom mjestu.

Članovi 16 i 17 Konvencije se odnose na tzv. prezervaciju podataka, a ne na retenciju. Oni ne određuju kolekciju i retenciju svih ili nekih podataka koji su prikupljeni od strane internet servis provajdera 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.

2.5.2. 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 zaplenu pohranjenih računarskih podataka (član 19),
- prikupljanje podataka u realnom vremenu,
- prikupljanje podataka o saobraćaju u realnom vremenu (član 20),
- presretanje podataka o sadržini komunikacije (član 21).

Od navedenih mjera posebno je interesantno osvrnuti se na tzv. „naredbu o pružanju podataka", koja predstavlja fleksibilnu mjeru koju bi pripadnici organa otkrivanja mogli da primijene u različitim slučajevima, posebno u onim momentima kada druge vrste mjera, kao što su naredbe o pretresu, zapleni, presrijetanju komunikacija i sl., zahtijevaju ispunjavanje značajnijih i zahtjevnijih pravnih i tehničkih uslova.

Primjena ovog proceduralnog mehanizama je posebno korisan i može se odnositi na računarske podatke ili podatke o pretplatniku koji se nalazi u posjedu ili kontroli određene osobe ili provajdera. Naravno, ova mjera je primjenjiva, ukoliko osoba ili servis provajder takvu vrstu podataka čuva. Treba biti svjestan da u pojedinim zemljama u svijetu ne postoji obaveza Internet servis provajdera 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, podataka o pretplatniku, su definisani na takav način da se odnose na bilo koju informaciju koja je zadržana od strane servis provajdera i koja se odnosi na pretplatnika njihovih usluga. Pretplatnički podaci mogu biti čuvani u bilo kojoj formi od elektronske do papirne.

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

U toku krivične istrage, pretplatnička informacija će najverovatnije biti zatražena u dvije situacije, tj. primjera. U prvom primjeru, pretplatnička informacija je potrebna radi identifikacije koje servise i tehničke mjere je određeno lice koristilo ili ih još uvijek koristi, a to lice je pretplatnik, kao što su tip telefonskog servisa (da li je mobilna ili fiksna linija), tip drugih pridruženih servisa tj. usluga (npr, prosleđivanje 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 biti zatražena i biće potrebna radi ustanovljavanja identiteta osobe u pitanju.

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

Takođe, podaci o pretplatniku nijesu ograničeni samo na inforamcije koje se odnose na direktnu upotrebu komunikacionih servisa. One takođe mogu podrazumijevati bilo koju informaciju, osim informacije 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 takođe mogu obuhvatiti i podatke gdje je određena komunikaciona oprema instalirana (kablovski modem), a koja informacija je na raspolaganju na osnovu ugovora o zasnivanju pretplatničkog odnosa i instalaciji navedenog uređaja od strane ovlašćenog servisnog lica internet servis provajdera, tj. preduzeća.

Pored informacije o mjestu i adresi gdje je navedena oprema instalirana, ovakva vrsta informacije je takođe bitna sa stanovištva utvrđivanja činjenice da takva vrsta opreme nije lako pomjerljiva, već da je na osnovu tehničkih pokazatelja u okviru rada navedenog preduzeća – Internet servis provajdera, potvrđeno da je takva vrsta opreme funkcionalna na adresi, na kojoj je ista i instalirana od strane ovlašćenih lica, shodno čemu je jasno da podaci koji se nalaze u ugovoru o zasnivanju pretplatničkog odnosa, odgovaraju realnom stanju stvari.

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

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

2. 6. Međunarodna saradnja

Konvencija o Sajber kriminalu Savjeta Evrope (CETS 185) u svom trećem poglavlju reguliše u članovima od 23.do 35. Međunarodnu pravnu pomoć u krivičnim stvarima u oblasti tzv. „sajber kriminaliteta". Konvencija u navedenim članovima, a posebno u uvodnim, naglašava i podvlači neophodnost proširenja međunarodne saradnje na najširi i najobuhvatniji mogući način. Praktično, Konvencija kroz uspostavljanje principa međunarodne saradnje omogućava uspostavljanje intenzivne i ekstezivne međusobne saradnje država i njenih organa i pokušava da umanji svaki negativni uticaj na brzine, ometanja i protok informacija i dokaza u međunarodnom okruženju.

Takođe, međunarodna saradnja bi trebalo da bude usmjerena i da obuhvata i sva krivična djela koja se odnose na računare i računarske sisteme, kao i podatke koji su generisani od strane računara, koji su upotrebljeni ili na drugi način iskorišćeni u toku računarske komunikacije kao i prikupljanje dokaza u elektronskoj formi u vezi izvršenja krivičnih djela. Ovo znači da, bez obzira da li je 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 sajber kriminala treba da bude u skladu sa odredbama ove Glave i kroz primjer, ali i kroz primjenu svih relevantnih međunarodnih sporazuma u vezi međunarodne saradnje 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.

2.6.1. 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 krivično pravna odgovornost njegovog počinioca bila onemogućena. Neki oblici računarskih podataka su pohranjeni samo u vrlo kratkom vremenskom periodu prije nego što budu obrisani, tj. učinjeni na drugi način trajno nedostupnim. U drugim slučajevima, značajna šteta može biti pričinjena kako ljudima, tako i imovini, ukoliko ova vrsta dokaza nije prikupljena vrlo brzo.

U takvim hitnim slučajevima, ne samo slanje zahtjeva na hitan način veći odgovor na hitan način, moraju biti omogućeni i izvršeni. Iz tog razloga, od krucijalne važnosti je omogućavanje ubrzavanja procesa ostvarivanja međunarodne pravne pomoći u krivičnim stvarima, upravo u cilju izbjegavanja gubitaka kritičnih informacija ili dokaza, koji bi, ukoliko ovakva vrsta i način postupanja i izvršenja ne bi bila preuzeta, 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 korišćenje složenih međunarodnih procedura. Ovakav način pružanja međunarodne pravne pomoći u oblasti visokotehnološkog kriminala praktično predstavlja jednu od glavnih, ako ne i glavnu prepreku usupješnom krivičnom gonjenju u ovoj oblasti kriminaliteta.

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

Iz tih razloga se korišćenje modernih sredstava komunikacije, kao što su elektronska pošta, faks, VOIP komunikacija, teleconferencing, upotreba direktne komunikacije i razmjene podataka putem mobilnih uređaja koji koriste Internet okruženje, itd. postavlja kao uslov bez koga se ne može postići željeni cilj.

Posebno je bitno naglasiti neophodnost praćenja razvoja informaciono-komunikacionih tehnologija i njihovo iskorišćavanje radi što brže razmjene podataka i komuniciranja prilikom ostvarivanja 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.

2.6.2. 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 tačke kontakta 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 kriminaliteta, tj. krivičnih djela koja su počinjena korišćenjem računarskih sistema i računara, kao i efektivno prikupljanje dokaza u elektronskoj formi.

Bitno je imati u vidu radnje koje preduzimamo za tastaturom našeg računara u toku, radnog vremena, skoro momentalno imaju posljedice na i u računarima, koji se nalaze možda desetinama hiljada kilometara daleko, u različitim vremenskim zonama. Iz ovih razloga postojanje već navedene klasične, tj. standardne saradnje i modeliteta saradnje u međunarodnoj pravnoj 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 takođe za potrebe saradnje te grupe zemalja formirala sličnu „24/7 mrežu" kontakata i saradnje, ukazala su na mogućnost uspostavljanja takvog modeliteta direktne saradnje u hitnim slučajevima na osnovu, kao i u okvirima ove Konvencije Savjeta Evrope.

Članom 35 ove Konvencije, svaka zemlja koja ju je ratifikovala ima obavezu da odredi tačku kontakta koja će biti na raspolaganju 24 časa dnevno, 7 dana u nedjelji, tokom cijele godine, radi omogućavanja hitnog, tj. momentalnog odgovora i pomoći u istragama, kao i procedurama međunarodne pravne pomoći. Zemlje koje su ratifikovale Konvenciju su se složile 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, „24/7" tačke kontakta, 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 osumnjičeno lice.

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

Razlog uspješnosti saradnje državnih, tj. državnih (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 strane istražnog odjeljenja-istražnog sudije suda, čime se znatno, sa jedne strane, ubrzava vođenje krivične istrage, dok sa druge strane, imajući u vidu kvalitet državnih tužilaštava u smislu njihovog autonomnog ili nezavisnog položaja u okviru pravosudne grane vlasti, omogućava da tužilaštva kroz svoje radnje kontrolišu radnje i mjere koje pripadnici ministarstava unutrašnjih poslova primjenjuju.

Ovo posebno stoga što se u stavu 2 člana 35 Konvencije navodi da je jedan od ključnih zadataka koje kontakt tačke ove mreže treba da ispune upravo mogućnost uspostavljanja brzog izvršenja onih funkcija i zadataka koji su neophodni radi brzog postupanja u ovoj krivično pravnoj materiji. Npr, 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 krivično pravnog sistema svoje zemlje, kao što su npr. ovlašćeno 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. Takođe, ne treba zanemariti ni potrebu da tačka kontakta ima takav kapacitet da na najbrži mogući način izvrši komunikaciju sa drugim članicama, tj. drugim kontakt tačkama ove mreže na najbrži mogući način.

2. 7. Direktiva 2013/40/EU

Direktiva 2013/40/EU je donijeta od strane Evropskog parlamenta 20.avgusta 2013. godine i odnosi se na napade usmjerene protiv informacionih sistema. Direktiva mijenja okvirnu odluku Savjeta 2005/222/JHA i predstavlja sastavni dio tzv. „ACQUI COMMUNAUTAIRE“ -zajedničkog 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 krivično-pravnih 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, EUROPO ili njegov Evropski centar za Sajber krajm (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 korišćenja navedenih sistema. Neometana upotreba takvih sistema, kao i njihova sigurnost u okviru zemalja članica Unije je od vitalnog 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 predstavljaju 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 djelove kritične infrastrukture, te bi prekidanje rada ili uništenje ovakve vrste infrastrukture imalo za posljedicu nanošenje značajne štete kako direktno žiteljima 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 i 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 propraćena i razvojem sofisticiranih metoda, kao što su proizvodnja i korišćenje tzv. „botnetova", 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 korišćenja tzv. „botnetova", kao čin uspostavljanja udaljene kontrole nad značajnim brojem računara putem inficiranja istih kroz instalaciju malicioznog softvera, a kroz precizno usmjerene sajber napade. Jednom kad se takva mreža kreira ona konstituiše „botnet" koji može biti aktiviran bez znanja i pristanka 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 i gubitak ili izmjenu komercijalno bitnih povjerljivih informacija i podataka. Posebna pažnja treba da bude usmjerena ka podizanju svijesti malih i srednjih kompanija i preduzeća u cilju identifikacije ovakve vrste opasnosti, kao i ranjivosti tih preduzeća u ovom smislu, a kroz njihovu rastuću

zavisnost od korišćenja informacionih sistema. Bitno je takođe 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 sa njihovim nacionalnim zakonodavstvima i praksom. Na primjer, 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 krivično-pravne 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 krivično-pravne sankcije i njihovu visinu, kao i unapređenje saradnje među pravosudnim i drugim nadležnim organima, a što sve ne može biti postignuto samo od strane pojedinačnih zemalja članica, već bi trebalo da bude postignuto na nivou same Evropske Unije, iz kojih razloga Unija može ostvariti takve vrste mjera, koje su u skladu sa principom supsidijariteta koje je propisano članom 5. Ugovora o Evropskoj Uniji.

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

- **„Pravno lice“** predstavlja entitet koji ima status pravnog lica pod primjenjivim zakonom, ali ne uključuje države, tj. državne ili javne organe, institutcije 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 presrijetanje, kojim nije ovlašćen od strane vlasnika ili drugog ovlašćenog nosioca određenog prava na sistemu ili dijelu istog, ili nije dozvoljeno na osnovu domaćeg zakonodavstva.

U svom daljem tekstu Direktiva daje elemente bića krivičnog djela neovlašćeni pristup informacionom sistemu, neovlašćeno ometanje sistema, neovlašćeno ometanje podataka, korišćenje 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 za navedena krivična djela bude zaprijećena kazna zatvora sa najdužim rokom trajanja od najmanje 2 godine, i to za krivična djela koja se ne smatraju manje društveno opasnim.

Takođe, za krivična djela neovlašćenog ometanja sistema i neovlašćenog

ometanja podataka kada su učinjena sa umišljajem, moraju biti zaprijećena sa maksimumom od najmanje 3 godine, kada je došlo do značajnijeg oštećenja informacionog sistema i njihovog broja kroz korišćenje alata na koje se odnosi član 7 Direktive, tj. uređaja i programa koji su dizajnirani ili adaptirani prevashodno u tu svrhu.

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

- su ovakva krivična djela izvršena od strane 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;
- 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 Savjetu u okviru kog će postojati procjena primjene ove Direktive od strane zemalja članica, u smislu da li su preduzele neophodne mjere radi poštovanja Direktive, i ukoliko je to potrebno, dostavljanje zakonodavnih prijedloga. Komisija će, takođe, uzeti u obzir i tehnički i pravni razvoj u oblasti sajber kriminala, posebno imajući u vidu obuhvat ove Direktive.

III ZAKONODAVNI OKVIR U OKRUŽENJU - REPUBLIKA SRBIJA

3.1. Zakon o potvrđivanju Konvencije o Sajber kriminalu (2009)

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

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

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

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala predstavlja specifičnost Republike Srbije i primjenjuje se radi otkrivanja, krivičnog gonjenja i suđenja za krivična djela protiv bezbjednosti računarskih podataka, intelektualne svojine, imovine, privrede i pravnog saobraćaja, kod kojih se kao objekat ili sredstvo

izvršenja krivičnih djela javljaju računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj primjeraka autorskih djela prelazi 2000 ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara; krivična djela protiv sloboda i prava čovjeka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbjednosti Republike Srbije, koja se zbog načina izvršenja ili upotrijebljenih sredstava mogu smatrati krivičnim djelima visokotehnološkog kriminala.

Krivični zakonik Republike Srbije propisuje krivična djela protiv bezbjednosti računarskih podataka čije je krivično gonjenje u isključivoj nadležnosti Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala, kao i ostala krivična djela iz nadležnosti ovog tužilaštva. Takođe, definiše značenje izraza od važnosti za visokotehnološki kriminal.

Zakonik o krivičnom postupku utvrđuje pravila čiji je cilj da niko nevin ne bude osuđen, da se učiniocu krivičnog djela izrekne krivična sankcija pod uslovima koje propisuje Krivični zakon, na osnovu zakonito i pravično sprovedenog postupka.

Bitno je napomenuti da Zakonik propisuje i niz posebnih dokaznih radnji koje se mogu primijeniti u krivičnim postupcima protivu činilaca krivičnih djela iz stvarne nadležnosti Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala. Takođe, definiše značenje izraza od važnosti za visokotehnološki kriminal.

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

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

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

Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine uređuje posebna ovlašćenja organa državne

uprave i organizacija koje vrše javna ovlašćenja radi efikasne zaštite prava intelektualne svojine u skladu sa propisima kojima se uređuje pravo intelektualne svojine.

3.1.1. Podzakonski akti

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

Pravilnik o uslovima za pružanje usluga prenosa govora korišćenjem Interneta i sadržaja odobrenja je takođe usvojen od strane Republičke agencije za telekomunikacije. Propisuje uslove neophodne za pružanje usluga prenosa govora korišćenjem Interneta (VoIP), na komercijalnoj osnovi i bez dodjeljivanja posebnih brojeva operatoru za potrebe krajnjih korisnika.

3. 2. Institucionalni okvir

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

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

Takođe, odredbom Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, u okviru Ministarstva unutrašnjih poslova, obrazovana je **Služba za borbu protiv visokotehnološkog kriminala** koja postupa po nalozima Posebnog tužioca za visokotehnoški kriminal.

Značajnu ulogu u ovoj oblasti ima i **Ministarstvo spoljne i unutrašnje trgovine i telekomunikacija**, tako što doprinosi usklađivanju domaćih propisa u oblasti elektronskih komunikacija sa odgovarajućim propisima Evropske unije; Preduzima mjere za podsticanje istraživanja i razvoja u oblasti elektronskih komunikacija, u saradnji sa ministarstvom nadležnim za poslove razvoja i unapređenja naučno-istraživačke djelatnosti;

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

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

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

IV UPOREDNA ANALIZA ODREDBI KONVENCIJE O SAJBER KRIMINALU I PRAVNOG OKVIRA U REPUBLICI SRBIJI

4.1. Značenje pojmova računarski sistem, računarski podaci, davalac usluga, promet podataka

4.1.1. U članu 1. Konvencije određeno je značenje pojmova "računarski sistem", "računarski podaci", "davalac usluga", "promet podataka".

Krivični zakonik Republike Srbije određuje ove pojmove u članu 112 - Značenje izraza u ovom zakoniku na sljedeći način:

- Pokretnom stvari se smatra i svaka proizvedena ili sakupljena energija za davanje svjetlosti, toplote ili kretanja, telefonski impuls, kao i računarski podatak i računarski program.
- Računarski podatak je svako predstavljanje činjenica, informacija ili koncepta u obliku koji je podesan za njihovu obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski sistem obavlja svoju funkciju.
- Računarskom mrežom smatra se skup međusobno povezanih računara, odnosno računarsih sistema koji komuniciraju razmjenjujući podatke.
- Računarskim programom smatra se uređeni skup naredbi koje služe za upravljanje radom računara, kao i za rješavanje određenog zadatka pomoću računara.
- Računarski virus je računarski program ili neki drugi skup naredbi unijet u računar ili računarsku mrežu koji je napravljen da sam sebe umnožava i djeluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka.
- I spravom se smatra svaki predmet koji je podoban ili određen da služi kao dokaz kakve činjenice koja ima značaj za pravne odnose, kao i računarski podatak.
- Spis, pismo, pošiljka i dokument mogu biti i u elektronskom obliku.

- Računar je svaki elektronski uređaj koji na osnovu programa automatski obrađuje i razmjenjuje podatke.
- Računarski sistem je svaki uređaj ili grupa međusobno povezanih ili zavisnih uređaja od kojih jedan ili više njih, na osnovu programa, vrši automatsku obradu podataka.

Zakonik o krivičnom postupku u članu 2 određuje značenje izraza na sljedeći način:

- elektronski zapis je zvučni, video ili grafički podatak dobijen u elektronskom (digitalnom) obliku;
- elektronska adresa je niz znakova, slova, cifara i signala koji je namijenjen za određivanje odredišta veze;
- elektronski dokument je skup podataka koji je određen kao elektronski dokument u skladu sa zakonom koji uređuje elektronski dokument.

4.1.2. Konvencija u članovima 2 i 3 određuje elemente potrebne za definisanje krivično-pravnih normi u vezi nezakonitog pristupa i neovlašćenog presretanja.

Krivični zakonik Republike Srbije, ove norme reguliše i sankcioniše u članu 302 "Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka" na sljedeći način:

(1) Ko se, kršeći mjere zaštite, neovlašćeno uključi u računar ili računarsku mrežu, ili neovlašćeno pristupi elektronskoj obradi podataka, kazniće se novčanom kaznom ili zatvorom do šest (6) mjeseci.

(2) Ko snimi ili upotrijebi podatak dobijen na način predviđen u stavu 1. ovog člana, kazniće se novčanom kaznom ili zatvorom do dvije (2) godine.

(3) Ako je usljed djela iz stava 1. ovog člana došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili mreže ili su nastupile druge teške posljedice, učinilac će se kazniti zatvorom do tri (3) godine.

4.1.3. Konvencija u članovima 4 i 5 određuje elemente potrebne za definisanje krivično pravnih normi u vezi ometanja podataka i ometanja sistema.

Krivični zakonik, Republike Srbije, to čini u članu 299 **"Računarska sabotaža"** na sljedeći način:

Ko unese, uništi, izbriše, izmijeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program ili uništi ili ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka sa namjerom da onemogući ili znatno omete postupak elektronske obrade i prenosa

podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte, kazniće se zatvorom od šest (6)mjeseci do pet (5) godina.

4.1.4. Članom 6. Konvencije određeni su elementi koji se odnose na zloupotrebu uređaja u kontekstu informaciono-komunikacionih tehnologija.

Krivični zakonik, Republike Srbije, u članu 304a "**Pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih djela protiv bezbjednosti računarskih podataka"** normu i sankciju određuje na sljedeći način:

(1) Ko posjeduje, pravi, nabavlja, prodaje ili daje drugom na upotrebu računare, računarske sisteme, računarske podatke i programe radi izvršenja krivičnog djela iz čl.298. do 303.ovog Zakonika, kazniće se zatvorom od šest (6) mjeseci do tri (3)godine.

(2) Predmeti iz stava 1. Ovog člana oduzeće se.

4.1.5. Falsifikovanje u vezi sa računarima je opisano u članu 7 Konvencije Savjeta Evrope CETS 185.

Krivični zakonik, Republike Srbije, to čini u članu 355 **"Falsifikovanje isprave"**na sljedeći način:

(1) Ko napravi lažnu ili preinači pravu ispravu u namjeri da se takva isprava upotrijebi kao prava ili ko lažnu ili neistinitu ispravu upotrebi kao pravu ili je nabavi radi upotrebe, kazniće se zatvorom do tri (3) godine.

(2) Ako je djelo iz stava 1. ovog člana učinjeno u pogledu javne isprave, testamenta, mjenice, čeka, javne ili službene knjige ili druge knjige koja se mora voditi na osnovu zakona, učinilac će se kazniti zatvorom od tri (3) mjeseca do pet (5) godina.

(3) Za pokušaj djela iz stava 1. ovog člana kazniće se.

Takođe u članu 356 **"Posebni slučajevi falsifikovanja isprave"** stoji da:

Smatraće se da čini djelo falsifikovanja isprave, kazniće se po članu 355 ovog Zakonika:

(1) ko hartiju, blanket ili drugi predmet na kojem je neko lice stavilo svoj potpis neovlašćeno popuni izjavom koja ima vrijednost za pravne odnose;

(2) ko drugog obmane o sadržaju isprave i ovaj stavi svoj potpis na tu ispravu, smatrajući da se potpisuje pod drugu ispravu ili pod drugi sadržaj;

(3) ko ispravu izda u ime drugog lica bez njegovog ovlašćenja ili u ime lica koje ne postoji;

(4) ko kao izdavalac isprave uz svoj potpis stavi da ima položaj ili čin ili zvanje i ako nema takav položaj, čin ili zvanje, a ovo ima bitni uticaj na dokaznu snagu isprave;

(5) ko ispravu načini na taj način što neovlašćeno upotrijebi pravi pečat ili znak. Takođe, Krivični zakonik u članu 112, **"Značenje izraza u ovom zakoniku"** propisuje vrlo bitno određenje pojmova koji u mnogome razjašnjavaju i pomažu prilikom otkrivanja i gonjenja krivičnih djela i njihovih počinilaca u oblasti računarskog kriminaliteta, i to na sljedeći način:

"Ispravom se smatra svaki predmet koji je podoban ili određen da služi kao dokaz kakve činjenice koja ima značaj za pravne odnose, kao i računarski podatak".

4.1.6. Prevara u vezi sa računarima je opisana u članu 8 Konvencije.

Krivični zakonik RS u članu 301 **"Računarska prevara",** to čini na sljedeći način:

(1) Ko unese netačan podatak, propusti unošenje tačnog podatka ili na drugi način prikrije ili lažno prikaže podatak i time utiče na rezultat elektronske obrade i prenosa podataka u namjeri da sebi ili drugom pribavi protiv pravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, kazniće se novčanom kaznom ili zatvorom do tri (3) godine.

(2) Ako je djelom iz stava 1 ovog člana pribavljena imovinska korist koja prelazi iznos od četiristo pedeset hiljada dinara, učinilac će se kazniti zatvorom od jedne do osam godina.

(3) Ako je dijelom iz stava 1 ovog člana pribavljena imovinska korist koja prelazi iznos od milion i petsto hiljada dinara, učinilac će se kazniti zatvorom od dvije do deset (2-10) godina.

(4) Ko djelo iz stava 1 ovog člana učini samo u namjeri da drugog ošteti, kazniće se novčanom kaznom ili zatvorom do šest mjeseci.

4.1.7. Član 9 Konvencije propisuje djela u vezi sa dječijom pornografijom.

Krivični zakonik Srbije to čini u članu 185 p*rikazivanje, pribavljanje i posjedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju*:

(1) Ko maloljetniku proda, prikaže ili javnim izlaganjem ili na drugi način učini dostupnim tekstove, slike, audio-vizuelne ili druge predmete pornografske sadržine ili mu prikaže pornografsku predstavu,

kazniće se novčanom kaznom ili zatvorom do šest mjeseci.

(2) Ko iskoristi maloljetnika za proizvodnju slika, audio-vizuelnih ili drugih predmeta pornografske sadržine ili za pornografsku predstavu, kazniće se zatvorom od šest mjeseci do pet godina.

(3) Ako je djelo iz st.1 i 2 ovog člana izvršeno prema djetetu, učinilac će se kazniti za delo iz stava 1. zatvorom od šest meseci do tri godine, a za djelo iz stava 2 zatvorom od jedne do osam godina.

(4) Ko pribavlja za sebe ili drugog, posjeduje, prodaje, prikazuje, javno izlaže ili elektronski ili na drugi način čini dostupnim slike, audio-vizuelne ili druge predmete pornografske sadržine nastale iskorišćavanjem maloletnog lica, kazniće se zatvorom od tri mjeseca do tri godine.

(5) Predmeti iz st.1 do 4 ovog člana oduzeće se.

Srodno krivično djelo je i *iskorišćavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih djela protiv polne slobode prema maloljetnom licu - Član 185 b*

(1) Ko u namjeri izvršenja krivičnog djela iz čl.178 stav 4, 179 stav 3, 180. st.1. i 2, 181 st.2 i 3, 182 stav 1, 183 stav 2, 184 stav 3, 185 stav 2. i 185a ovog zakonika, koristeći računarsku mrežu ili komunikaciju drugim tehničkim sredstvima dogovori sa maloljetnikom sastanak i pojavi se na dogovorenom mjestu radi sastanka, kazniće se zatvorom od šest mjeseci do pet godina i novčanom kaznom.

(2) Ko djelo iz stava 1 ovog člana izvrši prema djetetu, kazniće se zatvorom od jedne do osam godina.

Bitno je napomenuti da Zakon o potvrđivanju konvencije Savjeta Evrope o zaštiti djece od seksualnog iskorišćavanja i seksualnog zlostavljanja u članu 20 propisuje krivična djela u vezi sa dječijom pornografijom.

4.1.8. Član 10 Konvencije razmatra djela u vezi sa kršenjem autorskih prava, dok se u Krivičnom zakoniku Republike Srbije ovo značajno poglavlje reguliše kroz sljedeća krivična djela:

Povreda moralnih prava autora i interpretatora *- Član 198*

(1) Ko pod svojim imenom ili imenom drugog u cjelini ili djelimično objavi, stavi u promet primjerke tuđeg autorskog djela ili interpretacije, ili na drugi način javno saopšti tuđe autorsko djelo ili interpretaciju, kazniće se novčanom kaznom ili zatvorom do tri godine.

(2) Ko bez dozvole autora izmijeni ili preradi tuđe autorsko djelo ili izmijeni tuđu snimljenu interpretaciju, kazniće se novčanom kaznom ili zatvorom do jedne godine.

(3) Ko stavlja u promet primjerke tuđeg autorskog djela ili interpretacije

na način kojim se vređa čast ili ugled autora ili izvođača, kazniće se novčanom kaznom ili zatvorom do šest mjeseci.

(4) Predmeti iz st.1 do 3 ovog člana oduzeće se.

(5) Gonjenje za djelo iz stava 2 ovog člana preduzima se po prijedlogu, a za djelo iz stava 3 ovog člana po privatnoj tužbi.

Neovlašćeno iskorišćavanje autorskog djela ili predmeta srodnog prava *- Član 199*

(1) Ko neovlašćeno objavi, snimi, umnoži, ili na drugi način javno saopšti u cjelini ili djelimično autorsko djelo, interpretaciju, fonogram, videogram, emisiju, računarski program ili bazu podataka, kazniće se zatvorom do tri godine.

(2) Kaznom iz stava 1 ovog člana kazniće se i ko stavi u promet ili u namjeri stavljanja u promet drži neovlašćeno umnožene ili neovlašćeno stavljene u promet primjerke autorskog djela, interpretacije, fonograma, videograma, emisije, računarskog programa ili baze podataka.

(3) Ako je djelo iz st.1 i 2 ovog člana učinjeno u namjeri pribavljanja imovinske koristi za sebe ili drugog, učinilac će se kazniti zatvorom od šest mjeseci do pet godina.

(4) Ko proizvede, uveze, stavi u promet, proda, da u zakup, reklamira u cilju prodaje ili davanja u zakup ili drži u komercijalne svrhe uređaje ili sredstva čija je osnovna ili pretežna namijena uklanjanje, zaobilaženje ili osujećivanje tehnoloških mjera namijenjenih sprječavanju povreda autorskih i srodnih prava, ili ko takve uređaje ili sredstva koristi u cilju povrede autorskog ili srodnog prava, kazniće se novčanom kaznom ili kaznom zatvora do tri godine.

(5) Predmeti iz st.1 do 4 ovog člana oduzeće se i uništiti.

Neovlašćeno uklanjanje ili mijenjanje elektronske informacije o autorskom i srodnim pravima *- Član 200*

(2) Predmeti iz stava 1. oduzeće se i uništiti.

Povreda pronalazačkog prava *- Član 201*

(1) Ko neovlašćeno proizvodi, uvozi, izvozi, nudi radi stavljanja u promet, stavlja u promet, skladišti ili koristi u privrednom prometu proizvod ili postupak zaštićen patentom, kazniće se novčanom kaznom ili zatvorom do tri godine.

(2) Ako je djelom iz stava 1 ovog člana pribavljena imovinska korist ili prouzrokovana šteta u iznosu kojiprelazi milion dinara, učinilac će se kazniti zatvorom od jedne do osam godina.

(3) Ko neovlašćeno objavi ili na drugi način učini dostupnim suštinu tuđeg prijavljenog pronalaska prije nego što je ovaj pronalazak

objavljen na način utvrđen zakonom, kazniće se novčanom kaznom ili zatvorom do dvije godine.

(4) Ko neovlašćeno podnese prijavu patenta ili u prijavi ne navede ili lažno navede pronalazača, kazniće se zatvorom od šest mjeseci do pet godina.

(5) Predmeti iz st.1 i 2 oduzeće se i uništiti.

Neovlašćeno korišćenje tuđeg dizajna *- Član 202*

(1) Ko na svom proizvodu u prometu neovlašćeno upotrijebi, u cjelosti ili djelimično, tuđi prijavljeni, odnosno zaštićeni dizajn proizvoda, kazniće se novčanom kaznom ili zatvorom do tri godine.

(2) Ko neovlašćeno objavi ili na drugi način učini dostupnim javnosti predmet prijave tuđeg dizajna prije nego što je objavljen na način utvrđen zakonom, kazniće se novčanom kaznom ili zatvorom do jedne godine.

(3) Proizvodi iz stava 1 ovog člana oduzeće se.

Takođe, Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine u svom članu 15 predviđa sljedeće mjere koje mogu preduzeti nadležni državni organi:

(1) Nadležni organ, ako neposrednim uvidom utvrdi da je povrijeđeno pravo intelektualne svojine, na licu mjesta po službenoj dužnosti:

1. privremeno oduzima svu zatečenu robu, odnosno sve proizvode koji su predmet ili sredstvo povrede prava intelektualne svojine;
2. izriče mjeru privremene zabrane obavljanja djelatnosti kojom se povređuje pravo intelektualne svojine.

Privredni prestup *- član 39*

Izricanje novčane kazne pravnom licu i odgovornom licu i pravnom licu za privredni prestup ako neovlašćeno proizvodi, uvozi, izvozi, nudi radi stavljanja u promet, stavlja upromet, skladišti ili koristi u komercijalne svrhe proizvod ili postupak zaštićen patentom, odnosno malim patentom.

4.1.9. Članom 11 Konvencije regulisani su oblici saizvršilaštva kroz pokušaj, pomaganje ili podstrekavanje.

Krivični zakonik Republike Srbije to čini u sljedećim članovima:

Pokušaj *– član 30*

(1) Ko sa umišljajem započne izvršenje krivičnog djela, ali ga ne dovrši, kazniće se za pokušaj krivičnog dela za koje se po zakonu može izreći kazna zatvora od pet godina ili teža kazna, a za pokušaj drugog krivičnog djela samo kad zakon izričito propisuje kažnjavanje i za pokušaj.

(2) Učinilac će se za pokušaj kazniti kaznom propisanom za krivično djelo, ili ublaženom kaznom.

Podstrekavanje *– član 34*

(1) Ko drugog sa umišljajem podstrekava da izvrši krivično djelo, kazniće se kaznom propisanom za to krivično djelo.

(2) Ko drugog sa umišljajem podstrekava na izvršenje krivičnog djela čiji pokušaj je po zakonu kažnjiv, a djelo ne bude ni pokušano, kazniće se kao za pokušaj krivičnog djela.

Pomaganje *– član 35*

(1) Ko drugom sa umišljajem pomogne u izvršenju krivičnog djela, kazniće se kaznom propisanom za to krivično djelo, ili ublaženom kaznom.

(2) Kao pomaganje u izvršenju krivičnog djela smatra se naročito: davanje savjeta ili uputstava kako da se izvrši krivično djelo, stavljanje učiniocu na raspolaganje sredstava za izvršenje krivičnog djela, stvaranje uslova ili otklanjanje prepreka za izvršenje krivičnog djela, kao unaprijed obećano prikrivanje krivičnog djela, učinioca, sredstava kojima je krivično djelo izvršeno, tragova krivičnog djela ili predmeta pribavljenih krivičnim djelom.

4.2. Odgovornost pravnog lica

4.2.1. Odgovornost pravnog lica, relativni novitet na našim prostorima, regulisan je članom 12 Konvencije.

U Republici Srbiji na snazi je Zakon o odgovornosti pravnih lica za krivična djela:

Osnov odgovornosti*- član 6*

Pravno lice odgovara za krivično djelo koje u okviru svojih poslova, odnosno ovlašćenja učini odgovorno lice u namjeri da za pravno lice ostvari korist.

Odgovornost pravnog lica iz st.1 postojii ako je zbog nepostojanja nadzora ili kontrole od strane odgovornog lica omogućeno izvršenje krivičnog djela u korist pravnog lica od strane fizičkog lica koje djeluje pod nadzorom i kontrolom odgovornog lica.

Takođe, Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine predviđa i postojanje privrednog prestupa u članu 39 na sljedeći način:

"Izricanje novčane kazne pravnom licu i odgovornom licu u pravnom licu za privredni prestup ako neovlašćeno proizvodi, uvozi, izvozi, nudi radi stavljanja u promet, stavlja u promet, skladišti ili koristi u komercijalne

svrhe proizvod ili postupak zaštićen patentom, odnosno malim patentom".

4.2.2. Procesno-pravni instituti koji nijesu u potpunosti i na identičan način implementirani u zakonodavstvu Srbije su Hitna zaštita sačuvanih računarskih podataka (čl.16) i Hitna zaštita i djelimično otkrivanje podataka o saobraćaju (čl.17) Konvencije.

Zakon o elektronskim komunikacijama ovo pitanje reguliše na sljedeći način:

***Obaveza zadržavanja podataka**- član 128*

Operator je dužan da zadrži podatke o elektronskim komunikacijama za potrebe sprovođenja istrage, otkrivanja krivičnih djela i vođenja krivičnog postupka, kao i za potrebe zaštite nacionalne i javne bezbjednosti Republike Srbije.

Operator je dužan da zadržane podatke čuva 12 mjeseci od dana obavljene komunikacije.

Operator je dužan da zadržava podatke tako da im se bez odlaganja može pristupiti, odnosno da se bez odlaganja mogu dostaviti.

Shodno čl.126 ovog zakona, obaveza operatora odnosi se na podatke potrebne za:

1. praćenje i utvrđivanje izvora komunikacije;
2. utvrđivanje odredišta komunikacije;
3. utvrđivanje početka, trajanja izavršetka komunikacije;
4. utvrđivanje vrste komunikacije;
5. identifikaciju terminalne opreme korisnika;
6. utvrđivanje lokacije mobilne terminalne opreme korisnika.

Obaveza zadržavanja podataka iz stava 1. ovog člana obuhvata ipodatke o uspostavljenim pozivima koji nijesu odgovoreni, ali ne obuhvata podatke o pozivima čije uspostavljanje nije uspjelo.

Zabranjeno je zadržavanje podataka koji otkrivaju sadržaj komunikacije.

***Zakonito presretanje elektronskih komunikacija**- član 127*

Operator je dužan da omogući zakonito presretanje elektronskih komunikacija.

Nadležni državni organ koji sprovodi poslove zakonitog presretanja dužan je da vodi evidenciju o presretnutim elektronskim komunikacijama, koja naročito sadrži određenje akta koji predstavlja pravni osnov za vršenje presretanja, datum i vrijeme vršenja presretanja, kao i da ovu evidenciju čuva kao tajnu, u skladu sa zakonom kojim se uređuje tajnost podataka.

Članom 17 b) Konvencije predviđeno je da nadležni organi strane ugovornice ili lica koje ti organii mijenuju, mogu hitno da otkriju količinu podataka o saobraćaju, koja je dovoljna za identifikaciju davaoca usluga i putanje kojim je saobraćaj izvršen, što je u Srbiji moguće u skladu sa *Zakonom o međunarodnoj pravnoj pomoći u krivičnim stvarima*

4.2.3. Članom 18 Konvencije je regulisano izdavanje naredbe odstrane nadležnog državnog organa. Zakonik o krivičnom postupku propisuje ovlašćenja javnog tužioca. Takođe, Zakon o elektronskim komunikacijama u svojim odredbama takođe predviđa preduzimanje određenih mjera ovog karaktera.

Postupanje javnog tužioca po krivičnoj prijavi *- član 282.*

Ako javni tužilac iz same krivične prijave ne može ocijeniti da li su vjerovatni navodi prijave ili ako podaci u prijavi ne pružaju dovoljno osnova da može odlučiti da li će sprovesti istragu ili ako je na drugi način saznao da je izvršeno krivično djelo, javni tužilac može:

1. sam prikupiti potrebne podatke;
2. pozivati građane
3. podnijeti zahtjev državnim i drugim organima i pravnim licima da mu pruže potrebna obavještenja.

Za nepostupanje po zahtjevu javnog tužioca člana odgovorno lice se može novčano kazniti do 150.000 dinara, a ako i poslije toga odbije da da potrebne podatke, može se još jednom kazniti istom kaznom.

4.2.4. Članom 19 Konvencije propisane su krivčnopravne procesne odredbe u vezi sa pretraživanjem i zaplenom sačuvanih računarskih podataka.

Zakonik o krivičnom postupku Srbije to čini u članovima 147, 148 i 152 na sljedeći način:

Privremeno oduzimanje predmeta *–član 147*

Predmete koji se po Krivičnom zakoniku moraju oduzeti ili koji mogu poslužiti kao dokaz u krivičnom postupku, organ postupka će privremeno oduzeti i obezbijediti njihovo čuvanje.

Odluku o privremenom oduzimanju sredstava koja su predmet sumnjive transakcije (član 145) i njihovom stavljanju na poseban račun radi čuvanja donosi sud.

U predmete iz stava 1. ovog člana spadaju i uređaji za automatsku obradu podataka i uređaji i oprema na kojoj se čuvaju ili se mogu čuvati elektronski zapisi.

Dužnost držaoca predmeta *- Član 148.*

Lice koje drži predmete iz člana 147 st.1 i 2 ovog zakonika dužno je da organu postupka omogući pristup predmetima, pruži obavještenja potrebna za njihovu upotrebu i da ih na zahtjev organa preda. Prije oduzimanja predmeta organ postupka će po potrebi u prisustvu stručnog lica pregledati predmete.

Pretresanje*- član 152*

Pretresanje stana i drugih prostorija ili lica može se preduzeti ako je vjerovatno da će se pretresanjem pronaći okrivljeni, tragovi krivičnog djela ili predmeti važni za postupak.

Pretresanje stana i drugih prostorija ili lica se preduzima na osnovu naredbe suda ili izuzetno bez naredbe, na osnovu zakonskog ovlašćenja.

Pretresanje uređaja za automatsku obradu podataka i opreme na kojoj se čuvaju ili se mogu čuvati elektronski zapisi preduzima se na osnovu naredbe suda i, po potrebi, uz pomoć stručnog lica.

4.2.5. Član 20 Konvencije - prikupljanje podataka o saobraćaju u realnom vremenu, u nedostatku sadržajnije i jasnije norme, u praksi potpada pod primjenu ne tako jasnog i, možda, ne potpuno pravilno primijenjenog instituta računarskog pretraživanja podataka:

Računarsko pretraživanje podataka - član 178.

Ako su ispunjeni uslovi iz člana 161 st.1 i 2 ovog Zakonika, na obrazloženi prijedlog javnog tužioca sud može odrediti računarsko pretraživanje već obrađenih ličnih i drugih podataka i njihovo poređenje sa podacima koji se odnose na osumnjičenog i krivično djelo.

U skladu sa odredbom član 179 ZKP, ovu posebnu dokaznu radnju određuje sudija za prethodni postupak obrazloženom naredbom.

Primjena ovog člana Zakonika i njegovo tumačenje kako od strane tužilaca i sudija, tako i od strane drugih državnih institucija, posebno Povjerenika za informacije od javnog značaja i zaštitu podataka o ličnosti, ovih dana je predmet živih stručnih polemika, posebno imajući u vidu da usko tumačenje primjene može dovesti do svojevrsne blokade rada organa otkrivanja i gonjenja.

4.2.6. Članom 21 regulisano je standardno presretanje podataka o sadržaju komunikacije, koje je Zakonikom o krivičnom postupku propisano članovima 166, 167 i 168.

***Tajni nadzor komunikacije**- član 166*

Ako su ispunjeni uslovi iz člana 161 st.1 i 2 ovog Zakonika, na obrazloženi prijedlog javnog tužioca sud može odrediti nadzor i snimanje komunikacije koja se obavlja putem telefona ili drugih tehničkih sredstava ili nadzor elektronske ili druge adrese osumnjičenog i zaplenu pisama i drugih pošiljki.

***Naredba o tajnom nadzoru komunikacije** - član 167.*

Posebnu dokaznu radnju iz člana 166 ovog Zakonika određuje sudija za prethodni postupak obrazloženom naredbom.

***Sprovođenje tajnog nadzora komunikacije** - član 168.*

Poštanska, telegrafska i druga preduzeća, društva i lica registrovana za prenošenje informacija dužna su da državnom organu koji izvršava naredbu, omoguće sprovođenje nadzora i snimanja komunikacije i da, uz potvrdu prijema, predaju pisma i druge pošiljke.

Članom 35 Konvencije propisuju se razlozi, uslovi i način rada kontakt tačaka Mreže 24/7 za brzu međunarodnu saradnju i pravnu pomoć u krivičnim stvarima iz oblasti "sajber" kriminaliteta.

Srbija i Crna Gora direktno primjenjuju ovaj član kroz određivanje kontakt tačaka u skladu sa Konvencijom, te pružanju uslova i omogućavanju pravilnog funkcionisanja kroz obezbjeđivanje odgovarajućih ljudskih i tehničkih resursa.

4.2.7. Član 22 Konvencije -nadležnost:

Krivični Zakonik-*Važenje krivičnog zakonodavstva na teritoriji Srbije – član 6*

(1) Krivično zakonodavstvo Republike Srbije važi za svakog ko na njenoj teritoriji učini krivično djelo.

(2) Krivično zakonodavstvo Srbije važi i za svakog ko učini krivično djelo na domaćem brodu, bez obzira gdje se brod nalazi u vrijeme izvršenja djela.

(3) Krivično zakonodavstvo Srbije važi i za svakog ko učini krivično djelo u domaćem civilnom vazduhoplovu dok je u letu ili u domaćem vojnom vazduhoplovu, bez obzira gdje se vazduhoplov nalazio u vrijeme izvršenja krivičnog djela.

(4) Ako je u slučajevima iz st.1 do 3 ovog člana u stranoj državi pokrenut ili dovršen krivični postupak, krivično gonjenje u Srbiji preduzeće se samo po odobrenju republičkog javnog tužioca.

(5) Krivično gonjenje stranca u slučajevima iz st.1 do 3 ovog člana može se, pod uslovom uzajamnosti, ustupiti stranoj državi.

4.2.8. Član24 Konvencije - ekstradicija

Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima *-Izručenje okrivljenog ili osuđenog - članovi 13-37.*

Predmet izručenja*- član 13*

Izručenje okrivljenog ili osuđenog stranoj državi dozvoljava se:

1. radi vođenja krivičnog postupka za krivično djelo za koje se prema zakonu Republike Srbije i zakonu države, molilje, može izreći kazna zatvora od godinu dana ili teža kazna;
2. radi izvršenja krivične sankcije koju je sud države, molilje, izrekao za krivično djelo iz tačke 1) ovog stava u trajanju od najmanje četiri mjeseca.

Ako se zamolnica odnosi na više krivičnih djela od kojih pojedina ne ispunjavaju uslove iz stava 1 ovog člana, izručenje se može dozvolitii za ova krivična djela.

Pretpostavke za izručenje *- član 16*

Pored pretpostavki predviđenih članom 7 ovog zakona, pretpostavke za izručenje su:

1. da lice čije se izručenje zahtijeva nije državljanin Republike Srbije;
2. da djelo povodom kojeg se zahtijeva izručenje nije izvršeno na teritoriji Republike Srbije, protiv nje ili njenog državljanina;
3. da se protiv istog lica u Republici Srbiji ne vodi krivični postupak zbog krivičnog djela povodom kojeg se zahtijeva izručenje;
4. da po domaćem zakonu postoje uslovi za ponavljanje krivičnog postupka za krivično djelo povodom kojeg se zahtijeva izručenje lica protiv kojeg je pravnosnažno okončan postupak pred domaćim sudom;
5. da je utvrđena istovjetnost lica čije se izručenje zahtijeva;
6. da ima dovoljno dokaza za osnovanu sumnju odnosno da postoji pravnosnažna sudska odluka da je lice čije se izručenje traži učinilo krivično djelo povodom kojeg se zahtijeva izručenje;
7. da država, molilja, da garancije da će u slučaju osude u odsustvu postupak biti ponovljen u prisustvu izručenog lica;
8. da država, molilja, da garancije da smrtna kazna koja je propisana za krivično djelo povodom kojeg se zahtijeva izručenje neće biti izrečena, odnosno izvršena.

4.2.9. U članovima od 25 do 35 Konvencije propisana su opšta načela u vezi sa uzajamnom međunarodno pravnom pomoći u krivičnim stvarima.

Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima Srbije to čini na sljedeći način:

***Uzajamnost** – član 8*

Domaći pravosudni organi pružaju međunarodnu pravnu pomoć pod uslovom uzajamnosti. Na zahtjev domaćeg pravosudnog organa, ministarstvo nadležno za pravosuđe daje obavještenje o postojanju uzajamnosti.

Ako nema podataka o uzajamnosti, pretpostavlja se da uzajamnost postoji.

*Član 26 -**slučajne informacije** - Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima - Dostavljanje podataka bez zamolnice - član 98*

Domaći pravosudni organi mogu, pod uslovom uzajamnosti, bez zamolnice dostavljati nadležnim organima strane države podatke o krivičnim djelima i učiniocima, ako bi to bilo od koristi za vođenje krivičnog postupka u inostranstvu.

Dostavljanje podataka iz stava 1 ovog člana vrši se samo u slučaju da to ne ometa vođenje krivičnih postupaka u Republici Srbiji.

Domaći pravosudni organi mogu zahtijevati od nadležnih organa države, molilje, kojima sud ostavljeni podaci iz stava 1 ovog člana da ih obavijeste o preduzetim radnjama i donijetim odlukama.

Član 27- postupci koji se odnose na zahtjeve za uzajamnu pomoć u slučaju nepostojanja važećih međunarodnih sporazuma – Odredbe Zakona o međunarodnoj pravnoj pomoći u krivičnim stvarima, primjenjuju se u slučaju nepostojanja važećih međunarodnih sporazuma.

Član 28 -tajnosti ograničenja korišćenja - Zakon o međunarodnoj pravnoj pomoćiu krivičnim stvarima - Vršenje međunarodne pravne pomoći - član 3:

Međunarodna pravna pomoć pruža se u postupku koji se odnosi na krivično djelo koje u trenutku kada je zatražena pomoć spada u nadležnost suda države, molilje.

Međunarodna pravna pomoć pruža se i u postupku koji je pokrenut pred organima uprave za djelo koje je kažnjivo prema zakonodavstvu države, molilje, ili zamoljene države, u slučaju kada odluka upravnog organa može da predstavlja osnov za pokretanje krivičnog postupka. Međunarodna pravna pomoć pruža se i po zahtjevu Međunarodnog suda pravde, Međunarodnog krivičnog suda, Evropskog suda za ljudska prava i drugih međunarodnih institucija koje su osnovane međunarodnim ugovorom koji je potvrdila Republika Srbija.

***Tajnost podataka** - član 9*

Državni organi dužni su da čuvaju tajnost podataka dobijenih u postupku pružanja međunarodne pravne pomoći.

Podaci o ličnosti mogu da se koriste isključivo u krivičnom ili u pravnom postupku u vezi sa kojim je podneta zamolnica.

Predmet ostalih oblika međunarodne pravne pomoći *- Član 83*

Ostali oblici međunarodne pravne pomoći obuhvataju:

1. izvršenje procesnih radnji, kao što su pozivanje i dostavljanje pismena, saslušanje okrivljenog, ispitivanje svjedoka i vještaka, uviđaj, pretresanje prostorija i lica, privremeno oduzimanje predmeta;
2. primjenu mjera, kao što su nadzor i snimanje telefonskih i drugih razgovora ili komunikacija i optička snimanja lica, kontrolisana isporuka, pružanje simulovanih poslovnih usluga, sklapanje simulovanih pravnih poslova, angažovanje prikrivenog islednika, računarsko pretraživanje i obrada podataka;
3. razmjenu obavještenja i dostavljanje pismena i predmeta koji su u vezi sa krivičnim postupkom u državi, molilji, dostavljanje podataka bez zamolnice; korišćenje audio I video-konferencijske veze, formiranje zajedničkih istražnih timova;
4. privremenu predaju lica lišenog slobode radi ispitivanja pred nadležnim organom države, molilje.

Član 29, 30 i 31 - hitna zaštita sačuvanih računarskih podataka i hitno otkrivanje zaštićenih podataka o saobraćaju, kao i uzajmna pomoć u odnosu na pristupanje sačuvanim računarskim podacima - Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima - Predmet ostalih oblika međunarodne pravne pomoći - Član 83

Zakon o elektronskim komunikacijama Republike Srbije propisuje obavezu zadržavanja podataka u članu 128, a zakonito presretanje elektronskih komunikacija u članu 127.

Član 32 –prekogranični pristup sačuvanim računarskim podacima uz saglasnost ili kada su dostupni javnosti, je omogućen kroz direktnu primjenu Konvencije.

Član 33 - uzajamna pomoć u prikupljanju podataka o saobraćaju u realnom vremenu je saobrazan na domaćem planu primjenom člana 20 Konvencije - prikupljanje podataka o saobraćaju u realnom vremenu.

Kao što je to već ranije navedeno, u nedostatku sadržajnije i jasnije norme, ovaj član u praksi potpada pod primjenu ne tako jasnog i, možda, ne potpuno pravilno primjenjenog instituta računarskog pretraživanja podataka:

Računarsko pretraživanje podataka *- član 178.*

Ako su ispunjeni uslovi iz člana 161 st.1 i 2 ovog Zakonika, na obrazloženi prijedlog javnog tužioca sud može odrediti računarsko pretraživanje već obrađenih ličnih i drugih podataka i njihovo poređenje sa podacima koji se

odnose na osumnjičenog i krivično djelo.

U skladu sa odredbom član 179 ZKP ovu posebnu dokaznu radnju određuje sudija za prethodni postupak obrazloženom naredbom.

Član 34 – uzajamna pomoć u presretanju podataka o sadržaja, saobrazan je primjeni ovlašćenja u vezi presretanja podataka o sadržaju komunikacije, koje je Zakonikom o krivičnom postupku propisano članovima 166, 167 i 168.

V PROTOKOL UZ KONVENCIJU O SAJBER KRIMINALU KOJI SE ODNOSI NA INKRIMINACIJU DJELA RASISTIČKE I KSENOFOBIČNE PRIRODE IZVRŠENIH PREKO RAČUNARSKIH SISTEMA

5.1. Uporedna analiza

5.1.1. Član 2 Protokola daje definicije rasističkog i ksenofobičnog materijala.

Zakonodavstvo Srbije trenutno nije propisalo definiciju navedenog pojma.

Članom 3 Protokola sankcionisano je širenje rasističkog i ksenofobičnog materijala preko računarskih sistema, što Krivični Zakonik Srbije čini kroz djelo Rasna i druga diskriminacija iz člana 387 na sljedeći način:

(1) Ko na osnovu razlike u rasi, boji kože, vjerskoj pripadnosti, nacionalnosti, etničkom porijeklu ili nekom drugom ličnom svojstvu krši osnovna ljudska prava i slobode zajamčena opšte prihvaćenim pravilima međunarodnog prava i ratifikovanim međunarodnim ugovorima odstrane Srbije, kazniće se zatvorom od šest mjeseci do pet godina.

(2) Kaznom iz stava 1 ovog člana kazniće se ko vrši proganjanje organizacija ili pojedinaca zbog njihovog zalaganja za ravnopravnost ljudi.

(3) Ko širi ideje o superiornosti jedne rase nad drugom ili propagira rasnu mržnju ili podstiče na rasnu diskriminaciju, kazniće se zatvorom od tri mjeseca do tri godine.

(4) Ko širi ili na drugi načinu čini javno dostupnim tekstove, slike ili svako

drugo predstavljanje ideja ili teorija koje zagovaraju ili podstrekavaju mržnju, diskriminaciju ili nasilje, protiv bilo kojeg lica ili grupe lica, zasnovanih na rasi, boji kože, vjerskoj pripadnosti, nacionalnosti, etničkom porijeklu ili nekom drugom ličnom svojstvu, kazniće se zatvorom od tri mjeseca do tri godine.

(5) Ko javno prijeti da će, protiv lica ili grupe lice zbog pripadnosti određenoj rasi, boji kože, vjeri, nacionalnosti, etničkom porijeklu ili zbog nekog drugog ličnog svojstva, izvršiti krivično djelo za koje je zaprijećena kazna zatvora veća od četiri godine zatvora, kazniće se zatvorom od tri mjeseca do tri godine.

5.1.2. Član 4 "Rasistički i ksenofobički motivisana prijetnja", član 5 "Rasistički i ksenofobički motivisana uvreda" u Krivični Zakoniku Srbije su regulisani članom 317 Izazivanje nacionalne, rasne i vjerske mržnje i netrpeljivosti:

(1) Ko izaziva ili raspiruje nacionalnu, rasnu ili vjersku mržnju, ili netrpeljivost među narodima ili etničkim zajednicama koje žive u Srbiji, kazniće se zatvorom od šest mjeseci do pet godina.

(2) Ako je djelo iz stava 1 ovog člana učinjeno prinudom, zlostavljanjem, ugrožavanjem sigurnosti, izlaganjem poruzi nacionalnih, etničkih ili vjerskih simbola, oštećenjem tuđih stvari, skrnavljenjem spomenika, spomen-obilježja ili grobova, učinilac će se kazniti zatvorom od jedne do osam godina.

(3) Ko djelo iz st.1 i 2 ovog člana vrši zloupotrebom položaja ili ovlašćenja ili ako je usljed tih djela došlo do nereda, nasilja ili drugih teških posljedica za zajednički život naroda, nacionalnih manjina ili etničkih grupa koje žive u Srbiji, kazniće se za djelo iz stava 1 zatvorom od jedne do osam godina, a za djelo iz stava 2 zatvorom od dvije do deset godina.

5.1.3. Član 6 Protokola sakncionisano je poricanje, minimalizovanje, odobravanje ili opravdavanje genocida ili zločina protiv čovječnosti.

Navedeno krivično djelo nije predviđeno kao krivično djelo u okviru pozitivno pravnog krivičnog poretka Republike Srbije.

Ipak, Krivični zakonik Srbije predviđa posebne okolnosti za odmjeravanje kazne za krivično djelo učinjeno iz mržnje, i to u svom članu 54 a, na sljedeći način:

"Ako je krivično djelo učinjeno iz mržnje zbog pripadnosti rasi i vjeroispovesti, nacionalne ili etničke pripadnosti, pola, seksualne orjentacije ili rodnog identiteta drugog lica, tu okolnost sud će cijeniti kao otežavajuću, osim ako ona nije propisana kao obilježje krivičnog djela".

VI REZULTATI I STATISTIČKI POKAZATELJI POSEBNOG TUŽILAŠTVA ZA VISOKOTEHNOLOŠKI KRIMINAL REPUBLIKE SRBIJE

(PERIOD 2006 DO 14. MARTA 2014.)

Čl. 185 KZ "Dečja pornografija"	Broj predmeta	Broj lica	Istrage	Optužni akti	Presude
2010	14	14	13	12	10
2011	40	40	40	40	35
2012	18	21	20	20	14
2013	16	16	9	5	4
2014	7	7	7		
UKUPNO	**95**	**98**	**89**	**77**	**63**

Ukupan broj prijava KT 2006-2014

Godina	Broj predmeta	lica
2006	**19**	**32**
2007	75	84
2008	110	166
2009	91	121
2010	116	131
2011	130	154
2012	114	144
2013	**160**	**185**
2014	52	58
Ukupno	**867**	**1105**

Ukupan broj prijava KTR 2007-2014

Godina	Broj predmeta
2007	**60**
2008	68
2009	114
2010	443
2011	502
2012	**609**
2013	558
2014	43
Ukupno	**2397**

Ukupan broj prijava KTN 2007-2014

Godina	Broj predmeta
2007	**11**
2008	14
2009	42
2010	13
2011	28
2012	65
2013	**243**
2014	144
Ukupno	**560**

Ukupan broj predmeta KT + KTR + KTN do 14. 03.2014.

	KT	KTR	KTN	
2006	**19**			19
2007	**75**	**68**	**11**	**154**
2008	110	60	14	184
2009	91	114	42	247
2010	116	443	13	572
2011	130	502	28	660
2012	114	609	65	788
2013	**160**	**558**	**243**	**986**
2014	52	43	144	245
UKUPNO	**867**	**2397**	**560**	**3855**

VII OTKRIVANJE I GONJENJE PRIMJERI IZ OKRUŽENJA (REPUBLIKA SRBIJA)

7.1. Policijski službenici Odjeljenja za borbu protiv visokotehnološkog kriminala, operativnim radom došli su do saznanja da je NN lice „Srđan" iz Beograda pribavio fotografije i audio vizuelni materijal pornografske sadržine nastale iskorišćavanjem djece i maloljetnika u pornografske svrhe.

Provjerom kroz JIS MUP Republike Srbije, utvrđeno je da na lociranoj adresi prijavljeno prebivalište ima prijavljeni M. S.

Postupajući po naredbi istražnog sudije Višeg suda u Beogradu, izvršen je pretres stana i drugih prostorija na adresi na kojoj osumnjičeni ima prijavljeno prebivalište, o čemu je sačinjen zapisnik o pretresanju stana i drugih prostorija. Prilikom pretresa stana i drugih prostorija pronađena je i oduzeta informatička oprema koju imenovani koristi, i to 4 hard diska i 27 DVD medija.

Prilikom izvršenja naredbe o pretresu stana policijskim službenicima je bio onemogućen ulazak u stan više od 45 minuta zato jer majka prijavljenog M. S. nije željela da otvori vrata stana tvrdeći da njen sin nije kod kuće, nakon što je policijskim službenicima omogućen ulazak u stan, u istom je zatečen prijavljeni M. S. od koga je uz potvrdu o privremeno oduzetim predmetima oduzeta informatička oprema.

Takođe, prilikom pretresa stana uočeno je da se na tlu ispod prozora prijavljenog M. S. nalazi odbačen jedan hard disk, a imajući u vidu da je zbog proteka vremena omogućavanja ulaska u stan i postupanja po navedenoj naredbi, postojao osnov sumnje da odbačeni hard disk pripada prijavljenom, te da ga je osumnjičeni neposredno prije omogućavanja vršenja pretresa odbacio kroz prozor. Od strane policijskih službenika PS Voždovac izvršen je uviđaj lica mjesta i izuzimanja odbačenog hard diska. O naprijed navedenom, sačinjena je službena bilješka.

Policijski službenici Službe za specijalne istražne metode, postupajući po navedenoj naredbi, u službenim prostorijama SBPOK u prisustvu osumnjičenog M. S. izvršili su uvid i pregled 4 privremeno oduzeta hard diska računara, prilikom čega je utvrđeno da se na jednom hard disku

(koji je pronađen u sobi prijavljenog van kućišta računara), nalazi materijal nastao iskorišćavanjem djece i maloljetnika u pornografske svrhe u do tada utvrđenoj količini od 865 MB.

Takođe, prilikom uvida u 2 hard diska koji su se u trenutku vršenja pretresa nalazili u kućištu računara prijavljenog, utvrđeno je da nedostaje sistemski hard disk, odnosno hard disk na kome se nalazi operativni sistem, obzirom da se na navedena 2 diska nalaze samo skladišteni podaci.

Materijal nastao iskorišćavanjem maloljetnih lica za pornografiju, pronađen je prilikom uvida u hard disk marke „Maxtor" kapaciteta 80 GB i bio je smješten u „C" particiji računara, u folderu „Documents and settings", u podfolderu pod nazivom „Bambi", u kome se nalazilo 16 video klipova ukupne veličine 865 MB.

Služba za borbu protiv organizovanog kriminala Odjeljenje za borbu protiv visokotehnološkog kriminala podnijelo je Višem javnom tužilaštvu u Beogradu, Posebnom odeljenju za borbu protiv visokotehnološkog kriminala krivičnu prijavu protiv M. S. zbog krivičnog dijela prikazivanje, pribavljanje i postavljanje pornografskog materijala i iskorišćavanje maloljetnog lica za pornografiju iz čl.185 st.4 Krivičnog zakonika.

I to na taj način što je u periodu od 2008.godine do februara 2013. godine, sa svog računara, elektronskim putem koristeći softver pod nazivom „Lime Wire" koji funkcioniše kao zatvorena mreža, pribavio i sačuvao u svom računaru fotografije i audio vizuelni materijal koji je nastao iskorišćavanjem djece i maloljetnika u pornografske svrhe.

Kao prilog tj. kao dokaz uz krivičnu prijavu dostavljen je zapisnik o saslušanju okrivljenog u prisustvu branioca, a kojom prilikom je okrivljeni izjavio da je internet koristio za skidanje pornografije, ali da nije svjesno skidao dječiju pornografiju, već običnu pornografiju koristeći torent, frostfajer, lajmvajer programe, te da je prilikom odabira šta će da daunluduje, odabirao više stvari i puštao da se isti skidaju preko noći, te da nije gledao sve što skida sa interneta. Naveo je i da je kada prilikom pregledanja skinutog materijala nailazio na dječiju pornografiju odmah bi to izbrisao.

U februaru 2013. godine Posebno tužilaštvo za borbu protiv visokotehnološkog kriminala podnijelo je prijedlog za preduzimanje određenih istražnih radnji prema okrivljenom MS u pravcu utvrđivanja postojanja elemenata krivičnog djela prikazivanje, pribavljanje i postavljanje pornografski materijal i iskorišćavanje maloljetnog lica za pornografiju iz čl.185 st.4 KZ, kojom prilikom je predloženo da se protiv okrivljenog MS odredi pritvor po osnovu čl.436 st.1 tač. 2 ZKP, obzirom da količina pronađenih fotografija i audio-vizuelnih zapisa nastalih iskorišćavanjem maloljetnih lica u pornografske svrhe, kao i njihov sadržaj i uzrast lica čije je seksualno zlostavljanje prikazano na navedenom materijalu ukazuju na opasnost da će okrivljeni ponoviti krivično djelo ukoliko bude pušten na slobodu.

22.02.2013. godine rješenjem odredio pritvor okrivljenom MS, obzirom da je tokom postupka pribavljeno dovoljno dokaza protiv okrivljenog MS. Dana 28.02.2013. godine podnijet je optužni prijedlog protiv istog zbog krivičnog djela iz čl.185 st.4 KZ, kojom prilikom je stavljen i prijedlog da se prema okrivljenom produži pritvor shodno odredbi čl.436 st.1 tač. 2 ZKP, jer količina pornografskog materijala koja je od okrivljenog oduzeta, kontinuitet inkriminisanog djelovanja, prikupljanje pornografskog sadržaja nastalog iskorišćavanjem maloljetnih lica, i to djece uzrasta od 3 do 7 godina, jeste posebna okolnost koja ukazuje da bi puštanjem na slobodu, isti ponovio ovakvo ili slično krivično djelo.

Prema okrivljenom MS ukinut je pritvor jer po nalaženju Vijeća u konkretnom slučaju ne stoje zakonski osnovi za zadržavanje okrivljenog u pritvoru propisanih odredbom čl.436 st.1 tač. 2 ZKP, a imajući u vidu da je okrivljeni lice starosti 32 godine, te da isti nije ranije osuđivan, te imajući u vidu i činjenicu da je od okrivljenog oduzeta informatička oprema, kao i činjenicu da se okrivljenom stavlja na teret izvršenje svršenog krivičnog djela, to je vijeće našlo da od drugih okolnosti ne stoje osobite okolnosti koje ukazuju na opravdanu bojazan da će okrivljeni ukoliko bude na slobodi ponoviti izvršenje krivičnog djela.

Protiv ovog rješenja Više tužilaštvo je izjavilo žalbu zbog pogrešno utvrđenog činjeničnog stanja iz čl.367 tač. 3 u vezi čl.370 st.1 ZKP, obzirom da po mišljenju Tužilaštva činjenica da okrivljeni MS do sada nije osuđivan ne može biti od uticaja na produženje pritvora u konkretnoj situaciji, iako ranija ne osuđivanost nesporno ukazuje na eventualnu sklonost okrivljenog na vršenje krivičnih djela, ali je navedenoj činjenici sud dao preveliki značaj a pri tom nije u dovoljnoj mjeri cijenio ono što je od ključne važnosti, a to je izražena upornost koju je okrivljeni pokazao prilikom izvršenja ovog krivičnog djela, obzirom da je u dužem vremenskom periodu, u kontinuitetu, pribavljao pornografski materijal nastao iskorišćavanjem maloljetnih lica, a između ostalog i djece uzrasta od 3 do 7 godina, te da okolnost da je od okrivljenog oduzeta računarska oprema koju je posjedovao, ne može biti garancija da on ubuduće neće ponoviti krivično djelo, jer je u pitanju osoba koja koristi računare i internet i po sopstvenom saznanju, skoro svakodnevno sa interneta pribavlja pornografski materijal, i imajući u vidu pristupačnost interneta i njegovu naklonost ka računarskim tehnologijama, ali i sklonost ka zloupotrebi istih, te očiglednu posebnu sklonost ka pribavljanju pornografskog materijala nastalog zloupotrebom i iskorišćavanjem maloljetnih lica, to sve predstavlja okolnosti koje ukazuju da bi puštanjem na slobodu isti ponovio ovakvo ili slično krivično djelo.

Apelacioni sud u Beogradu je rješenjem odbio kao neosnovanu žalbu Posebnog tužioca za visokotehnološki kriminal, kojom prilikom je našao da je prvostepeni sud pravilno postupio kada je prema okrivljenom MS ukinuo pritvor jer ne postoji zakonski osnov za produženje pritvora prema

okrivljenom propisan odredbom čl.436 st.1 tač. 2 ZKP.

21.02.2013. godine stavljen je prijedlog istražnom sudiji Višeg suda u Beogradu za preduzimanje određenih istražnih radnji, odnosno za izdavanje naredbe za uzimanje brisa i izradu DNK profila od strane MS, a takođe i izrade DNK profila sa brisa sa predmeta pronađenog na licu mjesta, i to jednog hard diska, te upoređivanja ova dva DNK profila.

Dana 21.02.2013. godine istražni sudija Višeg suda u Beogradu donio je navedenu naredbu.

U toku marta 2013. godine dostavljen je zapisnik o vještačenju od strane Nacionalno kriminalističko-tehničkog centra iz čijeg mišljenja proizilazi da je DNK analizom spornog biološkog traga uzetog sa hard diska marke „Samsung" dobijen DNK profil koji se u potpunosti poklapa sa DNK profilom okrivljenog MS.

28.06.2013. godine podnijet je prijedlog istražnom sudiji Višeg suda u Beogradu za preduzimanje određenih istražnih radnji a u cilju utvrđivanja svih bitnih elemenata krivičnog djela prikazivanje, pribavljanje i postavljanje pornografskog materijala i iskorišćavanje maloljetnog lica za pornografiju iz čl.185. KZ izda naredbu da se obavi fiksiranje i ekstrakcija digitalnih dokaza koji se nalaze na hard disku marke „Samsung", a za koji je vještačenjem Nacionalnog kriminalističko-tehničkog centra utvrđeno da se biološki trag koji je nađen na istom u potpunosti poklapa sa DNK profilom okrivljenog MS.

Istražni sudija Višeg suda u Beogradu donio je naredbu kojom se povjerava vještačenje preduzeću „Data Solutions", da izvrši fiksiranje i ekstrakciju digitalnih dokaza sa predmetnog hard diska. Iz nalaza i mišljenja preduzeća „Data Solutions" proizilazi da je oštećenje predmetnog hard diska bilo tolikog intenziteta da je spašavanje podataka, rekonstrukcija i forenzičku analizu bilo nemoguće izvršiti na datom mediju.

U konkretnom slučaju izvršilac ovog krivičnog djela je lice starosti 32 godine, po zanimanju građevinski tehničar, neoženjen, civilno služio vojni rok, srednjeg imovnog stanja, ne osuđivan prema izvještaju iz KE i protiv istog se ne vodi postupak za bilo koje drugo krivično djelo.

U konkretnom slučaju izvršilac ovog krivičnog djela je morao imati računar sa pristupom internetu, sa instaliranim posebnim programima koji omogućavaju razmjenu fajlova između lica koja imaju instaliran ovaj softverna svojim računarima.

Specifičnost konkretnog slučaja se ogleda u tome što je učinilac pokušao da prije izvršenja naredbe za pretres od strane policije uništi dokaze o izvršenju ovog krivičnog djela, a na taj način što je iz svog računara izvadio hard disk i bacio ga kroz prozor. U svojoj namjeri nije u potpunosti uspio obzirom da je kod istog na još jednom hard disku pronađen pornografski

materijal nastao iskorišćavanjem i zlostavljanjem maloljetnih lica.

Obzirom da pri pretresu stana osumnjičenog u njegovom računaru nije nađen sistemski hard disk, tj. disk na kome se nalazi operativni sistem – windows, a bez koga računar ne može da se pokrene, to je sve ukazalo policijskim službenicima da isti nedostaje i da je osumnjičeni pokušao da ga se riješi. Iz tog razloga policijski službenici su izvršili pretraživanje okoline zgrade osumnjičenog, kojom prilikom su našli na zemlji jedan hard disk marke „Samsung", a za koji su zbog naprijed navedenog sa pravom pretpostavili da isti potiče od osumnjičenog.

Obzirom da je osumnjičeni negirao da je pronađeni hard disk njegov, Tužilaštvo je stavilo prijedlog istražnom sudiji da se izvrši vještačenje DNK profila osumnjičenog i brisa uzetog sa predmetnog hard diska, a u cilju utvrđivanja da li predmetni hard disk pripada osumnjičenom.

Nakon što je vještačenjem DNK profila utvrđeno da se na predmetnom hard disku nalazi DNK trag koji potiče od okrivljenog, od istražnog sudije je zatraženo da odredi vještačenje kojim će se rekonstruisati podaci, koji su se nalazili na hard disku, a iz razloga zato jer istom nije bilo moguće pristupiti na normalan način, obzirom da je isti oštećen prilikom pada na zemlju, kada ga je osumnjičeni izbacio kroz prozor.

Obzirom da vještačenjem nije bilo moguće izvršiti rekonstrukciju podataka sa predmetnog hard diska, to je okrivljenom stavljeno na teret posjedovanje pornografskog materijala nastalog iskorišćavanjem i zlostavljanjem djece a koja je pronađena pri prvobitnom pregledu na jednom od oduzetih hard diskova.

7.2. Policijski službenici Odjeljenja za borbu protiv visokotehnološkog kriminala MUPRS, podnijeli su dana 15.06.2010. godine, krivičnu prijavu protiv tri lica, zbog postojanja osnova sumnje da su u saizvršilaštvu izvršili krivično djelo računarska prevara iz čl.301 st.1 Krivičnog zakonika, u vezi čl.33 Krivičnog zakonika i krivično djelo falsifikovanje i zloupotreba platnih kartica iz čl.225 st.1 i st.2, a u vezi čl.33 Krivičnog zakonika.

U krivičnoj prijavi je navedeno da je prijavljeni C.N. u namjeri da sebi pribavi protivpravnu imovinsku korist kako sebi tako i I.T. i K.I. U periodu od 14.05.2010. godine do 25.05.2010. godine, koristeći elektronski nalog za elektronsko naručivanje i plaćanje preduzeća „Card Servise" d.o.o. na internet stranici navedenom preduzeću koje se nalazi na adresi www.tikets.rs koristeći lažne elektronske adrese petar. marković@mailinator.com i dejan.petrović@mailinator.com i lažno se predstavljajući kao Petra Marković i Dejan Petrović, dana 14. 05.2010. godine, 17.05.2010. godine, 24.05.2010. godine i 25.05.2010. godine, zloupotrijebio podatke sa 11 platnih kartica izdavalaca banaka sa teritorije SAD-a u ukupno 98 navrata, a za ukupan iznos od 1.344.370,00 dinara, na taj način što je na internet

stranicama elektronske prodavnice koja se nalazi na adresi www.tikets.rs i na kojima se vrši elektronska kupovina, zajedno sa I.T. unosio prethodno neovlašćeno pribavljene podatke o platnim karticama u polje predviđeno za popunjavanje podataka o platnim karticama, lažno se predstavljajući kao njihov pravi korisnik, unoseći pri tom, lažne podatke u polja predviđena za unos imena i prezimena i to „Dejan Marković" i elektronsku adresu petar.marković@mailinator.com i „Dejan Petrović" zajedno sa elektronskom adresom dejan.petrović@mailinator.com i kupovao karte za koncerte Eltona Johna, Bob Dylana, Erica Cleptona i Steve Winwooda, da bi potom prijavljeni I.T. predavao prijavljenom K.I. i brojeve šifri naručenih karata za koncerte, nakon čega je K.I. podizao karte sa koncerta na biletarnici u Sportskom centru „Arena", gdje je saopštavao šifre rezervisanih karata koje mu je I.T. davao, čime su izvršili krivično djelo računarska prevara iz čl.301 st.1 KZ u vezi čl.33 KZ I krivično djelo falsifikovanje i zloupotreba platnih kartica iz čl.225 st.2 u vezi st.1 KZ, u vezi čl.33 KZ.

Posebno tužilaštvo za borbu protiv visokotehnološkog kriminala, podnijelo je zahtjev republičkom javnom tužilaštvu za povjeravanje stvarne nadležnosti u ovom predmetu, nakon čega je podnijet zahtjev za sprovođenje istrage Višem sudu u Beogradu, protiv tri lica zbog postojanja osnovane sumnje da su izvršili krivično djelo falsifikovanje i zloupotreba platnih kartica iz čl.225 st.4 u vezi st.2 KZ, u vezi čl.33 KZ, u sticaju sa krivičnim djelom računarska prevara iz čl.301 st.2 u vezi st.1, u vezi čl.33 Krivičnog zakonika.

Nakon sprovedene istrage u aprilu 2011. godine, posebno tužilaštvo za borbu protiv visokotehnološkog kriminala podiglo je optužnicu protiv okrivljenih zato što su:

- N.C. izvršio krivično djelo falsifikovanje i zloupotreba platnih kartica iz čl.225 st.4 u vezi st.2 Krivičnog zakonika.
- I.T. i K.I. izvršili krivično djelo prikrivanje iz čl.221 st.1 KZ, u vezi čl.33 KZ.

Naime, u iskazu datom u prisustvu branioca u policiji, kao i u iskazu datom u predistražnim sudijom okrivljeni C.N. priznaje izvršenje krivičnog djela koje mu je optužnicom stavljeno na teret, a kojom prilikom je naveo da je do podataka o platnim karticama došao na internet sajtu na kome se prodaju podaci o istima, te da se radi o internet sajtu www.cvv2.su te da je podatke o platnim karticama platio 200 dolara.

Nakon što je došao do podataka o platnim karticama a koje su sadržale pan broj, datum isteka registracije icvv2 broj isti je pristupio sajtu www.arenabeograd.com i tu rezervisao karte za neki koncert kako bi isprobao da li se može izvršiti plaćanje sa podacima koje je kupio o platnim karticama.

U polje zone podataka je unosio izmišljene podatke i to Petra Marković i Dejana Petrović, a kada bi došlo do opcije za plaćanje unosio je podatke sa platnih kartica koje je i kupio. Po završetku procedure, stizalo mu je obavještenje da je karta uspješno rezervisana, kao i broj – šifra sa kojom se

karta može podići, te brojeve davao je Ivanu Todoroviću koji je trebao da podiže karte sa blagajne i da ih dalje prodaje, a novac su trebali da dijele.

Izjavio je da, koliko mu je poznato karte nije podizao lično I., već njegov drug K. koga ne poznaje. Prilikom kupovine ovih karata koristio je računar, koji se nalazi u prostorijama škole „Gimnazija Crnjanski", u sali za računare, kao isvoj kućni računar, s tim što je prilikom kupovine karata iz „Gimnazije Crnjanski." Pored njega bio i I.T., kome je tom prilikom objašnjavao šta radi. Hard disk iz svog kućnog računa koji je koristio za ove transakcije je bacio u Savu prije nego što je uhapšen u blizni TC „Ušće", a iz razloga jer je smatrao da mu više nije potreban.

Prilikom saslušanja okrivljeni T.I. je izjavio da se njegov drug C.N. dobro razumije u kompjutere i da ima iskustva sa „hakovanjem", te da mu je mjesec dana prije kritičnog događaja ponudio da zarade novac i rekao mu da će da obezbijedi karte za koncerte, a da on treba da ih proda, te da će mu za uzvrat dati dio novca od prodatih karata. To mu je C.N. rekao u školskom dvorištu „Gimnazije Crnjanski" obzirom da su tada još uvijek obojica pohađali navedenu školu i bili četvrta godina.

Njemu su trebale pare za more, kao i njegovom drugu K.I. kome je on ponudio da ode da podigne te karte. Naveo je i da je K. U. bilo poznato da je C.N. nekako nabavio te karte preko interneta. Jedan dio šifara za podizanje karata mu je okrivljeni C. proslijedio putem mejla, a jedan dio na njegov fejsbuk nalog. To je radio u dva navrata, s tim što mu je prvi put proslijedio šifre za podizanje karata za koncert Eltona Johna, a poslije tri nedjelje za koncert Bob Dylana i Erica Cleptona i to dan prije nego što je uhapšen.

Po dogovoru sa C.N. on je upoznao svoga druga Konstantina i rekao mu da može da zaradi nešto novca, s tim što su mislili da uzmu karte za sebe, a nakon toga su došli na ideju da prodaju sve karte i da tako zarade novac. Konstantinu je prvi dio šifre dao tri nedelje prije spornog događaja i tada je isti otišao u biletarnicu „Arene" i tada podigao 70 karata za koncerte Bob Dylana i Erica Cleptona.

Prilikom pretresa policijski službenici su pronašli od tih 70 karata samo 32, dok je ostatak prodao K. za iznos od 1. 300 eura od kojih je isti uzeo 300 eura, a T.I. dao 1.000 eura koje je on trebao da podijeli sa C. Dan prije nego što su privedeni, C. je T.I. proslijedio šifre za podizanje 246 karata preko četa na servisu ICQ, a on je dio tih rezervacija proslijedio K. SMS porukom. Dogovor je bio da u toku dana K. proda svih 246 karata i od druge ture za iznos od 5.000 eura, a po dogovoru koji je prethodno postigao sa licem kome je prethodno prodao karte iz prve ture.

Taj iznos predstavlja 60% od pune vrijednosti karata koji iznosi oko 8.000 eura. K. je trebalo da dobije novac za prodaju tih karata, ali okrivljeni nije-su imali precizan dogovor koliko će ko da dobije od ukupne sume koju bi dobili od prodaje karata.

Prilikom saslušanja okrivljeni I.K. je izjavio da I.T. poznaje od malena, jer žive u istom kraju, te ga je isti pozvao telefonom kojom prilikom ga je pitao da li bi otišao da podigne neke karte za koncert, na šta je on pristao. Kada se našao sa okrivljenim T. isti mu je dao šifre za podizanje karata na biletarnici SC „Arena" i obećao mu 200-300 eura kada mu donese karte, te tom prilikom nije pitao zašto on to sam ne uradi, zato jer mu je bio potreban novac. Isti je u dva navrata podizao karte i to prvom prilikom 70 karata, a u drugom navratu preko 200 karata, a kojom prilikom su ga posle izlaska iz „Arene" policijski službenici lišili slobode.

Predstavnik oštećenog preduzeća „Card Service" d. o. o. i u toku postupka izjavio da je njegovo preduzeće ovlašćeno za elektronsku prodaju preko interneta ulaznica za koncerte koji se održavaju u SC „Arena" Beograd, tj. da sa „Arenom" Beograd imaju zaključen Ugovor o prodaji ulaznica elektronskim putem fizičku prodaju preko same blagajne „Arene", a da sa „Intesa bankom" imaju zaključen Ugovor o korišćenju onlajn sistema za novčane transakcije radi elektronske prodaje i to za kartice „Visa" i „Mastercard", s obzirom da ispunjavaju sve tehničke i druge uslove koje propisuje kako „Intesa banka" kao korespodenska banka sa bankama koje inače izdaju „Visa" i „Mastercard", te u tom smislu imaju licencu za obavljanje navedene djelatnosti.

Isti je naveo da prodaju karata vrše preko sajta www.tiket.rs te da je u konkretnom slučaju dana 14.05.2010. godine, koristeći ime Dejan Petrović i emejl adresu dejan.petrović@majlnapr.com u više navrata bukirano ukupno 12 ulaznica za koncert Eltona Johna. Isti je pojasnio da se zainteresovani kupac predstavlja imenom i prezimenom, tj. na navedenom sajtu upisuje ime i prezime, ostavlja broj mobilnog telefona, kada se slaže sa uslovima prodaje, a potom se sa njihovog sajta prelazi na stranicu „Intesa banke", gdje se elektronskim putem vrši plaćanje, i to tako što se u okviru sajta banke unose podaci sa konkretnih kartica „Visa" ili „Mastercard". Nakon što se plaćanje sa navedenih kartica izvršii „Inteza banka" im potvrdi da je došlo do plaćanja, onda se od strane njihovog preduzeća izdaju brojevi – šifre pod kojima mogu da se podignu karte za koje je izvršeno plaćanje.

Predstavnik oštećenog je tom prilikom naveo da je dana 17.05.2010. godine, lice pod imenom Petar Marković koristeći emejl adresu petar.marković@mailinator.com kupio 60 ulaznica za koncerte Eltona Johna, Bob Dylana i Erica Cleptona, na osnovu evidencije utvrđeno je da su kupljene karte u najskupljoj cjenovnoj kategoriji, a od „Intesa banke" da je obavljena novčana transakcija. Međutim, banka je kasnije dobila povratnu informaciju koja glasi kako izdavaoci navedenih kartica povodom toga im uputilo informaciju da sumnja na neku prevarnu radnju i povodom toga im uputilo zahtjev da predaju sve podatke iz informatičkog sistema. Kako je dana 24 i 25.05.2010. godine, naručeno preko 200 ulaznica za sva tri koncerta od strane policije je sugerisano da odobre i navedenu transakciju

i odobre izdavanje karata da bi bili u mogućnosti da identifikuju i liše slobode lice koje dođe da podigne karte.

Svjedok oštećenih je takođe naveo da su sve karte kupljene od strane lica Dejan Petrović i Petar Marković, a da su tom prilikom ostavljena dva ili tri ista broja mobilnih telefona.

Dana 25.05.2010. godine, po naredbi istražnog sudije Višeg suda u Beogradu izvršen je pretres stana i drugih prostorija okrivljenog Cicmil Nikole, kojom prilikom su našli tri lap-topa od kojih jedan nije posjedovao hard disk.

25.05.2010. godine po naredbi istražnog sudije Višeg suda u Beogradu obavljeno je pretresanje stana i drugih prostorija okrivljenog T.I. kojom prilikom je od istog oduzeto 32 karte za koncert Eltona Johna, za dan 03.06.2010. godine, jedan lap-top računar i jedan mobilni telefon.

Prilikom lišenja slobode okrivljenog I.K. od istog je oduzeto 46 karata za koncert Eltona Johna, za dan 03.06.2010. godine, 100 karata za koncert Bob Dylana, za dan 06.06.2010. godine, 100 karata za koncert Erica Cleptona i Steve Winwooda, za dan 09.06.2010. godine, jedan papir na kome su bile ispisane šifre za podizanje karata, kao i jedan mobilni telefon marke „Nokia".

Služba za specijalne istražne metode, Odsjeka za prikupljanje i obradu digitalnih dokaza je sastavila izvještaj o pregledu jednog hard diska iz lap-top računara oduzetog od okrivljenog T.I., a u kome je navedeno da je analizom sadržaja uz pomoć softvera za forenzičku obradu na predmetnom hard disku pronađena dva korisnička emejl naloga i korisnička imena sa lozinkama za logovanje na internet sajtove, a koji su korišćeni u konkretnom slučaju prilikom izvršenja ovog krivičnog djela.

Iz listinga izvršenih transakcija na prodajnom mjestu www.tiket.com je utvrđeno da su prilikom transakcija koje su izvršili Petar Marković i Dejan Petrović korišćeni podaci platnih kartica koje pripadaju stranim državljanima i koje su na ovaj način zloupotrijebljene.

Uvidom u izvještaj o korisniku IP adrese Telekoma Srbije od 31.05.2010. godine, utvrđeno je da je korisnik IP adrese sa koje je pristupano sajtu www.tiket.com u datom trenutku bila OŠ „M.C".

Iz izvještaja Službe za specijalne istražne metode, Odjeljenja za elektronski nadzor od 15.10.2010. godine o vještačenju mobilnih telefona i SIM kartica oduzetih od T.I., a uvidom u telefonski imenik i listu poziva i SMS poruke, utvrđeno je da su okrivljeni T.I. i okrivljeni C.N. imali komunikaciju, te da se u tekstu poruka okrivljenog pored imena Eltona Johna, nalaze šifre.

Uvidom u izvještaj iz KE za okrivljene C.N., T.I. i I.K. utvrđeno je da isti nijesu ranije bili krivično osuđivani, međutim, protiv trećeg okrivljenog I.K. se u isto vrijeme vodila istraga u Prvom osnovnom sudu u Beogradu, zbog izvršenja dva krivična djela teška krađa iz čl.204 st.1 tač.1 KZ i krivičnog

djela neovlašćeno korišćenje tuđeg vozila iz čl.213 st.2 u vezi st.1 KZ, u vezi čl.33 KZ.

10.09.2012. godine, Viši sud u Beogradu je drugo okrivljenog T.I. i treće okrivljenog I.K. oglasio krivima zato što su izvršili krivično djelo prikrivanje iz čl.221 st.1 KZ, u vezi čl.33 KZ i izrekao im uslovne osude, tako što je svakom od njih utvrdio kaznu zatvora u trajanju od 5 mjeseci i istovremeno odredio da se utvrđena kazna zatvora neće izvršiti ukoliko okrivljeni u roku od 3 godine po pravnosnažnosti presude ne izvrše drugo krivično djelo, a uz kazne im izrekao i mjeru bezbjednosti oduzimanja predmeta, dok je prema okrivljenom C.N., kao mlađem punoljetnom licu izrekao vaspitnu mjeru pojačanog nadzora od strane organa starateljstva koja može trajati najmanje 6 meseci, a najduže 2 godine, zatim posebnu obavezu da se osposobljava za zanimanje koje odgovara njegovim sposobnostima i sklonostima, a u trajanju do 1 godine, kao i mjeru bezbjednosti oduzimanja predmeta. Ova presuda je pravnosnažna.

Specifičnost u konkretnom predmetu se ogleda u tome što je od trojice okrivljenih samo prvo okrivljeni dobro poznavao rad na računaru, isti je pribavio sredstava i alate za izvršenje istog, dok su mu drugo okrivljeni i treće okrivljeni bili veza sa „stvarnim svijetom" obzirom da je karte koje je kupio preko interneta elektronskim putem, a koje je platio koristeći tj. zloupotrebivši podatke sa tuđih platnih kartica morao neko fizički da podigne sa blagajne „Arene".

7.3. 31.07.2012. godine u MUP RS, Direkcija policije, Uprava kriminalističke policije, Služba za borbu protiv organizovanog kriminala podnijela je krivičnu prijavu protiv M.R. Zbog krivičnog djela neovlašćeno bavljenje određenom djelatnošću iz čl.353 Krivičnog zakonika i neovlašćeno iskorišćavanje autorskog djela ili predmeta srodnog prava iz čl.199 Krivičnog zakonika.

07.09.2012. godine Posebno tužilaštvo za visokotehnološki kriminal podnijelo je zahtev za povjeravanje stvarne nadležnosti Republičkom javnom tužilaštvu za postupanje po navedenoj krivičnoj prijavi.

U septembru 2012. godine Republičko javno tužilaštvo donijelo je rješenje kojim se povjerava u stvarnu nadležnost Posebnom tužilaštvu za visokotehnološki kriminal postupanje po krivičnoj prijavi podnijetoj protiv R.M. Zbog krivičnog djela neovlašćeno bavljenje određenom djelatnošću iz čl.353 Krivičnog zakonika i krivičnog djela neovlašćeno iskorišćavanje autorskog djela ili predmeta srodnog prava iz čl.199 Krivičnog zakonika.

U septembru 2012. godine Višem sudu u Beogradu podnijet je prijedlog za preduzimanje određenih istražnih radnji kojim je predloženo da se osumnjičeni R. M. sasluša na sve navode krivične prijave, da se u svojstvu svjedoka ispita predstavnik RRA i u svojstvu svjedoka ispita predstavnik SOKOJ-a.

Naime u krivičnoj prijavi je navedeno da je R. M. kao direktor preduzeća „J." doo Valjevo u čijem sastavu funkcioniše Poslovna jedinica „Radio" u dužem vremenskom periodu, a do dana podnošenja krivične prijave 30.07.2012. godine neovlašćeno emitovao radio program pod identifikacionim nazivom „Radio" na području grada Valjeva na frekvenciji 102 MNz i bez potrebnih dozvola nadležnog organa Republičke radio-difuzne agencije, koristeći predajnik i računarsku mrežu u cilju emitovanja radio programa, pri čemu je neovlašćeno emitovao muzički program domaće narodne muzike a preko zakupljenog kratkog broja 064/5881 i naplaćivao emitovanje naručenih muzičkih želja po cijeni od 80 dinara po muzičkoj numeri, pri čemu je emitovao autorska djela za koja ne posjeduje zaključene ugovore sa ovlašćenim nosiocima autorskih ili distributerskih prava čime je izvršio krivično djelo neovlašćeno bavljenje određenom djelatnošću iz čl.353 KZ i krivično djelo neovlašćeno iskorišćavanje autorskog djela ili predmeta srodnog prava iz čl.199 Krivičnog zakonika.

Nakon sprovedenih istražnih radnji, od strane Višeg suda u Beogradu, Posebno tužilaštvo za VTK je u martu 2013. godine podnijelo optužni prijedlog protiv okrivljenog R. M. što je svjestan svog djela i da je ono zabranjeno, pri čemu je htio njegovo izvršenje, neovlašćeno i za nagradu bavio emitovanjem radio programa bez dozvole Republičke radio difuzne agencije, koja je potrebna za obavljanje ove djelatnosti po Zakonu o radio difuziji, na način što je kao direktor preduzeća „J." d. o. o u čijem sastavu funkcioniše Poslovna jedinica „Radio" na području grada Valjeva, preko računara koji je bio povezan sa predajnikom, emitovao radio program sa identifikacionim nazivom „Radio" na frekvenciji 102 MNz i 102, 49 MNz, koji je bio zabavnog karaktera i sastojao se od emitovanja muzike, na koji način je ostvarivao imovinsku korist u ne utvrđenom iznosu, čime je izvršio krivično djelo neovlašćeno bavljenje određenom djelatnošću iz čl.353 KZ, kao i da se u periodu od 31.08.2008.godine do 25.07.2012. godine u Valjevu, u stanju uračunljivosti, svjestan svog djela i da je ono zabranjeno, pri čemu je htio njegovo izvršenje, u namjeri pribavljanja imovinske koristi za sebe, neovlašćeno i javno saopštavao autorska djela na taj način što je u sklopu radijskog programa „Radio" čiji je bio vlasnik emitovao muzički program sastavljen od pjesama narodne muzike domaćih autora pri čemu je preko zakupljenog kratkog broja 064/5881 primao muzičke želje slušalaca koje su se odnosile na pjesme koje su emitovane u radio programu su naplaćivane 80 dinara po numeri, iako nije imao zaključen ugovor sa SOKOJ-em – Organizacijom muzičkih autora Srbije, kao kolektivnom organizacijom za zaštitu prava autora, čime je izvršio krivično djelo neovlašćeno iskorišćavanje autorskog djela ili predmeta srodnog prava iz čl.199 st.3 u vezi st.1 KZ.

U optužnom prijedlogu je predloženo da se izvedu dokazi čitanjem izvještaja RATEL-a o kontroli radio frekvencijskog spektra, zatim zapisnika o pretresanju stana i drugih prostorija, te potvrde o privremeno oduzetim predmetima od Rajka Milinkovića, izvještaj iz KE i PE za okrivljenog, te da se

izvrši uvid u kriminalističko-tehničku dokumentaciju PU Valjevo.

Navedeni predmet se još uvijek nalazi u fazi glavnog pretresa.

7.4. Policijski službenici MUPRS, PU Požarevac, podnijeli su krivičnu prijavu protiv P.S., zbog krivičnog djela ugrožavanje sigurnosti iz čl.138 st.2 u vezi st.1 KZ.

Republičko javno tužilaštvo donijelo je rješenje kojim se povjerava u stvarnu nadležnost Posebnom tužilaštvu za borbu protiv visokotehnološkog kriminala, postupanje po krivičnoj prijavi podnijetoj protiv P.S., zbog krivičnog djela ugrožavanja sigurnosti iz čl.138 st.2 u vezi st.1 KZ.

Dana 08.12.2010. godine, Višem sudu u Beogradu, podnijet je prijedlog za preduzimanje određenih istražnih radnji kojim je predloženo da se osumljičeni P.S. sasluša na sve navode krivične prijave.

Naime, u krivičnoj prijavi je navedeno da je osumljičeni P.S., krajem mjeseca septembra 2010. godine na društvenoj mreži „Fejsbuk" sa svog profila pod nazivom „S.P." u okviru grupe „Gej parada bruka Srbije" uputio prijetnju sljedeće sadržine „Zaklati naravno", a koja je bila upućena svim eventualnim učesnicima skupa „Parada ponosa 2010", a koja je bila zakazana za 10.10.2010. godine, u Beogradu.

Nakon sprovedenih istražnih radnji od strane Višeg suda u Beogradu Posebno tužilaštvo je dana 06.04.2011. godine, podnijelo optužni prijedlog protiv okrivljenog P. S., što je dana 25.09.2010. godine, u Požarevcu, u stanju uračunljivosti, svjestan svog djela i da je ono zabranjeno, pri čemu je htio da njegovo izvršenje ugrozi sigurnost više lica – osoba koje namjeravaju učestvovati na manifestaciji „Parada ponosa 2010", koja je zakazana za 10.10.2010. godine u Beogradu, prijetnjom da će napasti na život i tijelo tih lica, na taj način što je na internet prezentaciji društvene mreže „Fejsbuk" u okviru grupe „Gej parada – bruka Srbije", čiji je član, sa svog profila „S.K. P." uputio prijeteću poruku sljedeće sadržine – „Zaklati naravno", a koja je bila upućena svim eventualnim učesnicima planiranog događaja, čime je izvršio krivično djelo ugrožavanje sigurnosti iz čl.138 st.2 u vezi st.1 KZ.

Viši sud u Beogradu, donio je rješenje kojim se odbija optužni prijedlog Posebnog tužilaštva za visokotehnološki kriminal, podnijet protiv okrivljenog P.S., zbog krivičnog djela ugrožavanje sigurnosti iz čl.138 st.2 u vezi st.1 KZ, a iz razloga zato što nijesu individualizovani i tačno određeni pasivni subjekti predmetnog krivičnog djela.

Naime, sud je mišljenja da se posljedica krivičnog djela ugrožavanja sigurnosti određuje subjektivno, što podrazumijeva da mora postojati konkretna ugrožena sigurnost tačno određenog lica, koja je za posljedicu imala osećaj nesigurnosti kod pasivnog subjekta, pri čemu pasivni subjekt mora tu prijetnju shvatiti ozbiljno, te se shodno navedenom po ocjeni suda

pasivnim subjektima – oštećenima ne mogu smatrati svi eventualni, budući učesnici planiranog događaja „Parade ponosa“, jer je na taj način potpuno nemoguće subjektivizovati i individualizovati pasivne subjekte izvršenja predmetnog krivičnog djela, te učinjeničnom opisu predmetnog krivičnog djela nedostaje bitan objektivni element krivičnog djela, jer se iz toka činjeničnog opisa ne može utvrditi koja su to lica čija je sigurnost ugrožena preduzimanjem radnji koje se okrivljenom P.S. stavljaju na teret.

Posebno tužilaštvo je podnijelo Apelacionom sudu u Beogradu žalbu protiv navedenog rješenja, zbog povrede Krivičnog zakona i pogrešno utvrđenog činjeničnog stanja, a iz razloga zato što je nejasno zašto je sud mišljenja da u konkretnom slučaju u radnjama okrivljenog nijesu ostvarena bitna obilježja krivičnog iz čl.138 st.2 u vezi st.1 KZ, s obzirom da neizvršena individualizacija pasivnog subjekta, a posebno što su optužnim aktom VJT-a u Beogradu, jasno određena lica prema kojima je izvršeno krivično djelo – riječ je o pripadnicima gej populacije koja će dana 10.10.2010. godine, u Beogradu, unaprijed određeno vrijeme, na dogovorenom mjestu učestvovati na javnom skupu „Parada ponosa 2010“, te shodno tome, poruka koju je okrivljeni ostavio na društvenoj mreži „Facebook“ u okviru grupe „Gej parada – bruka Srbije“, bila upućena jasno određenoj grupi građana, kod koje je i nastupila posljedica manifestovano u vidu nesigurnosti i straha, izazvana pretnjom upućenom kako od strane okrivljenog, tako i od strane drugih lica.

Takođe, incidenti izazvani održavanjem parade ponosa 2010. godine, u Beogradu, dana 10.10.2010. godine, jasni su pokazatelji da su prijetnje upućene gej populaciji koja planira da učestvuje na pomenutom skupu bile ne samo ozbiljne, već i ostvarene.

19.05.2011. godine, Apelacioni sud u Beogradu, donio je rješenje kojim se odbija kao neosnovana žalba Posebnog tužilaštva za visokotehnološki kriminal izjavljena protiv rješenja Višeg suda u Beogradu

22.06.2011. godine, Posebno tužilaštvo za visokotehnološki kriminal je podnijelo inicijativu za podnošenje zahtjeva za zaštitu zakonitosti protiv rješenja Apelacionog suda u Beogradu, kojim se odbija kao neosnovana žalba Višeg javnog tužilaštva u Beogradu, izjavljena protiv rješenja Višeg suda u Beogradu.

31.08.2011. godine, Vrhovni kasacioni sud, donio je presudu kojom je uvažio kao osnovan zahtjev za zaštitu zakonitosti Republičkog javnog tužioca i utvrdio da je pravosnažnim rješenjima Višeg suda u Beogradu i Apelacionog suda u Beogradu, povrijeđen Krivični zakon u korist okrivljenog S.P.

Naime, po ocjeni Vrhovnog kasacionog suda osnovanost u zahtjevu za zaštitu zakonitosti ukazuje na neprihvatljivost pravnog stanovišta prvostepenog i drugostepenog suda da djelo okrivljenog koje je predmet oputžbe, a kako je opisano u činjeničnom opisu optužnog akta, po zakonu nije krivično

djelo, jer nedostaje objektivno obilježje tog djela koje se tiče postojanja pasivnog subjekta – lica oštećenih izvršenjem krivičnog djela, a koja se ne mogu utvrditi iz tog činjeničnog opisa, te za postojanje krivičnog djela u pitanju mora postojati konkretna ugroženost sigurnosti tačno određenog broja lica koje za posljedicu ima osjećaj nesigurnosti kod pasivnog subjekta koji prijetnju mora shvatiti ozbiljno, te se oštećenima u konkretnom slučaju ne mogu smatrati svi eventualno budući učesnici predmetnog događaja, jer su u toj mjeri neodređeni da ih je potpuno nemoguće subjektivizovati i individualizovati kao pasivni subjekt, tj. žrtve izvršenja djela.

Naime, Vrhovni sud je mišljenja da je tačno da za postojanje ovog krivičnog djela, gdje je reč o više lica kao pasivnom subjektu, potrebno da se zna na koja lica se odnosi prijetnja napadom na život ili tijelo i čija je lična sigurnost ugrožena, ali to ne znači da identitet tih lica mora biti unapred poznat i tačno određen, kako pogrešno smatraju prvostepeni i drugostepeni sud, te da je dovoljno da ta lica, na koja se odnosi prijetnja, moguće odrediti prema nekoj okolnosti koja stoji u vezi sa upućenom prijetnjom, te da upravo na takav način krug lica koja se mogu pojaviti kao pasivni subjekti – oštećeni, određen je u optužnom aktu u konkretnom slučaju, prema prirodi prijetnje, načinu i sredstvu kojim je upućena, tako da se odnosi na svakog pojedinca koji namjerava biti učesnik predmetnog događaja.

Naime, prema činjeničnom opisu djela okrivljeni prijetnju, čiji je smisao lišavanje života, ili bar tjelesno povređivanje učesnika predmetne manifestacije, uputio kao jedan od članova grupe, koja na internet prezentacije društvene mreže zagovara primjenu nasilja prema grupi pojedinaca koji pripadaju gej populaciji ili joj se pridružuju na javnom skupu, a prijetnju je uputio putem elektronskog medija namijenjenog opštoj javnosti, koji je dostupan svakom pojedincu, što je način da prijetnju sazna širok krug lica. Dakle, pomenuta lica kojima je prijetnja upućena koji namjeravaju da budu učesnici predmetne manifestacije zakazane za određeni dan i na određenom mjestu, tako da ova prijetnja s obzirom na navedene okolnosti pod kojima je upućena i mogla biti saznata, objektivno može stvoriti osjećaj uznemirenja, nesigurnosti i straha za ličnu bezbjednost kod pripadnika tog kruga lica, koji su kao pasivni subjekti mogući oštećeni naznačeni u optužnom aktu, na način koji dovoljno određuje kao pripadnike ciljne grupe kojoj je upućena prijetnja.

7.5. 12.06.2012. godine MUP RS – Direkcija policije, Policijska uprava u Zrenjaninu podnijela je krivičnu prijavu protiv Ć.S., zbog postojanja osnovane sumnje da je izvršio krivično djelo neovlašćeno iskorišćavanje autorskog djela ili predmeta srodnog prava iz člana 199 stav 3 u vezi st.2 KZ.

17.07.2012. godine Posebno tužilaštvo za borbu protiv visokotehnološkog

kriminala podnijelo je Republičkom javnom tužilaštvu zahtjev za povjeravanje stvarne nadležnosti za vođenje krivičnog postupka po navedenoj krivičnoj prijavi.

23.07.2012. godine Republičko javno tužilaštvo donijelo je rješenje kojim se povjerava u stvarnu nadležnost postupanje po krivičnoj prijavi podnijetoj protiv osumnjičenog Ć.S.

24.07.2012. godine Višem sudu u Beogradu podnijet je prijedlog za preduzimanje određenih istražnih radnji protiv osumnjičenog Ć.S. a zbog postojanja osnovane sumnje da je izvršio krivično djelo neovlašćeno iskorišćavanje autorskog djela ili predmete srodnog prava iz člana 190 st.3 u vezi st.2 KZ.

U iskazu datom pred istražnim sudijom okrivljeni Ć.S. je naveo da je tačno da je dana 14.03.2012. godine izvršen pretres njegovog stana, te da su tom prilikom policijski službenici oduzeli njegov računar sa monitorom i štampačem kao i da su prilikom pretresa stana u garaži pronađeni kompakt diskovi različite filmske sadržine u DVD formatu, te da je bilo 796 komada kompakt diskova sa preko 4.000 filmskih naslova.

Osumnjičeni je tada izjavio da se radi o njegovoj privatnoj filmskoj kolekciji koju nikada nije prodavao niti javno pokazivao i koja služi isključivo za njegovu ličnu upotrebu. Obzirom da je u memoriji računara okrivljeni imao fajlove sa omotom filmova spremljene za štampanje isti se izjasnio na tu okolnost i naveo da je ove omote nabavljao kupujući razne prospekte i brošure a zatim ih skenirao i skladištio u fajlove kako bi bio upoznat sa sadržajem filmova koje je skidao sa interneta. Takođe isti je izjavio da mu se ovo isto desilo tokom 2003.godine za vrijeme akcije „Sablja“ kada mu je policija takođe oduzela računari oko 1.000 filmova koje je imao u kolekciji, te da je to što mu je oduzeto policija držala oko šest mjeseci a zatim mu je sve vraćeno i protiv njega nije podnijeta krivična prijava.

Nakon vraćanja istražnih spisa od strane istražnog sudije tužilaštvu dana 10.10.2012. godine stavljen je prijedlog za preduzimanje određenih istražnih radnji kojim je zahtijevano da se u svojstvu svjedoka ispitaju policijski službenici koji su kritičnom prilikom vršili pretres stana okrivljenog Ć.S. i podnijeli krivičnu prijavu protiv istog na sve navode iz krivične prijave a posebno na okolnost da li su prilikom pretresa kod okrivljenog pronađeni blanko – prazni ne narezani cd-ovi, te ako jesu u kom broju a obzirom da su upotvrdi o oduzetim predmetima isti ne navode.

Nakon sprovedenih istražnih radnji 23.09.2013. godine Višem sudu u Beogradu podnijet je optužni prijedlog protiv Ć.S. što je u stanju uračunljivosti, u namjeri da stavi u promet, neovlašćeno umnožene primjere autorskog djela, optičke diskove sa nasnimljenim filmovima, na taj način što je u svom stanu i pripadajućoj garaži držao 796 optičkih nosača slike i zvuka na kojima je bilo nasnimljeno ukupno 4.485 primjeraka

autorskih djela – filmova te zatim veći broj fajlova sa filmovima i omotima za filmove koji su bili spremni za štampu, a koje je držao u svom računaru koji je posjedovao četiri DVD rezača za narezivanje optičkih diskova, kao i štampač u boji za štampanje omota filmova, pri čemu je bio svjestan svog djela i njegove protivpravnosti i htio njegovo izvršenje, čime je izvršio krivično djelo neovlašćeno iskorišćavanje autorskog djela ili predmeta srodnog prava iz člana 199 st.3 u vezi st.2 u vezi st.1 KZ.

Nakon održanog glavnog pretresa dana 12.12.2013. godine Viši sud u Beogradu je donio presudu kojom je okrivljenog Ć.S. oglasio krivim za krivično djelo kojim je optužnim prijedlogom stavljeno na teret i izrekao mu uslovnu osudu tako što mu je utvrdio kaznu zatvora u trajanju od šest mjeseci i istovremeno odredio da se utvrđena kazna neće izvršiti ukoliko okrivljeni u roku provjeravanja u trajanju od dvije godine ne izvrši novo krivično djelo, uz kaznu mu je izrekao i mjeru bezbjednosti oduzimanja predmeta iz čl.87 KZ.

Naime, sud nije prihvatio odbranu okrivljenog da je u pitanju njegova filmska kolekcija**,** a prije svega iz razloga što je poklonio vjeru iskazima svjedoka – policijskih službenika D.M. I Č.S. koji nemaju ni jedan razlog da neosnovano terete okrivljenog, a koji su između ostalog naveli, da su na osnovu operativnih saznanja, uz naredbu, izvršili pretres stana Ć.S., te da je tom prilikom dio kompakt diskova pronađen u sobi pored računara, a veći dio u garaži, svi obilježeni brojevima, što je potkrijepljeno i foto dokumentacijom, u sobi gdje je bio računar, bila je gomila praznih cd-ova, štampač kao i više rasklopljenih hard diskova, kao i dvije kutije sa po oko 50 praznih cd-ova, a iz čega jasno proizilazi, a s obzirom na iskaze svjedoka, te pronađene i oduzete predmete, da je okrivljeni imao namjeru da pribavi imovinsku korist.

Specifičnost ovog predmeta ogleda se utome što okrivljenom nije stavljeno na teret stavljanje u promet već držanje u namjeri stavljanja u promet, a kako okrivljeni nije imao niti jedan duplikat bilo kog filma, to je dokazivanje njegove namjere bilo otežano, iz kog razloga su u svojstvu svjedoka ispitani policijski službenici koji su vršili pretres stana i drugih prostorija okrivljenog a da se izjasne o svojim neposrednim saznanjima, što je pored materijalnih dokaza uvid u potvrde o oduzetim predmetima, zatimiu ovom slučaju veoma bitne fotodokumentacije na kojoj se vidi da oduzeti računar ima četiri dvd rezača za narezivanje diskova što ukazuje da se često narezuje više kompakt diskova odjednom, odnijelo je prevagu na odbranu okrivljenog i kod suda učvrstilo vjeru da je okrivljeni Ć.S. nesumnjivo kriv za krivično djelo koje mu je optužnim prijedlogom stavljeno na teret.

VIII CRNA GORA

8.1. CIRT

CIRT (Computer Incident Response Team/Tim za odaziv na incidentne situacije kod računarskih sistema) predstavlja organizacionu jedinicu Ministarstva za informaciono društvo i telekomunikacije. Tim je formiran 2011. godine i u dosadašnjem njegovom radu imao veći broj prijava kako od pravnih i fizičkih lica, tako i od partnerskih organizacija iz čitavog svijeta. CIRT Crne Gore je član FIRST udrženja, koji prestavlja krovno međunarodno udruženje za borbu protiv sajber kriminala.

U Tabeli je prikazana broj i struktura prijavljenih incidentnih situacija u sajber prostoru.

	Napad na web sajtove i IS	Finasijske prevare	Prijava fizičkog lica
2012	4	2	1
2013	10	4	9

8.2. Zloupotreba brojeva bankovnih kartica (na internetu i na ATM/POS terminalima)

Trenutno, ova vrsta kriminala je najzastupljenija u Crnoj Gori a i na čitavom Balkanu. Vršeći ove radnje, izvršioci ovih krivičnih djela imaju direktnu novčanu korist koju stiču podizanjem novca na ATM terminalima ili materijalnu koju stiču kupovinom posredstvom POS terminala.

Postoje razni načini kako se vrši priprema ovih krivičnih djela. Kroz razne periode od nastanka kompjuterskog kriminala, razvijali su se i načini kako se dolazilo do brojeva bankovnih kartica. Tako su u početku, kriminalci telefonskim putem i putem pisma, pokušavali da dođu do brojeva bankovnih kartica. Ta metoda koja se i dalje koristi ali ne u velikom obliku, naziva se socijalni inženjering.

Trenutno, najaktuelniji način prikupljanja brojeva bankovnih kartica, obavlja se uz pomoć metode FIŠING *(fishing – prim. prev. pecanje)*. Fišing metoda

se sastoji u tome, da se od lakovjernih korisnika interneta prikupe brojevi bankovnih kartica. Da li će se to uraditi kroz kreiranje internet sajta koji će u svojoj ponudi imati različite proizvode, prilikom čega morate ostaviti brojeve kartica, ili će na vašu elektronsku poštu stići obavještenje od vaše banke da su im hitno potrebni podaci o kartici kako bi izvršili neke ispravke, to zavisi od domišljatosti ili od načinu na koji kriminalac "peca" lakovjerne žrtve, odnosno korisnike interneta. Na ovaj način, kriminaci prikupljaju podatke kao što su: ime i prezime, broj, datum izdavanja i datum isteka kao i CCV broj bankovne kartice. Uz pomoć ovih podataka, može se vršiti trgovina na internetu, on-line kockanje, kupovina internet valute i slično. Mogućnosti korištenja ovako dobijenih podataka su neograničene.

Drugi način prikupljanja digitalnog zapisa bankovnih kartica, vrši se direktno na ATM bankomatima i POS terminalima, gdje kriminalac fizički postavlja elektronski uređaj (*SKIMME*R) na mjesto gde se ubacuje bankovna kartica. Uloga *skimmera* je da sa magnetne trake koja se nalazi na poleđini bankovne kartice očita digitalni zapis i memoriše ga. Kasnije, tako prikupljeni digitalni zapisi se uz pomoć posebnih uređaja, koji su lako dostupni na tržištu, narezuju na bijelu plastiku, odnosno na *blanko* kartice.

Kriminalci, koristeći razne računarske programe u uređaje koji se povezuju direktno na računar, upisuju digitalni zapis. Na ovaj način prave se duplikati originalnih bankovnih kartica.

Brojevi i digitalni zapisi bankovnih kartica koji su na ovaj način prikupljeni, najčešće se prodaju posredstvom zatvorenih internet foruma, a u rijetkim slučajevima postoji mogućnost da lice koje se bavi i prikupljanjem podataka vrši i izradu odnosno zloupotrebu istih.

Na crnom tržištu koje se nalazi u internetu okruženju, mogu naći skrivene internet lokacije, odnosno forumi, na kojima se prodaju brojevi bankovnih kartica. Cijene variraju u odnosu na status ponuđača, kao i porijekla prikupljenih kartica. Na primjer, nije ista cijena brojeva bankovnih kartica koje potiču iz Švajcarske, Njemačke i Holandije kao cijena brojeva kartica koje potiču iz zemalja Jugoistočne Evrope iz razloga platežne moći samih korisnika kartica.

Kriminalci koji dobiju već izrađenu falsifikovanu bankovnu karticu ili brojeve sa bankovne kartice mogu obavljati kupovina na POS terminalima ili podizati novac na ATM terminalima svugdje u svijetu.

Postoje različite mogućnosti otkrivanja ovih krivičnih djela. Većinom sve zavisi od ažurnosti odgovornih banaka koji su izdavaoci bankovnih kartica, banaka koji su vlasnici POS i ATM uređaja na kojima je izvršena zloupotreba kartica, kao i menadžera radnji u kojima se nalaze pomenuti uređaji. Zloupotrebu bankovne kartice može da primijeti ili vlasnik kartice ili odgovorno lice u banci koja je izdavalac kartice. Najčešće se dešava da vlasnik primijeti i prijavi krivično djelo kada uoči da mu se novac sa računa neovlašćeno "ski-

da" ili odgovorno lice u banci kada primijeti da su lokacije sa kojih se podiže novac, ili gdje se koriste bankovne kartice različite. Na primjer, programi u bankama su tako podešeni da se odmah pojavljuje sumnja u skimovanu karticu ukoliko je ista u istom danu korišćena u Sjedinjenim Američkim Državama i u Njemačkoj.

U tom slučaju, kao oštećeni se mogu javiti ili banka ili sam vlasnik bankovne kartice. U Crnoj Gori do sada su se većinom javljale banke kao oštećena pravna lica, jer je u njihovom interesu da zaštite klijenta banke.

Prilikom zloupotrebe brojeva bankovne kartice na internetu, potrebno je prikupiti dovoljan broj dokaza kako bi se nesporno utvrdilo sa koje lokacije i sa kojeg računara je obavljena transakcija kao i koja vrsta aktivnosti je obavljana sa određene lokacije, npr. da li je to bila internet kupovina, internet kladionica ili slično. Banka preko koje je izvršena transakcija mora u krivičnoj prijavi da navede sa koje IP adrese je pristupano određenom internet sajtu, koliko je novca "skinuto" sa računa za koji su vezani brojevi kreditne kartice. Nakon toga, vrši se analiza i identifikacija dobijenih IP adresa.

Analiza se vrši uz pomoć specijalnih javno dostupnih programa koji trebaju da nam utvrde državu i Internet servis provajdera (ISP) iz koje potiču IP adrese , dok se identifikacija IP adresa vrši preko ISP koji treba da nam dostave vlasnika, tačno lokaciju kao i sve druge raspoložive podatke u cilju lociranja mjesta sa koje je izvršeno krivično djelo.

Kako bi se ispunila sva zakonska procedura, a nakon saznanja o brojevima IP adresa sa koje je izvršeno krivično djelo, ovlašćeni policijski službenik se obraća sa zahtjevom prema nadležnom tužiocu koji nakon toga od sudije za istragu traži Naredbu za pretres službenih prostorija ISP u cilju identifikacije dobijenih IP adresa. Nakon izvršenja dobijene naredbe, dobijaju se podaci o lokaciji računara sa koje je izvršeno krivično djelo. Nakon dobijanja ovih podataka, policijski službenici se opet obraćaju nadležnom tužiocu sa ciljem izdavanja Inicijative za pretres stana, stvari i lica.

Prilikom zloupotrebe digitalnog zapisa bankovne kartice, krivičnoj prijavu, poželjno bi bilo da stoje osnovni podaci vezani za kreditnu karticu, ime vlasnika kartice, banka koja je izdala karticu, broj kartice kao i snimci sa ATM uređaja i snimci sa video nadzora koji su u vlasništvu banke. Kasnije, ukoliko je to potrebno, ovlašćeni službenici će zahtijevati i video nadzor sa okolnih objekata a sve u cilju bolje identifikacije izvršioca ovih krivičnih djela.

Važno je napomenuti da svaki ATM uređaj u sebi ima ugrađene male, skrivene digitalne kamere koje su programirane da detektuju i fotografišu svaki pokret u okolini uređaja. Tako da svaki put kada se vrši neka aktivnost na ATM uređajima, bilo da je to ovlašćeno ili neovlašćeno podizanje novca, ugrađene kamere se aktiviraju.

Statistički, u Crnoj Gori većinom su ova djela izvršavana u periodu turističke sezone a izvršioci bili mahom strani državljani koje je veoma teško identifi-

kovati. Stoga se morala ostvariti bolja saradnja između banaka i policije, jer banke posredstvom svojih sistema u realnom vremenu mogu da odrede na kojem ATM/POS terminalu se koristi određeni broj kartice koji je naveden u krivičnoj prijavi. U tom slučaju, sve zavisi od brzine i efikasnosti ili pripadnika Ministarstva unutrašnjih poslova ili sposobnosti radnika obezbjeđenja banke.

Postoje slučajevi u kojima su službenici banke primijetili da je na njihovim ATM uređajima postavljen skimer uređaj, nakon čega su dužni da obavijeste policiju. Ovlašćeni službenici MUP-a u ovom slučaju će postaviti "zamku" kod ATM uređaja kako bi se kriminalci uhvatili prilikom skidanja postavljenog uređaja.

Pretres stana, stvari i lica se vrši nakon dobijanja "naredbe za pretres". Prilikom svakog pretresa, mora se obratiti posebna pažnja na detalje, odnosno da se sačuva autentičnost i integritet digitalnih podataka, koja se obavlja po posebnoj proceduri. U zavisnosti od vrste krivičnog djela, timu koji vrši pretres se ukratko saopšti na koje dokaze treba obratiti pažnju.

U slučaju pretresa prostorija zbog izvršenog krivičnog djela zloupotrebe digitalnog zapisa bankovne kartice na internetu, prilikom pretresa stana, obavezno treba izuzeti: personalne računare, lap topove, kao i sve medijume za smještanje digitalnih podataka. Adekvatnom forenzičkom analizom ovih uređaja, može se doći do podataka kako je pristupano internet sajtovima, koje programe su koristili programeri prilikom izrade navedenog internet sajta, bazi podataka na kojima se nalaze digitalni zapisi bankovnih kartica kao i drugi neposredni dokazi koji ukazuju na izvršenje krivičnog djela.

U slučaju pretresa prostorija zbog izvršenog krivičnog djela zloupotrebe bankovnih kartica na POS i ATM terminalima, treba obratiti pažnju na personalne računare, lap topove, sve medijume za smještanje digitalnih podataka, skimere kao i magnetne čitače odnosno upisivače digitalnih zapisa na kartici, kao i blanko bankovne kartice.

8.3. Distribucija i posjedovanje dječije pornografije

Kako u Crnoj Gori, tako i u zemljama regiona, ovo krivično djelo predstavlja najveći izazov u smislu hvatanja osoba koje vrše ove nedozvoljene radnje kao i modalitete na koji se vrši razmjena nedozvoljenih sadržaja (fotografija i video-klipova) na internetu. U crnogorskom zakonodavstvu još uvjek nije definisano značenje termina dječija pornografija, ali u principu, ona obuhvata svaku zloupotrebu u cilju snimanja ili fotografisanja djece u seksualnim pozama ili seksualnom činu. Osobe koje vrše seksualni čin sa djetetom ili koje uživaju u gledanju dječije pornografije se nazivaju pedofili.

Ekstremna dječija pornografija podrazumijeva djecu do 4-5 godina uzrasta u nedozvoljenim seksualnim pozama sa odraslim ljudima.

Kada se napravi ova vrsta materijala, postoji nekoliko načina kako se ona dalje distribuira. U prošlosti se ova vrsta materijala slala u vidu fotografija i VHS kaseta posredstvom pošte, dok je nastankom interneta, digitalnih kamera i foto aparata, način prenosa i dostave znatno izmijenjen. U vezi sa tim, nije slučajno da se dječija pornografija skoro uvjek povezuje sa internetom i informacionim tehnologijama, zbog toga se i smatra jednim segmentom kompjuterskog kriminala.

Postoji više načina razmjene nedozvoljenog materijala posredstvom interneta. Prvi način je korišćenje torent fajlova i mreža. Torent fajlovi se razmjenjuju uz pomoć "peer to peer" (P2P) protokola, što u principu podrazumijeva razmjenu podataka od korisnika do korisnika. Uz pomoć torenta se razmjenjuju sva dozvoljena dokumenta kao što su knjige, aplikacije i slično, dok se na drugu stranu, uz pomoć njega može vršiti razmjena nedozvoljenog sadržaja kao što je dječija pornografija i piraterija.

Ukoliko kriminalac želi da objavi neku fotografiju ili video zapis posredstvom torent mreže, on se mora prijaviti na neku od mnogih torent internet sajtova, tom materijalu dati naziv i pri tom izvršiti indeksiranje na serveru koji služi za razmjenu torent fajlova. Na ovaj način kriminalci ne ostavljaju sadržaj na serveru, već se isti i dalje nalazi na njegovom računaru, ali će objavljeni indeks sadržati potrebne informacije koje će automatski početi preuzimanje sadržaj sa računara kriminalca. U većini slučajeva, osoba koja je objavila pedofilski materijal nije ni svjesna da druga osoba preuzima materijal s njegovog računara. Takođe, moramo napomenuti da vlasnici internet sajtova na kojima se nalaze pomenuti indeksi, ne znaju čemu isti služe kao i koje vrste informacija nosi.

Postoje nekoliko načina kako se vrši pretraživanje torent fajlova na kojima se nalazi dječija pornografija. Prvi način je da kriminalac koji želi da preuzme dječiju pornografiju zna tačan indeks traženog materijala. Pritiskom na traženi indeks, automatski mu počinje presnimavanje željenog materijala i ostvaruje se, posredstvom već pomenutog P2P protokola, direktna veza između dva korisnika interneta.

Drugi način je osnovnim pretraživanjem po nazivu indeksa. Dovoljno je da na torent internet sajtovima ukucamo željenu ključnu riječ kao što su: djeca, dječija pornografija, seks sa djecom, gola djeca i slično a kao rezultat će nam se pojaviti svi indeksi na navedenom serveru koji u svom nazivu imaju traženu riječ. Ova metoda se rjeđe koristi, iz razloga što kriminalci rijetko stavljaju ovako prepoznatljive riječi u nazivima svojih indeksa.

Kada se preko torent sajtova obično vrši razmjena pedofilskog sadržaja ili se vrši razmjena kolekcije slika i klipova između dva pedofila, kriminalci ne očekuju novčanu korist od pedofilskog materijala koji posjeduju. Jedan od

najboljih i najunosnijih načina za sticanje protiv pravne imovinske koristi je kreiranje tajnih internet sajtova, odnosno foruma na kojima se vrši distribucija ekstremne dječije pornografije. Lokacije ovih internet foruma su jako skrivene a pristup skoro nemoguć. U svijetu internet ili sajber (cyber) kriminala, ova mjesta se zovu podzemlje interneta.

Pristup ovim forumima je strogo čuvana tajna, članovi ovih foruma dobijaju posebne pozivnice za pristup, a prilikom pristupa mora se objaviti neka fotografija pedofilskog sadržaja. Razlog zbog čega se zahtijeva objavljivanje fotografije jeste zbog takozvanih rupa u zakonu, jer su kriminalci svjesni da kada bi policajac objavio neku fotografiju i sam bi izvršio krivično djelo.

Kada članovi foruma žele da prodaju svoju kolekciju, oni objave informaciju da je kreirana datoteka sa pedofilskim materijalom, da je navedena datoteka zaključana šifrom a da se dobijanje šifre naplaćuje posredstvom bankovnih kartica. Cijena pedofilskog materijala se kreće u zavisnosti od količine materijala, vrste materijala (da li su fotografije ili filmovi) kao i starosti djece koja se nalaze na njima.

Drugi način razmjene pedofilskog sadržaja jeste posredstvom programa za komunikaciju. Programi kao što si Skype, ICQ, IRC, Facebook i dr. imaju mogućnost razmjene govora, teksta kao i razmjene digitalnog materijala. Potrebno je samo izvršiti instaliranje željenog programa na svom računaru ili pametnom telefonu i registrujete se na jedan od željenih programa. Ovdje ne predstavlja problem razmjena materijala, već pronalazak osoba sa kojima se vrši razmjena, odnosno drugih pedofila.

Svaki pedofil, prilikom registracije svog imena na neki od navedenih programa, će staviti prepoznatljivu riječ koja će ukazivati da je osoba koja se nalazi iza imena zapravo osoba koja je zainteresovana za razmjenu pedofilskog sadržaja. Odnos i povjerenje između dva pedofila se postepeno gradi i stiče. Prednost u svemu mu daje anonimnost, odnosno laki prestanak komunikacije ukoliko im aspiracije nijesu iste.

Prilikom svake od ovih aktivnosti, postoje određeni digitalni tragovi koji mogu dovesti do izvršilaca ovih krivičnih djela. U slučaju kada se vrši prenos podataka posredstvom torent mreža, na serverima na kojima se vrši indeksiranje, ostaju tragovi u vidu IP adresa kao i adresa elektronske pošte koju dajete prilikom registracije, kojima se može ući u trag. Ista ili slična procedura postoji i kada se registrujete za korišćenje programa za komunikaciju. Prilkom registracije na programima za komunikaciju, mora ostati trag u vidu IP adrese ili elektronske pošte na serverima.

Moramo napomenuti, da i ako je evidentno da je izvršeno krivično djelo i kao dokaz imamo trag u vidu IP adrese ili u vidu naziva elektronske pošte, identifikacija vlasnika je rijetko moguća. Razlog tome je što su serveri na kojima se nalaze potrebni podaci smješteni u zemljama van naše jurisdikcije, najčešće u SAD-u i dobijanje te vrste podataka podliježu procedurama nadležnih država.

Prilikom pretresa prostorija lica koja su izvršila ovo krivično djelo, potrebno je posebno obratiti pažnju na Personalni računar, Lap Top, sve medijume za smještanje digitalnih podataka (USB memorije, eksterni hard diskovi, CD, DVD, VHS kasete, digitalne kamere i foto aparati). Pravilnom i adekvatnom forenzičkom analizom ovih predmeta mogu se ekstrahovati sve vrste podataka. Pod ovim i podrazumijevamo i davno izbrisane podatke sa izuzetih predmeta.

8.4. Klasična djela kompjuterskog kriminala (hakovanje)

Pod hakovanjem se obično podrazumijeva neovlašćeni upad u zaštićenu bazu podataka. Osobe koje vrše ove vrste neovlašćenih upada nazivaju se hakeri.

U dosadašnjoj praksi, imali smo dosta krivičnih prijava podnešenih od strane pravnih i fizičkih lica, ali ipak većina ovih krivičnih djela i dalje ostaje neprijavljena od strane građana iz razloga što u većini slučajeva nije napravljena nikakva materijalna šteta kao i usljed nemogućnosti prikupljana dokaza od strane lica koja podnose prijave.

Postoje više načina kako da se "obori", odnosno "hakuje" određeni internet sajt. Dvije najpopularnije metode su SKL injekcija (SQL Injection) i DDoS napad (Distributet Denial of Service).

U principu SKL injekcija podrazumijeva ubacivanje malicioznog koda u već postojeći programski kod internet sajta. Obično se ovom metodom u internet sajt ubacuje određena vrsta teksta ili fotografija. Ova vrsta krivičnih djela se ne izvršava u cilju sticanja materijalne koristi, već se ista izvršava u cilju sticanja "hakerskog renomea" u internet podzemlju ili već o pokušaju da se hakeri nametnu velikim svjetskim korporacijama koje se bavi sigurnošću na internetu. U svakom slučaju, evidento je da lica vrše krivična djela.

Ukoliko se želi izvršiti napad SKL injekcijom, hakeru je potrebno da posjeduje određenu vrstu računarskih programa, odnosno skripti, koje su posebno napravljene kako bi tražili "rupe" u računarskom kodu. U skriptama se unesu određene sekvence, odnosno niz naredbi, nakon čega skripta neprekidno skenira određeni internet sajt i pokušava pronaći propuste u kodu istog i nakon toga umetnuti određenu unaprijed zadatu sekvencu, odnosno niz željenih riječi.

DDoS napadi su mnogo ozbiljniji način hakovanja internet sajtova od SKL. Ova vrsta hakera se smatraju ozbiljnim neprijateljima nacionalne bezbjednosti, jer za ozbiljan DDoS napad potrebna je velika logistika, dosta vremena i umjeća pravljena različitih računarskih virusa. DDoS napadi se izvršavaju kako na informacionim sistemima velikih korporacija i banaka, tako i nad IT državnih institucija.

DDoS napadi se izvode na način što se u određenom trenutku jednom serveru, sa više računara, šalju upiti za dobijanje informacija. Kada broj upita prema serveru bude prevelik, odnosno broj upita pređe određeni limit koji server može da obradi, dolazi do restartovanja samog servera, ili žargonski rečeno "obaranja" servera. U tom trenutku, sam server postaje ranjiv i lako je izvršiti upad u njega i mijenjati njegovu sadržinu ili preuzeti podatke koji se nalaze u njemu. Obično su to podaci koji imaju status državne tajne ukoliko se radi o upadu u Vladine nformacione sisteme, podaci o bankovnim računima ili se radi o korporacijskoj špijunaži.

Logistika izvršenja DDoS napada je mnogo komplikovanija u praksi nego na papiru. Ukoliko haker želi da izvrši napad na određeni server on mora da u svom posjedu ima veliku "armiju" računara koja je pod njegovom kontrolom.

Pomenuta "armija" ili u internet svijetu nazvana "zombi armija", se stiče na način što hakeri na razne načine ubacuju računarske viruse koji su programirani da zaposjednu računar korisnika interneta. Ubacivanje ovih računarskih virusa se vrši na mnogo načina, ali najčešći posredstvom elektronske pošte, slanjem fotografija ili razmjenom USB memorija i CD/DVD diskova. Kada je u računar umetnut računarski virus, on istog trenutka postaje zombi računar a da toga vlasnici zaraženog računara nijesu ni svjesni. Haker posredstvom njihovih računara može da vrši krivično djelo.

Što je brojnija armija zombija koju posjeduje haker, to je prijetnja po informacione sisteme veća. Nakon zaposijedanja računara korisnika interneta, hakeri na istima instaliraju razne skripte koji su dizajnirane da šalju određeni broj upita prema određenom serveru. Uzmimo primjer da haker u svom posjedu ima preko 2.000 zombi računara, koji u sebi imaju instalirane skripte koje su programirane da u jednoj sekundi šalju preko 1.000 upita prema određenom serveru. Dolazimo do cifre od 2 miliona upita u sekundi. Ukoliko je server napravljen da podnese manji broj upita, doći će do njegovog zagušenja i obaranja.

U svakom od ovih slučajeva, radnje dokazivanja su veoma teške. Moraju se posjedovati različiti kompjuterski programi kako bi se izvršilo nadziranje računara koji koriste hakeri kao i pronalaženje prave IP adrese sa koje je izvršen DDoS napad. Ukoliko se dođe do prave IP adrese sa koje je izvršen napad ili eventualno do IP adrese sa koje je zaražen neki od zombi računara, mora se pristupiti, kao i u svim slučajevim do sada, identifikaciji IP adresa kao i pronalasku vlasnika navedene IP adrese.

Prilikom pretresa prostorija, potrebno je izuzeti personalni računar kao i sve medijume za smještanje digitalnih podataka. Digitalnom forenzikom nad oduzetim predmetima se izvršava analiza u cilju pronalaženja računarskih programa, izvornih kodova virusa i svih drugih kodova u cilju dokazivanja sredstva izvršenja krivičnog djela.

8.5. Piraterija

U principu, pod piraterijom se smatra svaka prodaja i iskorišćavanje autorskog djela za koju prodavac ne posjeduje autorska prava. Najviše je zastupljena prodaja piratskog materijala na CD i DVD-ovima. Obično su na navedenim diskovima nasnimljeni filmovi i muzika, kao i poslednji računarski programi, odnosno operativni sistemi.

Stopa piraterije u Crnoj Gori po statistikama prevazilazi 80 posto. Ovaj podatak je alarmantan, kada se uzme u obzir da je najveći u regionu.

Postoje dva načina na koji se distribuira piraterija. Ulična prodaja u Crnoj Gori je veoma zastupljena, dok on-line prodaja na internet stranicama skoro i da nema, ali se ne smije zanemariti.

U oba slučaja šteta koja se nanosi budžetu Crne Gore je veoma velika, dok je interesovanje za originalnim izdanjima veoma malo ili ga nema.

Već smo u dijelu kada smo pričali o dječijoj pornografiji, opisali funkcionisanje torent mreža i čemu služe torent dajlovi.

Princip preuzimanja filmova, muzike i računarskih programa je isti.

Kada kriminalac preuzme navedeni materijal za koji nema autorsko pravo, isti može distribuirati na gore dva pomenuta načina: on-line i ulična prodaja.

Za on-line prodaju, potrebno je da posjeduje solidno znanje o izradi internet stranica. Internet stranica se dizajnira tako da se ostavlja mogućnost direktnog preuzimanja filmova i muzike uz novčanu naknadu. Takođe, postoji mogućnost pravljenja internet stranica na kojima se plaća mjesečna članarina i sa kojih možete direktno da gledate i preuzimate filmove. U ovim slučajevima, procedura pronalaženja lica koja su dizajnirala stranicu i koja su odgovorna za rad iste, dosta zavisi od inostranih službi, jer su podaci o IP adresama sa koje se vrši administracija navedenog sajta obično u inostranoj nadležnosti.

Za uličnu prodaju, kriminalac mora da posjeduje dobar štampač u boji, kako bi mogao da štampa korice za filmove. Kada se izvrši nasnimavanje materijala na praznim DVD i CD-ovima, isti dalje plasira, da li kroz svoju mrežu prodavaca ili on lično.

Kada se vrši pretres prostorija zbog izvršenja ovog krivičnog djela, mora se obratiti pažnja kako bi se izuzeli računar, lap-topovi, printeri, kao i svi drugi medijumi za smještanje digitalnih podataka. Forenzičkim vještačenjem oduzetog materijala, može se utvrditi sa kojih stranica je izvršio “skidanje” navedenog materijala, lista njegovih kupaca i distibutera.

IX NACIONALNI PRAVNI OKVIR MATERIJALNO-PRAVNI I PROCESNO-PRAVNI OKVIR VISOKOTEHNOLOŠKOG KRIMINALA U CRNOJ GORI

9.1. Kada je u pitanju oblast visokotehnološkog kriminala, koji obuhvata kriminalne aktivnosti u kojima su kompjuteri i slični informatički uređaji i kompjuterska mreža predmet, sredstvo, cilj ili mjesto krivičnog djela, Crna Gora je svoj zakonodavno pravni okvir, koji pravno onemogućava svaki vid slučajnog ili namjernog narušavanja i sprječavanja funkcionisanja info--rmatičkog sistema, započela da izgrađuje u posljednjih nekoliko godina, praktično možemo reći od 2005.godine i to čini kroz reformu krivičnog zakonodavstva.

Odgovarajući zakonski okvir predstavlja sponu pravne i informacione obla--sti koja će zajedničkom saradnjom doprinijeti uspješnom rasvjetljavanju slučajeva iz oblasti računarskog kriminala i sankcionisanja počinilaca.

Ustav Crne Gore u članu 9 predviđa da su potvrđeni i objavljeni međunarodni ugovori i opšteprihvaćena pravila međunarodnog prava sastavni dio unutrašnjeg pravnog poretka i da imaju primat nad domaćim zakonodavstvom i neposredno se primjenjuju kada odnose uređuju drugačije od unutrašnjeg zakonodavstva.

Evropska konvencija iz 1959. godine o pružanju međusobne pravne pomoći u krivičnim stvarima predstavlja preteču Konvencije o računarskom kriminalu (Sajber kriminalu), koja je donijeta da bi poslužila kao okvir državama koje žele da pravno kodifikuju ovu vrstu društveno opasnog ponašanja.

Kada je u pitanju oblast računarskog kriminala, Crna Gora je 2005.godine potpisala Konvenciju koja je poznata kao Budimpeštanska konvencija i koja je donijeta 21.11.2001. godine, a na snazi je od 2004.godine.

Crna Gora je 03.03.2010. godine donijela Zakon o potvrđivanju Konvencije o računarskom kriminalu, koji je stupio na snagu 01. 07.2010. godine, a

takođe je ratifikovala i dodatni Protokol o rasizmu i ksenofobiji (CETS 189), kao i Konvenciju o zaštiti djece od seksualne eksploatacije i seksualnog zlostavljanja (CETS 201).

Nakon što je donijela zakone o potvrđivanju odnosno ratifikaciji konve--ncija, Crna Gora je kroz reformu krivičnog zakonodavstva pristupila implementaciji i usklađivanju svog nacionalnog pravnog okvira (zakonodavstva) sa odredbama ovih konvencija kao i sa odredbama ***Okvirne odluke Savjeta Evrope 2005/222*****,** koja govori o napadima na informacione sisteme i ***Okvi--rne odluke Savjeta Evrope 32000D0375*** koja govori o suzbijanju dječije pornografije na internetu.

Osim ovog Crna Gora je potpisala u Dubrovniku 15.02.2013. godine *Regionalnu deklaraciju o strateškim prioritetima u borbi protiv računarskog kriminala*, u kojoj su prepoznati strateški prioriteti u borbi protiv ove vrste kriminala koje ova strategija prati i dalje razvija, kroz period od 2013. do 2017. godine i strategijom Sajber bezbjednosti koja između ostalog definiše ključne korake u jačanju kapaciteta i obukama za efikasnu borbu represivnih organa protiv računarskog kriminaliteta.

Shodno Konvenciji o računarskom kriminalu, Crna Gora aktivno učestvuje u radu TC-Y Komiteta Savjeta Evrope koji prati sprovođenje Konvencije o računarskom kriminalu, a ima i svog predstavnika, odnosno kontakt tačku 24/7 u mreži Savjeta Evrope, koja je uspostavljena na osnovu Konvencije o računarskom kriminalu i koja je dužna da u svakom trenutku bude na raspolaganju u davanju asistencije ostalim članicama Savjeta Evrope u stvarima vezanim za računarski kriminal, a tiče se Crne Gore.

9.2. Kako Konvencija o računarskom kriminalu obuhvata široku lepezu krivičnih djela koja se tiču računara, računarske mreže, to obuhvata i ostala krivična djela kod kojih se u njihovom izvršenju na bilo koji način koristi kompjuter. U tom smislu crnogorsko krivično zakonodavstvo, poslednjih godina, usaglašavalo je svoje odredbe sa odredbama Budimpeštanske konvencije, pa su tako u XIII glavi pod pojmom „Značenje izraza“ u članu 142 Krivičnog zakonika unijete definicije, odnosno značenje određenih pojmova koji su od značaja za krivična djela protiv bezbjednosti računarskih podataka, a definicije se zasnivaju na savremenoj kompjuterskoj tehnologiji i informatici, te mogu da posluže i budu od značaja i za primjenu drugih krivičnih djela čije izvršenje je povezano sa kompjuterom. Mogu se primijeniti i kod onih krivičnih djela koja u svom činjeničnom opisu nemaju te pojmove.

Tako pod tačkom 15 (tačka 18 izmjenama i dopunama Krivičnog zakonika Sl. list 40/13)

Računarski podatak i računarski program smatra pokretnom stvari

Određivanjem računarskog podatka, odnosno računarskog programa kao pokretne stvari, zakonodavac je želio da pruži krivičnopravnu zaštitu i kod drugih krivičih djela kod kojih se direktno u zakonskom opisu bića krivičnog djela ne pojavljuje pojam Računarskog podatka ili računarskog programa, tako da stavljanjem kao definisanog pojma stvari, odnosno pokretne stvari računarskog podatka, predviđena je krivičnopravna zaštita i kod onih krivičnih djela koja su upravljena protiv imovine. Sledstveno tome, računarski program i računarski podatak mogu se oduzeti od bilo kojeg lica za koje postoji osnov sumnje da je počinio određeno krivično djelo, a u skladu sa ostalim odredbama koje važe za oduzimanje predmeta.

Pod tačkom 16 (tačka 19) **računarskim sistemom** se smatra svaki uređaj ili grupa međusobno povezanih ili uslovljenih uređaja, od kojih jedan ili više njih u zavisnosti od programa vrši automatsku obradu podataka.

Pod tačkom 17 (tačka 20) **računarskim podatkom** smatra se svako izlaganje činjenica, podataka ili koncepata u obliku koji je pogodan za obradu u računarskom sistemu, uključujući i tu programe pomoću kojih računarski sistem vrši svoje funkcije.

Pod tačkom 18 (tačka 21) **računarskim programom** smatra se skup uređenih računarskih podataka na osnovu kojih računarski sistem vrši svoje funkcije.

Pod tačkom 19 (tačka 22) **računarski virus** je računarski program koji ugrožava ili mijenja funkcije računarskog sistema i mijenja, ugrožava ili neovlašćeno koristi računarske podatke.

Pod tačkom 20 (tačka 23) **Podacima o računarskom saobraćaju** smatraju se svi računarski podaci koje generišu računarski sistemi, koji čine lanac komunikacije između dva računarska sistema koji komuniciraju uključujući i njih same.

Uvodeći ove pojmove i definicije u materijalno zakonodavstvo, Crna Gora je u potpunosti usaglasila svoje nacionalno zakonodavstvo sa Konvencijom o računarskom kriminalu, i, kroz uvođenje nove glave u Krivični zakonik, „Krivična djela protiv bezbjednosti računarskih podataka“, obuhvatila sva krivična djela visokotehnološkog kriminala. Član 2 Konvencije koji govori o krivičnom djelu nedozvoljenog pristupa kompjuterskom sistemu ili njegovom dijelu, sa namjerom pribavljanja kompjuterskih podataka; član 3 Konvencije koji govori o bespravnom presretanju prenosa kompjuterskih podataka koji nijesu javne prirode ka kompjuterskom sistemu i član 4 Konvencije koji govori o bespravnom oštećenju brisanju, kvarenju, mijenjaju ili prikrivanju kompjuterskih podatka, inkorporirani su *u naš Zakon.*

9.3. Član 353 Krivičnog zakonika - krivično djelo neovlašćeni pristup računarskom sistemu.

Ovo djelo postoji ako se učini neovlašćeni pristup računarskom sistemu, bilo kao cjelini ili nekom njegovom dijelu, i ono ima osnovni i dva teža oblika ispoljavanja. Za osnovni oblik ili stav 1 predviđena je , novčana kazna ili zatvor do jedne godine, a ako se učini teži oblik odnosno ako su prekršene mjere zaštite računarskog sistema (*to je slučaj kada učinilac pristupa računaru uz kršenje softverske mjere koja je poznata pod nazivom "password" ili lozinka, i predstavlja tajni kod koji je unijet u računar od strane vlasnika računara i bez njegovog znanja računaru se ne može pristupiti odnosno računar se ne može uključiti niti ući u određeni program),* učinilac će se kazniti novčanom kaznom ili zatvorom do tri godine.

U stavu 5 ovog člana se govori da, ukoliko se djelo izvrši radnjama koje su opisane pod stavom 1, 2, 3 i 4, tada se radi o neovlašćenom pristupu zaštićenom računaru, računarskoj mreži, neovlašćenom presrijetanju računarskih podataka ili uništavanju takvih podataka, i ako su pri tom nastupile teže posljedice za drugog, takvi počinioci će se kazniti zatvorom od 6 mjeseci do 5 godina. Kao teži oblik izvršenja ovog djela se navodi kad neko krši bezbjedonosni sistem zaštite, odnosno upada ili pristupi određenom računaru na način što povrijedi mjeru zaštite.

Kao mjera zaštite se pojavljuje tzv. lozinka ili softverska mjera, s tim da je kod nas odomaćen naziv "Password", a *password* predstavlja tajni podatak koji je unijet u računar od strane onoga ko koristi taj računar, kojim se pokušava spriječiti upad, odnosno neovlašćeno korišćenje tog kompjutera, bez znanja lica koje koristi kompjuter. Ovo krivično djelo može da učini svaki pojedinac ili bilo koje lice, u zakonodavstvu postoji tzv. grupa ili kategorija lica koja su poznata pod nazivom "hakeri". Oni se iz različitih motiva bave ilegalnim pristupanjem računarskim sistemima i hakeri su obučeni da savladaju i najsloženije mjere zaštite koje određeni kompjuterski sistem posjeduje.

Kod ovog djela je bitno da postoji uzročno-posljedična veza između posljedice koja je nastupila i koja se ispoljava kao teška za drugog, i preduzete radnje upada u zaštićeni računarski sistem.

Poseban oblik ovog krivičnog djela postoji kada imamo neovlašćeno presrijetanje računarskih podataka i tu je, po zakonu, potpuno irelevantno hoće li to biti presrijetanje podataka koji idu ka kompjuteru ili unutar samog kompjutera ili od kompjutera, i pri tom, uključuje se i elektromagnetna emisija. Međutim, to se ne odnosi na svako presrijetanje tih podataka, već samo onih koji ne smiju biti javne prirode, jer ukoliko se radi o podacima koji su javne prirode onda ne bi postojalo krivično djelo.

Takođe predviđene su i kazne za lica koja upotrijebe podatke dobijene na ovaj način, i to novčanom kaznom i zatvorom do tri godine.

Do izmjena i dopuna Krivičnog zakonika, koji su objavljeni u "Službenom listu CG", br. 25/10, ovi članovi Budimpeštanske konvencije bili su kodifikovani kao posebna krivična djela, dok su ovim zadnjim izmjenama KZ-a, svrstana pod ovaj član i pod ovo krivično djelo, tako da sada postoji 5 stavova krivičnog djela „neovlašćen pristup računarskom sistemu", a više nema kao posebna krivična djela „neovlašćen pristup zaštićenom računaru i računarskoj mreži" i „sprječavanje i ograničavanje pristupa računarskoj mreži", već su ova krivična djela unijeta kao stavovi pomenutog krivičnog djela "neovlašćen pristup računarskom sistemu", opisanog članom 353 KZ.

9.3.1. Primjer:

Neovlašćen pristup određenom zaštićenom računaru, zaštićenoj računarskoj mreži, postojaće npr. ako u pravosuđu imamo našu pravosudnu mrežu u kojoj pristup imaju zaposleni-službenici odnosno namještenici i sudije. Da bi određeni namještenik ili sudija pristupio pravosudnoj mreži neophodno je da unese svoju lozinku, odnosno svoj password, jer se radi o zaštićenoj mreži. Ukoliko neko lice to učini tako što je pristupilo serveru, otvorilo e-mail sudije, odnosno namještenika, a za to nije imao ovlašćenja, i neovlašćeno je pregledao sadržaj te pošte, to lice je počinilo neovlašćen pristup zaštićenom računaru ili računarskoj mreži.

Kako može da se vrši sprječavanje i ograničavanje pristupa javnoj računarskoj mreži navešćemo kao primjer pravosudnu mrežu koja postoji u Crnoj Gori i internet sajt sudske prakse. Ako se na taj sajt sudske prakse, odnosno na taj određeni server, pošalje ogroman broj ili veći broj bilo kakvih, a najčešće beskorisnih informacija, doći će do zagušenja saobraćaja prema tom serveru i time će biti onemogućeno da se pristupi mreži i uslugama koje taj sajt pruža. To se vrši pomoću tzv. malicioznog softvera, pomoću koga se vrši kontrola na softverima više računara. Složićemo se, veoma teško za dokazivanje, ali postoji.

9.4. Član 5 Konvencije govori o ometanju računarskog sistema i njime se predviđa da se bespravno i u većem stepenu ometanje funkcionisanja kompjuterskih sistema koje je učinjeno putem unošenja, prenošenja, oštećenja, brisanja, ili mijenjanja, ili prikrivanja kompjuterskih podataka, smatra krivičnim djelom. Crna Gora je ovaj član implementirala kroz **član 350** koji govori o **ometanju računarskog sistema** (*ovo krivično djelo u ranijem krivičnom zakonodavstvu je bilo poznato pod nazivom "računarska sabotaža"*).

Kao radnja izvršenja ovog krivičnog djela pojavljuje se unošenje, uništenje, brisanje, izmjena, oštećenje, prikrivanje ili na bilo koji drugi način činjenje nepotrebnim određenog računarskog podatka ili računarskog sistema, a objekat te radnje jeste računarski podatak ili računarski sistem, ali i računar,

odnosno drugi uređaj za elektronsku obradu ili prenos podataka. Da bi neko mogao biti krivično odgovoran po ovom članu nije neophodno samo da se preduzme neka od ovih radnji, već je neophodno da ta radnja koja se preduzima da se preduzima sa namjerom da ometa rad računarskog sistema. To znači, da ukoliko nedostaje ovaj subjektivan element, neće postojati ni ovo krivično djelo. Taj subjektivan element se cijeni samo u odnosu na mijenjanje, uništenje, prikrivanje računarskog podatka ili računarskog sistema.

Ako se radi o oštećenju, odnosno ako je djelo učinjeno prema sistemu koji je od značaja za državne organe, javne službe, privredna društva, onda će postojati teži, odnosno kvalifikovani oblik ovog djela, i za njega je predviđena kazna zatvora od 1 do 8 godina, dok je za osnovni oblik predviđena novčana kazna ili kazna zatvora do 3 godine.

Ovo krivično djelo kod nas je kažnjivo bez obzira kome računar, odnosno računarski sistem pripada, dok npr. u zemljama regiona (Srbiji) da bi ovo krivično djelo postojalo, neophodno je da objekat napada - računar ili računarski sistem pripada državnom organu ili nekoj javnoj ustanovi, što kod nas predstavlja samo teži oblik ovog krivičnog djela.

U stavu 3 ovog člana Krivičnog zakonika predviđeno je da će se uređaji i sredstva, kojima se izvrši ovo djelo, oduzeti tako što će im se izreći mjera bezbjednosti- oduzimanja predmeta, ali oni će se obavezno oduzeti samo u onom slučaju kad se dokaže da su u svojini počinioca, a ukoliko nijesu u svojini počinioca onda tu imamo ograničenje koje predviđa član 75 stav 2 Krivičnog zakonika, gdje ako se radi o stvarima i predmetima koji nijesu svojina učinioca oduzeće se samo onda ako to zahtijevaju razlozi bezbjednosti ljudi, imovine, ili razlozi morala, ili kad i dalje postoje opasnosti da će biti upotrijebljeni za izvršenje krivičnog djela, a time se ne dira u svojinu, odnosno prava trećih lica.

Sudovi mogu vršiti oduzimanje predmeta i sredstva koji nijesu svojina učinioca krivičnog djela koji je oglašen krivim, samo ako bi se dokazalo ili moglo dokazati da će oni biti upotrijebljeni u izvršenju novih krivičnih djela. Ovdje je pitanje bezbjednosti moguće primijeniti samo ako se radi o kvalifikovanom obliku ovog krivičnog djela a to je ometanje računarskih sistema, koji su od značaja za državne organe, javne službe ili ustanove. U svim ostalim slučajevima veoma bi bila diskutabilna primjena ove mjere bezbjednosti.

9.5. Član 6 Konvencije govori o zloupotrebi uređaja i to da će se krivično sankcionisati proizvodnja, prodaja, nabavljanje radi upotrebe; uvoz, distribucija i drugi način stavljanja na raspolaganje kompjuterske programe, projektovane ili preuređene prvenstveno za vršenje nekog od krivičnih djela koja su kodifikovana u članovima 2, 3, 4 i 5 Konvencije, te kompjuterskih loziniki, šifri za pristup bez kojih se ne može pristupiti kompjuterskom

sistemu. Ovaj član kod nas je predviđen kao krivično djelo u članu 354 i govori **o zloupotrebi uređaja i programa.**

Kada govorimo o njegovom karakteru možemo reći da on ima karakter delikta, prepreke, odnosno njime je inkriminisana proizvodnja, prodaja, nabavljanje radi upotrebe i stavljanja na raspologanje bilo kojeg uređaja ili sredstva koji može da posluži za izvršenje svih krivičnih djela iz XXVIII glave Krivičnog zakonika, odnosno za izvršenje svih krivičnih djela u vezi sa kompjuterima.

Kada ovo djelo posmatramo i hoćemo vidjeti šta je njegova radnja, a šta objekat, onda moramo reći da je radnja svako umnožavanje, prodaja, proizvodnja, nabavljanje radi upotrebe bilo kojeg podatka koji je predmet zloupotrebe, dok je objekat radnje uređaji ili računarski programi koji su projektovani, ili su prilagođeni, da bi se vršilo neko djelo iz ove XXVIII glave.

Za ovo krivično djelo našim zakonom je predviđena kazna zatvora od 3 mjeseca do 3 godine, s tim da je predviđen i lakši oblik ovog krivičnog djela koji se odnosi na samo posjedovanje bilo kojeg sredstva ili podatka koji je predmet ove inkriminacije. Dakle, za ovaj lakši oblik nije potrebno da se dokazuje namjera počinioca da želi sa time da nešto učini, već je dovoljno da samo posjeduje ta sredstva i podatke koji mogu da se upotrijebe u izvršenju krivičnog djela.

XXVIII glava Krivičnog zakonika, osim ovih krivičnih djela, sadrži još i krivična djela „pravljenja i unošenja računarskih virusa", što je predviđeno članom 351 i „računarsku prevaru" u članu 352 KZ.

9.6. Krivično djelo „pravljenje računarskog virusa" (član 351 Krivičnog zakonika) radi njegovog unošenja u kompjuterski sistem, po našem krivičnom zakonodavstvu je kažnjivo novčanom kaznom ili zatvorom do jedne godine, a ako je sa tim računarskim virusom, koji je unijet u računar ili računarsku mrežu, prouzrokovana šteta, onda će djelo biti teže sankcionisano, novčanom kaznom ili zatvorom do dvije godine.

Šta je to računarski virus. Taj pojam je kod nas objašnjen u članu 142 Krivičnog zakonika u značenje izraza i pod njim se podrazumijeva program koji ugrožava ili mijenja funkcije računarskog sistema, odnosno program koji ugrožava ili neovlašćeno koristi računarske podatke. Kod ovog krivičnog djela dilema se javila kada se djelo smatra svršenim, pa je uzeto da je djelo izvršeno kada je računarski virus, odnosno računarski program napravljen, a ono će ostati u pokušaju ako se preduzme samo određena radnja u cilju pravljenja računarskog virusa ili programa.

Takođe, djelo će biti učinjeno i ako taj računarski virus ili program nije unijet u tuđi računar, ali kod onog koji je otkriven i kod koga je pronađen taj računarski virus, ako se dokaže da je on napravljen u namjeri da se unese

u tuđi računarski sistem, dakle potrebno je da se dokaže direktan umišljaj. Ovdje je bez značaja da li je učinilac sam napravio taj virus ili je do njega došao na drugi način. Kao posljedica ovog krivičnog djela se javlja šteta i to u bilo kom svom obliku, apsolutno je nebitno je li ta šteta imovinski izražena. Šteta se može ogledati u gubitku nekog podatka, nekog programa, može se ogledati u činjenici da je došlo do zastoja u radu računara ili da je od unošenja tog virus ili podatka nastupio slabiji rad samog računara.

Dakle, dovoljno je samo da taj računarski virus funkcionalno proizvede štetu za funkcionisanje računarskog sistema. I za ovaj oblik je potreban umišljaj. Kod ovog krivičnog djela predviđeno je oduzimanje računarskog virusa.

I ako imamo zakonski određenu definiciju računarskog virusa, pitanja poput toga šta su to virusi, kako se prave, koje su njihove vrste i karakteristike, šta je njihova sadržina, predstavljaju pitanja koja sudsko vijeće mora da riješi u svakom konkretnom slučaju, kao faktičko pitanje. U tome sudu će pomoć pružiti stručno lice koje raspolaže određenim znanjima i vještinama, odnosno vještaci informatičke struke.

U sudskoj praksi Njemačke postoji slučaj da je jedan 18-o godišnji haker svojim virusom zarazio preko 20 miliona kompjutera za veoma kratak vremenski period, od svega par dana, i to je učinio tako što je svoj virus pustio i na taj način onemogućio dalji rad na određenom broju kompjutera, a na drugome je došlo do uništenja svih podataka. Epilog takvog krivičnog postupka u Njemačkoj je bio da je lice osuđeno na 21 mjesec zatvora.

9.7. Član 8 Konvencije govori **o prevarama u vezi sa kompjuterima**, i mi smo ih kodifikovali kroz krivično djelo **„računarske prevare"** pa se pod računarskom prevarom smatra:

- bilo kakvo unošenje, mijenjanje, brisanje ili prikrivanje kompjuterskih podataka;
- ili bilo kakvo ometanje rada računarskog sistema kojim se utiče na rezultat elektronske obrade, prenosa podataka, i funkcionisanja računarskog sistema, a pri tom se djeluje prevarno, odnosno sa namjerom da se sebi ili drugom pribavi protivpravna imovinska korist, a drugom prouzrokuje imovinska šteta.

Za ovo krivično djelo koje je kod nas kodifikovano članom 352 Krivičnog zakonika, može se reći da zauzima centralno mjesto u skupini računarskih krivičnih djela. Naš zakonodavac za počinioce ovog krivičnog djela predviđa kaznu zatvora od 6 mjeseci do 5 godina u osnovnom stavu, dok za teže oblike, a oni postoje ako je imovinska korist koja je pribavljena ili šteta koja je načinjena u iznosu većem od 3000€, onda je kazna od najmanje 2 godine do 10 godina i otišlo se još korak dalje, i ukoliko je ta imovinska šteta ili korist prešla granicu od 30.000€, onda je kazna zatvora od 2 do 12 godina. Dakle, vidi se da je kazna za počinioce ovog krivičnog djela određena u za-

visnosti od visine pribavljene imovinske koristi.

Ovo krivičnog djela zakonodavci smatraju za *specijalis* krivično djelo u odnosu na opšte krivično djelo prevare, jer ono i zaista jeste poseban oblik prevare, ali ono što ga razlikuje od klasične prevare jeste što za računarsku prevaru nema dovođenja ili održavanja u zabludi nekog lica, jer to u suštini nije ni moguće učiniti, pa se računarska prevara ne može svrstati u opšte krivično djelo prevare.

Kako ovdje prepoznati radnju izvršenja krivičnog djela?

Radnja izvršenja ovog krivičnog djela čini unošenje nekog podatka, brisanje nekog podatka, propuštanje da se unese neki podatak ili se, na bilo koji drugi način a koji nije ovim opisan, taj podatak prikrije ili lažno prikaže, ili na bilo koji način omete računarski sistem a da ta radnja koja se preduzima, preduzima se elektronskim putem i da taj podatak koji se na taj način uništava, prikriva, lažno prikazuje, utiče na rezultat elektronske obrade u onom izvornom smislu kako bi ona bila.

Šta je posljedica računarske prevare?

Posljedica ovih preduzetih radnji jeste da se dobije određeno stanje na računaru ili u računarskom sistemu koje ne bi bilo dobijeno, niti bi se do njega moglo doći a da nije taj podatak unijet, izbrisan, promijenjen.

Kada se ima taj podatak, odnosno kada je preduzeta radnja izvršenja ovog krivičnog djela u smislu njenog unošenja, prikrivanja, tada imamo objektivan uslov, s tim da onda moramo imati i subjektivnu stranu krivičnog djela, a to je da je umišljaj počinioca upravljen, dakle, da se unese, ošteti, ili prikrije taj podatak u računarski sistem, sa namjerom da se sebi ili nekom drugom pribavi korist, i to protivpravna imovinska korist, ili da se drugom prouzrokuje šteta.

Za sudije je veoma suptilno dokazati na koji način će se povezati umišljaj počinioca, koji vrši računarsku prevaru, sa njegovim subjektivnim odnosom da upravo tim podatkom on prouzrokuje imovinsku štetu, odnosno pribavlja protivpravnu imovinsku korist.

Da bi ovo djelo bilo dovršeno potrebno je da se i ta namjera ostvari.

Kada se govori o računarskoj prevari kao krivičnom djelu, ono u svoja dva stava ima sublimirano da se pribavi korist i nanese šteta i to je taj teži oblik računarske prevare i on je, kao takav, i teže kažnjiv, odnosno zaprijećen je veoma visokim kaznama zatvora. Kod nas postoji i tzv. privilegovani oblik računarske prevare, a to je da kada učinilac unese, promijeni, uništi ili na drugi način prikrije određeni podatak i to čini sa ciljem da drugom nanese štetu, dakle, nema namjere da sebi ili drugom pribavi korist, već to samo može učiniti sa namjerom da nanese štetu i da bi to djelo bilo dovršeno potrebno je da je ta namjera i ostvarena, odnosno da je ta šteta prouzrokovana. Za ovo djelo učinilac će se kazniti kaznom zatvora do 2 godine.

9.7.1. Primjer:

Polje gdje dolazi do pojave ovih krivičnih djela između ostalih jeste kod tzv. sportskih kladionica. Lica koja se bave i rade sa kompjuterima su izmjenom samo jednog podatka a taj podatak se odnosi na vrijeme, dakle na realno vrijeme na koje je podešen kompjuter, izmijenili taj podatak, izmijenili su ga sa namjerom da time pribave protivpravnu imovinsku korist za sebe i da nanesu štetu sportskim kladionicama u kojima su zaposleni, jer kod prognoziranja sportskih rezultata je veoma opipljivo unošenje takvog podatka.

Društvena mreža Facebook, kao što znamo i svjedoci smo, ima 800.000.000 korisnika. Na toj Facebook mreži veoma često dolazi do krađe identiteta da bi se vršile zloupotrebe sa istim, a ta krađa identiteta vrši se tako što se prvo izvrši krađa korisničkog imena i lozinke, zbog čega se vrši krađa identiteta. Ona može da se vrši i u cilju izvršavanja nekih drugih krivičnih djela i u tom slučaju uglavnom je povezana sa tim djelima npr. određeno poznato lice ima svoj profil, krađom njegovog identiteta i korišćenjem tog identiteta može da se prema tom licu počini uvreda, kleveta, iznošenje ličnih i porodičnih prilika, pa može doći i do sticaja određenih krivičnih djela.

Računarske prevare, kao krivična djela, predstavljaju najširi oblik računarskog kriminaliteta. Broj oblika prevare, kao i način njihove realizacije praktično je neograničen. U praksi se susrijeću, kako one prevare koje su veoma primitivne, možemo reći i grube, tako i one računarske prevare gdje postoji veliki stepen vještine i rafiniranosti u preduzetim radnjama i veoma teško ih je otkriti. Za kompjuterske prevare može se reći da predstavljaju jedan vid međunarodnog kriminaliteta, zbog radnje kojom se vrše i sredstava kojima se vrše. Zbog dostupnosti interneta kao tržišta, ove prevare se veoma brzo šire internetom, a i troškovi njihovog izvođenja su veoma niski. Kompjuterski prevaranti, odnosno počinioci kompjuterskih prevara, zloupotrebljavaju upravo karakteristike sajber prostora koje doprinose rastu elektronske trgovine, a to su anonimnost, distanca između prodavca i kupca, kao i trenutnu prirodu transakcija. Oni upravo i koriste tu prednost da prevara preko interneta ne zahtijeva pristup do nekog sistema za isplatu, kao što je to npr. neophodno da se učini kod obične prevare, već računarska prevara, kroz digitalno tržište koje još uvijek nedovoljno uređeno i kako takvo konfuzno za potrošače, u stvari predstavlja idealno mjesto za računarsku prevaru, Iz tog razloga svi moramo biti obazrivi kada putem interneta nešto kupujemo ili prodajemo ili vršimo bilo koju novčanu transakciju.

9.8. Crna Gora je izvršila harmonizaciju Krivičnog zakonika (glava XXVIII) sa Budimpeštanskom konvencijom, odnosno njenim članovima od 2 do 8 i na taj način ispoštovala preporuke iz te Konvencije.

Osim krivičnih djela koja su svrstana u Posebnu glavu krivičnih djela protiv bezbjednosti računarskih podataka Krivičnog zakonika, članom 211

Krivičnog zakonika predviđeno je i krivično djelo koje se tiče suzbijanja dječije pornografije i nosi naziv „prikazivanje pornografskog materijala djeci i proizvodnja i posjedovanje dječije pornografije". Naime, okvirnom odlukom Savjeta Evrope 32000D0375 predviđeno je niz konkretnih mjera o suzbijanju dječije pornografije na internetu, a u cilju prevencije i suzbijanja proizvodnje, obrade, posjedovanja i distribucije materijala sa dječijom pornografijom, kao i efikasnosti istraga i krivičnog progona za prestupe iz ove oblasti. U pomenutom članu Krivičnog zakonika inkorporirana je i odredba člana 9 Konvencije o sajber kriminalu, koji predviđa da nacionalna zakonodavstva država članica trebaju da predvide kao krivična djela radnje koje se učine namjerno i bespravno, a tiču se proizvodnje dječije pornografije u cilju njene distribucije preko kompjuterskih sistema, te nuđenje ili stavljanje na raspolaganje dječije pornografije preko kompjuterskih sistema; distribucije dječije pornografije; dobavljanja dječije pornografije bilo za sebe ili za drugog i samo posjedovanje dječije pornografije u kompjuterskom sistemu, a sve preko kompjuterskih sistema.

Pod pojmom ili izrazom *dječije pornografije* podrazumijeva se pornografski materijal koji vizuelno prikazuje:

- maloljetnika koji učestvuje u seksualnom činu
- lice po čijem se izgledu može zaključiti da je maloljetnik koji učestvuje u tom činu
- realističke slike koje predstavljaju maloljetnika koji učestvuje u tom činu.

Kada se govori o maloljetniku misli se na lica mlađa od 18 godina, mada ovim članom je ostavljena mogućnost da države članice mogu da postave i drugačiju starosnu godinu s tim da ona ne može biti manja od 16 godina. Države takođe mogu da rezervišu pravo u cjelini ili djelimično u vezi stavova o tome šta se podrazumijeva pod dječijom pornografijom.

Za krivično djelo „prikazivanje pornografskog materijala djeci i proizvodnja i posjedovanje dječije pornografije" može se izreći kazna zatvora i do 5 go--dina onome ko iskoristi maloljetnika za proizvodnju slika, audio-vizuelnih i drugih predmeta pornografske sadržine i ko nabavlja, prodaje, prikazuje ili prisustvuje prikazivanju ili na drugi način učini dostupnim audio-vizuelne i druge predmete pornografske sadržine, a na istima se nalazi dijete. Dakle, predmet izvršenja ovog krivičnog djela jeste dijete.

Nadalje, ovim članom je predviđeno da se neće kazniti lice koje posjeduje takve predmete ako je stariji maloljetnik prikazan na njima dao svoj pristanak na to, ili ako to lice drži te predmete isključivo za sopstvenu upotrebu.

Kao što je već pomenuto, u crnogorskom krivičnom zakonodavstvu upotrebljavaju se termini dijete i stariji maloljetnik. Evropsko pravo ne poznaje takva dva različita termina, već pod djetetom podrazumijeva svako lice mlađe od 18 godina.

Kada je vršili kodifikaciju ovog krivičnog djela u 2009.i 2010. godini mi smo ostavili mogućnost da se neće smatrati krivičnim djelom ako se nabavljanje dječije pornogarfije preko računarskog sistema za sebe i druga lica i posjedovanje te dječije pornografije smatrati krivičnim djelom ako je stariji maloljetnik prikazan na njima dao za to svoj pristanak ili je to lice isključivo držalo predmete za sopstvenu upotrebu. Međutim zadnjim izmjenama Krivičnog zakonika u 2011. godini a koji su objavljeni u Službenom listu Crne Gore broj 32/11 ovaj član je izbrisan.

9.9. Glava XXI - Krivična djela protiv intelektualne svojine

Konvencija je u svom **članu 10** predvidjela da nacionalna zakonodavstva u svojim Krivičnim zakonima predvide kažnjivost djela koja se odnose na kršenje autorskih i njima sličnih prava, i obaveze koje su preuzete iz Ko-nvencije iz Berna o zaštiti književnih i umjetničkih djela, zaštiti po ugovoru o komercijalnim aspektima prava na intelektualnu svojinu i WIPO ugovorom o autorskim pravima.

Kodifikaciju ovih krivičnih djela naš Krivični zakonik je dao u članovima 233 do 238 gdje su ubrojana krivična djela kao što su:

- povreda moralnih prava autora i interpretatora;
- neovlašćeno iskorišćavanje autorskog djela ili predmeta;
- neovlašćeno zaobilaženje mjera zaštite namijenjenih sprječavanju povreda autorskog i srodnih prava;
- neovlašćeno uklanjanje ili mijenjanje elektronske informacije o autorskom i srodnom pravu;
- neovlašćeno korišćenje tuđeg patenta i neovlašćeno korišćenje tuđeg dizajna.

Pošto se radi o grupi krivičnih djela koja mogu da se izvrše i putem računara, i veoma često se na taj način vrše, i ova djela možemo podvesti, u širem pojmu, pod kompjuterskim kriminalom. Na primjer, kod krivičnog djela „neovlašćeno uklanjanje ili mijenjanje elektronske informacije o autorskom ili srodnom pravu", objekat radnje jeste takva informacija ili autorsko pravo sa kojeg je ta informacija izmijenjena ili uklonjena. Pošto je ta informacija ili to autorsko pravo dato u elektronskom obliku, onda se ona čini putem računara. Najčešće se koristi za zaštitu računarskih programa, odnosno softvera, ali može da bude korišćena i kod zaštite drugih oblika autorskih djela koji su takvog oblika da su inkorporirana u primjercima koji tehnički omogućavaju unošenje elektronske informacije. Radnja može biti u dva oblika, prvi je uklanjanje ili izmjena elektronske informacije o autoskom pravu i ta izmjena mora biti izvršena neovlašćeno, dakle, bez saglasnosti nosioca autorskog prava, a drugi oblik je kad se ta informacija koja se odnosi na autorsko pravo, na primjer, stavlja u promet, uvozi se ili izvozi, emituje ili na bilo koji drugi način se saopštava.

Na primjer, ako jedno lice u svom stanu, na svom kompjuteru odnosno računaru, umnoži određene CD ili DVD, pa preko interneta oglasi njihovu prodaju, vrši prezentaciju tih neovlašćeno umnoženih CD i DVD koji predstavljaju autorska djela, i prima putem elektronske pošte porudžbenice, a sve sa ciljem da stvori imovinsku korist za sebe. Pri tom je izvršio neovlašćeno umnožavanje ovih primjeraka autorskih djela, neovlašćeno je oglasio njihovu prodaju preko interneta, biće odgovoran za krivično djelo iz glave XXI, s tim što to može biti krivično djelo neovlašćeno korišćenje tuđeg autorskog prava, odnosno njegova distribucija i stavljanje u promet.

Ova grupa krivičnih djela je krivično sankcionisana novčanom kaznom ili zatvorom do 3 godine, s tim da ukoliko je krivičnim djelom neovlašćenog korišćenja tuđeg patenta, odnosno autorskog prava, pribavljena imovinska korist ili nanijeta šteta koja prelazi imovinski cenzus od 30.000€, biće kažnjiva zatvorom od 1 do 8 godina.

9.10. Crna Gora je 2007.godine donijela Zakon o odgovornosti pravnih lica za krivična djela, pa je svojim članom 3 predvidjela da pravna lica mogu da odgovaraju za sva krivična djela iz posebnog dijela Krivičnog zakonika, kao i za sva druga krivična djela koja su propisana posebnim zakonom uz uslov da su ispunjeni uslovi za odgovornost pravnog lica koje propisuje Zakon o odgovornosti pravnih lica u svojim članovima 5 do 8, i na taj način pretočili član 12 Konvencije.

9.11. Crna Gora je ratifikovala dodatni Protokol uz Konvenciju o računarskom kriminalu, a ovaj dodatni Protokol govori o kažnjavanju akata rasizma i ksenofobije koji su učinjeni putem računarskih sistema. Ovaj Protokol je ratifikovan 03.03.2010. godine a stupio je na snagu 01.07.2010. godine. Protokol smo implementirali u naše zakonodavstvo kroz član 370 Krivičnog zakonika koji govori o izazivanju nacionalne, rasne i vjerske mržnje.

Zakonom o izmjenama i dopunama Krivičnog zakonika iz 2010. godine unijete su značajne novine u zakonskom formulisanju ovog krivičnog djela, a koje su uslijedile zbog usaglašavanja crnogorskog zakonodavstva sa međunarodnim konvencijama, između ostalog i u ovom dijelu.

9.12. I ako ne spada u XXVIII glavu Krivičnog zakonika, krivična djela koja su opisana članovima 260, 262 i 263 a radi se o krivičnim djelima:

- falsifikovanje i zloupotreba kreditnih kartica i kartica za bezgotovinsko plaćanje,
- pravljenje, nabavljanje i davanje drugom sredstava i materijala za falsifikovanje,
- izdavanje čeka i sredstava bezgotovinskog plaćanja bez pokrića.

I za ova krivična djela možemo reći da se radi o krivičnim djelima koja su povezana sa računarskim kriminalom. Naime, po našem Krivičnom zakoniku krivično je odgovoran onaj ko napravi lažnu karticu ili ko preinači pravu platnu karticu. Ovdje se radi o krivičnom djelu gdje je objekat zaštite platna kartica, kao instrument bezgotovinskog plaćanja. U poslednje vrijeme imamo sve veći broj ovih krivičnih djela. Radnja pravljenja se sprovodi pomoću računara, odnosno kompjutera ili drugih elektronskih sredstava.

Posebna opasnost postoji kod kopiranja kartica za koje niti izdavalac, niti korisnik kartica znaju da postoje. To je tzv."skimovanje" i radi se o pravlje--nju platnih kartica "bliznakinja" koje su napravljene na osnovu podataka sa prave platne kartice, a do koje se došlo na nedzovoljen način, iako se još uvijek originalna kartica nalazi u državini njenog pravnog vlasnika i on ne zna da je izvršeno skimovanje njegove kartice.

Jedan od načina kako se dolazi do tih podataka je internet, jer, kada vršimo plaćanja preko interneta preko platnih kartica, mi dajemo podatke sa svojih platnih kartica koje neko kopira i pravi lažnu platnu karticu. Upravo kodifikacijom ovih krivičnih djela, odnosno njihovim proširenjem koja su uslijedila Zakonom o izmjenama i dopunama Krivičnog zakonika iz 2010. godine proširen je krug izvršenja ovih krivičnih djela, a kao osnov je poslužila okvirna odluka EU o borbi protiv falsifikovanja bezgotovinskog sredstva plaćanja 2001/413/JHA.

X PROCESNE ODREDBE I ISTRAŽNE MJERE KOJE SE ODNOSE NA RAČUNARSKI KRIMINAL

10.1. Drugi dio Konvencije o sajber kriminalu govori o procesnim odredbama u oblasti sajber kriminala. Naime, Konvencija preporučuje državama potpisnicama da u svojim nacionalnim zakonodavstvima usvoji sve zakonske i ostale neophodne mjere kako bi se uspostavila određena ovlašćenja i procedure za kažnjivost krivičnih djela iz oblasti sajber kriminala.

Kao što je svima nama poznato Crna Gora je donijela novi Zakonik o krivičnom postupku u skladu sa međunarodnim pravom, i sve odredbe ili potpuno uskladila ili djelimično sa određenim procesnim odredbama koje se tiču Evropske unije.

Članovi Konvencije od **14** do **21** ugrađeni su u naš Zakonik o krivičnom postupku kroz odredbe članova 76 do 83 koji se odnose na radnje dokazivanja, odredbe koje se odnose na privremeno oduzimanje predmeta i imovinske koristi (član 85), te odredbe o mjerama koje stoje na raspolaganju državnim organima za pribavljanje dokaza, pri čemu se misli na mjere tajnog nadzora koje su propisane članovima 157 do 162.

Kada je riječ o odredbama koje se odnose na dokazivanje o primjeni Konvencije, ovdje, čisto radi podsjećanja, treba istaći da u našem procesnom pravu nijesu posebno odvojeni dokazi koji se prikupljaju elektronskim putem i drugi dokazi, jer jednim procesnim zakonom nije moguće posebno donijeti odredbe za jednu vrstu dokaza i posebno za drugu vrstu dokaza. U suštini to je urađeno na način što se sve te odredbe odnose na sve vrste dokaza pa uključujući i elektronske dokaze koji se pojavljuju u sudskim postupcima.

Da bi lakše shvatili i uočili razliku između tradicionalne forenzike i tradicionalnog obezbjeđenja dokaza sa digitalnom forenzikom, osvrnućemo se na definiciju elektronskog dokaza i samo ukratko podsjetiti što digitalna forenzika mora da da kao odgovor koji dokazi treba da se pojave pred sudom. Tradicionalna forenzička nauka poznaje analizu otiska prstiju, DNK profil, forenzičku etnomologiju i patologiju, balističko vještačenje, vještačenje krvi, što je bilo raspoloživo dosadašnjoj praksi.

10.2. Definicija elektronskog dokaza

Elektronski dokaz je svaki elektronski zapis koji je nastao na računaru ili njemu sličnom uređaju, a napravljen je od strane čovjeka ili je automatski generisan i kao takav može služiti u dokaznom postupku pred sudom ili nekim državnim organu koji odlučuje o tom pitanju. Definišući ovako elektronski dokaz, on ima snagu javne isprave i kao takav ravnopravno se pojavljuje u sudskim spisima.

Svjedoci smo da kada su u pitanju dokazi svakodnevno se susrijećemo sa problemom dokazivanja. Pošto naš ZKP-a propisuje jasnu i strogu formalnu proceduru prilikom obezbjeđenja ovih dokaza, organi koji obezbjeđuju te dokaze moraju strogo poštovati odredbe ZKP-a. U prvom redu to je tužilaštvo i policija. Shodno novom ZKP-u, Državno tužilaštvo je organ istrage, a poznato nam je da se u istrazi obezbjeđuju dokazi, ili u prethodnom postupku tzv. izviđaju, i da, ukoliko u izviđaju ili kasnije u fazi istrage, nije određeni dokaz na zakonit način pribavljen, izvršeno njegovo obilježavanje, izopštavanje, imaćemo na sudu problem.

10.3. Elektronski dokaz se mora obilježiti. To znači da se dokaz obilježava od strane osobe koja sa njim prva dolazi u kontakt. Prvo što treba da uradi ta osoba je da unese sopstvene inicijale ili svoje čitavo ime i prezime na tom predmetu. Ovo je važno kako bi se znalo ko je taj dokaz obilježio, u kom vremenskom intervalu i kojeg datuma, što daje identifikaciju tom dokazu. Obilježavanje dokaza može se sprovesti na dva načina. Jedan je fizičko obilježavanje dokaza. To podrazumijeva fizičko markiranje na samom objektu, na samom kompjuteru, ili fizičko markiranje na papiru koji se vezuje za taj objekat. Složićemo se da je prvi način fizičkog obilježavanja mnogo bolji i sigurniji, ali to uvijek nije moguće uraditi pa će se pribjegnuti drugom načinu. Elektronski dokaz je specifičan dokaz i kao takav on mora biti jasno obilježen, pogotovo u situaciji kad imamo veći broj elektronskih dokaza. Za svaki od tih dokaza unose se tačno određeni serijski brojevi, a potom se pravi popis u vidu dnevnika ili tabele koja će sadržavati te dokaze. Ovo je sve neophodno iz razloga što ti dokazi kasnije idu na forenziku tzv. kompjutersku forenziku, i služiće kao dokaz za sud.

Odbrana tokom postupka najviše se fokusira na obaranje dokaza. Odredba člana ZKP-a koja govori o pravno nevaljanim dokazima jeste najčešće upotrebljavana odredba, što je pokazala praksa. Elektronski dokaz, kao nova vrsta dokaza, podrazumijeva najšire polje pa osobe koje rade na obezbjeđenju tih dokaza ne smiju da pogriješe, moraju biti stručno osposobljene, kako u tehničkom smislu, tako i u pravnom, kako bi na zakonit način obezbijedile dokaze.

Veoma važna uloga u fazi istrage i izviđaja koja mora biti prepoznata od strane tužilaštva, kao nosioca ovog dijela posla, jeste da izvrši dokume-

ntovanje nadležnosti. Kada se govori o dokumentovanju nadležnosti onda se misli na kontinuitet dokaznog materijala, a to je u suštini legalno pravo jedne osobe da u određenom momentu posjeduje, rukuje iil transportuje dokazni materijal, što znači da je neophodno da u tom procesu, koga moramo nazvati pravnim procesom jer od tada to i postaje, mora biti zabilježeno sve što se dešava, od početka do kraja.

Ukoliko se samo u jednom dijelu pojavi možemo slobodno reći "rupa" u npr. dnevniku dokaznog materijala, isto će biti okarakterisano kao moguća zloupotreba na pribavljeni dokaz, ili da je dokaz namješten ili da je dokaz izmijenjen. Opšti pojam dokaza, pa onda to možemo prevesti i na elektronski dokaz, jeste da je to materijal koji je prikupljen na licu mjesta i on predstavlja iskaz osobe koja je prikupila dokaz kojim ta osoba potvrđuje da je identičan objekat u datom trenutku prisutan u sudskim spisima, odnosno u sudnici gdje se sudi, da sa tim dokazom nije manipulisano, već da on predstavlja vjernost onoga što se na licu mjesta obezbijedilo.

Kada se govori o dokazima prema ZKP-u, uopšteno se govori o dokazima, Zakon ih ne dijeli, pa samim tim se tu i ubrajaju elektronski dokazi. Međutim, specifičnost prikupljanja i obezbjeđivanja elektronskih dokaza u odnosu na sve ostale je velika. Ovo se prije svega ogleda u fazi izviđaja.

Kada se desio zločin ili krivično djelo inspektor na terenu, koji dođe na mjesto zločina ne zna na koju vrstu dokaza će naići, pa tako se dešava da naiđe ne samo na dokaze koji su uobičajeni, nailazi se i na dokaze koje možemo podvesti pod elektronske dokaze, te forenzički inspektor prvenstveno vrši fotografisanje zatečenog stanja na licu mjesta o čemu sačinjava svoj pisani izvještaj u koji unosi sve činjenice koje su relevantne informacije za dalju istragu. Ovo su stvari koje su tužiocima i istražnim sudijama dobro poznate, jer ih na taj način sprovode kada vrše izviđaj. Kada naiđemo na elektronske uređaje potrebno je da dokumentujemo sve mrežne i bežične pristupne tačke koje služe da se kompjuteri povežu na internet ili da se međusobno umreže.

Ono što je važno kada se dođe na lice mjesta i što forenzičar, odnosno, tužilac koji rukovodi izviđajem treba da odradi jeste da računar ostavi u stanju u kakvom ga je zatekao. To znači da ako je računar bio upaljen on ne smije da ga izgasi, jer ako bi došlo do isključivanja takvog računara, a on je umrežen u određenu mrežu, može da dođe do promjene datoteke koja se nalazi u njegovoj radnoj memoriji. Tom svojom radnjom ukoliko nije obučen, lice koje vrši uviđaj može da proizvede više štete nego što on misli da je time što je isključio računar obezbijedio ga.

10.4. Da bi smo to odradili potrebno je da preuzmemo niz koraka koji su preduslov toj radnji koju vršimo isključivo na osnovu naredbe suda, a to je da izvršimo prvo fotografisanje monitora, da izvršimo pravljenje imidža,

odnosno, kopije diska prije oduzimanja predmeta, da izvršimo provjeru integriteta te kopije, da isključenje kompjutera sa elektro mreže izvršimo prema pravilima operativnog sistema, da izvršimo fotografisanje svih ostalih priključnih aparata i uređaja koji su bili eventualno povezani na taj kompjuter, da izvršimo podjelu, odnosno razvezivanje svih kablove koji su u kompjuteru i njihovo markiranje, a sve to je neophodno da forenzičar uradi sa rukavicama kako bi se izbjegla potencijalna šteta usljed statičkog elektriciteta. Kada smo obezbijedili te elektronske dokaze, a radi se o uređajima ili drugim digitalnim dokazima, potrebno je da ih smjestimo u antistatičke kesice jer jedino na taj način možemo izvršiti pravilno obezbjeđenje dokaza.

Pri tom je veoma važno, ako je naravno to moguće uraditi, da uključimo korisnika kompjutera da nam omogući prikupljanje i analizu tih dokaza tako što će nam on saopštiti određene infromacije, a te informacije su: koji korisnički nalog koristi, koji mu je nalog za elektronsku poštu, sve moguće šifre koje postoje za pristup određenim diskovima iil datotekama. Ako sve to nije moguće da obezbijedimo onda idemo u pravljenje kopiranja i imidža, odnosno pretraživanje podataka, za šta nam je neophodno dobiti sudski nalog.

Kako to izgleda na primjeru, odnosno koja je razlika između analognog i digitalnog dokaza pokazaćemo kroz par slajdova:

Slika 3. Obezbjeđenje lica mjesta

Slika 4. Obezbjedjenje digitalnog dokaza

Slika 5. Obezbjeđenje analognih dokaza

Kada govorimo o računarskom kriminalu i elektronskom dokazu, stručnjaci ga poznaju kao "KLON" ili "IMIDŽ". To znači da je neophodno klonirati, napraviti potpunu repliku, odnosno postići potpunu istovjetnost originala i klona. To se postiže uz pomoć hardver write-blokera npr. bloker kompanije "Tableau" pomoću koga se vrši blokada kompjutera i pravljenje "imidža" kao dokaznog sredstva.

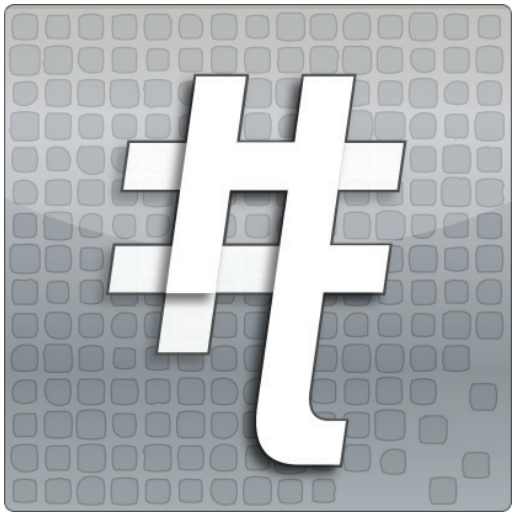
Slika 6. Bloker, kompanije "Tableau", pomoću koga se vrši blokada kompjutera i pravljenje "imidža" kao dokaznog sredstva.

Slika 7. Otisak analognog dokaza

6E 6B 73 63 61 70 65 2E 6F 72 67 9B
41 54 68 81 ED 99 7B 8C 5D 45 1D C7
D2 2E 65 03 42 2B 41 9A 06 81 C4 34
40 FB 40 11 56 41 B4 89 FC A5 18 21
52 10 03 12 21 06 4D 8C E2 16 5A 1B
BA DD DD 6E F7 EE 7D 9D D7 F8 C7 BD
A4 BF 64 32 E7 CE F9 9D 73 BE 9F F9
6C 6A A6 05 7C 50 3B 09 30 D3 76 12
C0 9C 88 73 77 57 DE 01 56 6A C7 BB
88 48 FD 37 28 01 B1 A0 44 10 AC 15
6B 95 20 AF D8 58 7E BC EA 81 C3 2F
9F 2D CA 7C 57 29 BD AE 73 E1 F9 6D
16 11 85 52 0E 28 83 68 0F A5 0D 4A
A0 B4 0B CA 41 19 07 11 4D 14 5B 2A
F6 44 51 7C 57 7A A8 F8 C4 CA 27 AC
F5 71 14 AE 3D ED 9C 65 F1 C2 0B AF
C0 07 6B B1 B6 D6 DD 4A 2C 5A 2B B4
EB 6D 52 2F 0A 94 92 DA B1 06 7F CE
D5 7B B0 54 28 94 82 58 AC FC FA 1B
19 37 BD A9 6D DE 82 6B 96 7E E5 CE
FC E7 75 4A 85 61 49 FA A9 BA 28 1B
01 31 28 2F 4B 1C 96 10 25 88 05 B1
82 65 36 7B D6 0A 7B 5E 7E 6B BE 50
CC 5D 0D 37 BD AF 08 3C 7A F3 9C 7B
8E 97 61 78 FF BF 29 F5 BF C5 F6 3F
1D 9F B8 8C CE 45 CB 41 A7 E9 DB B3
AC A5 B4 2F BC 84 96 F9 8B 19 1D 7A
7F D6 A2 A3 04 25 10 A5 E6 31 FF D2
10 B3 6B DF F0 A8 1F C5 F7 AC BA EF

Slika 8. Otisak digitalnog dokaza.

Kada je u pitanju analogni dokaz-otisak prsta, znamo da 1/64 biliona slučajeva se računa, a kada je u pitanju otisak digitalnog dokaza, koristeći "MD5" algoritma, može da se uporedi sa 1/340 biliona slučajeva. To je ono za što će nam odgovor dati digitalna forenzika, u zavisnosti od svakog pojedinačnog slučaja.



10.5. Sa procesnog aspekta važno je da je obezbjeđenje dokaza urađeno na zakonit način, pa sve te odredbe koje propisuju obezbjeđenje naredbe suda za pretrese, kako stanova, tako i poslovnih prostorija, računara, su sve preduslovi koje je neophodno potpuno ispoštovati kako bi se tek onda pristupilo obezbjeđenju elektronskog dokaza. Sve ovo govori nam o tome koliko je očigledno da je za očuvanje integriteta dokaznog materijala značajan i broj ljudi koji učestvuje u tome, kao i da je veoma važno da se radi o kontinuitetu npr. jedne osobe koja svugdje prati dokazni materijal. Mi imamo osobu koja prati dokazni material kada su u pitanju, nazovimo ih, obični dokazi i to nije problem obezbijediti, ali kada su u pitanju elektronski dokaz, i pa imamo obezbjeđenje njihovo, njihovo procesuiranje, njihovo analiziranje, nemoguće je odrediti prisustvo jedne osobe u forenzičkoj analizi.

Po stanovištu suda, u tom slučaju je neophodno da se kreira potvrda iz laboratorije radi ispitivanja, u momentu prijema, dokaznog materijala i u momentu isporuke rezultata, čime se obezbjeđuje integritet dokaza.

Kada su u pitanju krivična djela iz oblasti računarskog kriminala, postaviće se pitanje neophodnog svjedočenja forenzičara ili laboranta na sudu, koji će morati da svjedoče o tome na koji način su obezbijedili dokaz, kako je dokazni materijal skladišten i zaštićen u kompjuterskoj laboratoriji u kojoj je izvršena njihova analiza, odnosno forenzika.

Ako sve ovo nije odrađeno na propisan način, to znači da nije dobro sprovedena istraga, odnosno izviđaj, a ako se nešto proglasi za pravno nevaljan dokaz, shodno članu 84 ZKP, završava se postupak oslobađajućom presudom.

10.6. Prateći odredbe Konvencije i njeno implementiranje kroz odredbe ZKP-a, dolazimo do pojma vještačenja. Na sudu će se pojaviti vještaci informatičke struke, tako da sudije i tužioci moraju biti tehnički obrazovani da bi, prvenstveno, razumjeli elektronski dokaz i bili spremni da razumiju informatičko vještačenje i iz tog vještačenja izvuku one činjenice koje su neophodne za donošenje pravne odluke.

Praksa je pokazala da problem koji se javlja jeste upravo to što po Zakoniku ne postoji definicija elektronskog dokaza, kao informacije podatka koji je nastao na računaru ili je smješten u računar, ili je prenijet preko računara, ali širim tumačenjem ZKP-a on ima istu vrijednost kao i svi drugi materijalni dokazi. Međutim, upravo zbog mogućnosti da se taj dokaz može veoma lako izmijeniti, uništiti, modifikovati, ili na drugi način promijeniti svoj prvobitni oblik, on zahtijeva zaista posebnu pažnju i adekvatan pristup u postupku njegovog pribavljanja i obezbjeđivanja.

10.7. Način pribavljanja listinga telefonskog broja od strane provajdera

Prema Zakonu provajderi su obavezni da čuvaju svoje elektronske podatke -listinge na period do 6 mjeseci. U Crnoj Gori vrijeme čuvanja listinga je različito od provajdera do provajdera, tako da su policija, tužilaštvo i sudstvo, kao organi koji koriste te podatke kao dokaze, veoma ograničeni, a ovo zato što je taj period od 6 mjeseci veoma kratak. Veoma često se ne otkriju krivična djela u trenutku kad su ona izvršena, već po proteku izvjesnog vremenskog perioda, pa ako je taj period unazad dvije-tri godine, neće se moći dobiti takav dokaz od strane provajdera.

Odredbama koje se odnose na mjere tajnog nadzora, a koje su predviđene članom 157, moguće je takve mjere preduzeti prema licu koje prilikom izvršenja krivičnih djela koristi sredstva za elektronsku komunikaciju, ili poruke o počiniocima izvršenja krivičnih djela, ili o samom krivičnom djelu prenosi putem telefona ili elektronskim putem. Dakle, i u ovim odredbama je ostavljena mogućnost da se inkorporiraju odredbe Konvencije o sajber kriminalu.

Računarski kriminal nije kriminal koji se zadržava u nacionalnim okvirima, već možemo reći da ima elemente međunarodnog karaktera, pa se onda postavlja pitanje međunarodne saradnje u pogledu ovih krivičnih djela, koju i sama Konvencija predviđa, tako da odredbe od člana 24 do 28 Konvencije inkorporirane su u nacionalni Zakon o pružanju međunarodne pravne pomoći u krivičnim stvarima.

Kada je Crna Gora predala instrumente za potvrđivanje Konvencije, ona je dala izjavu da je Ministarstvo pravde CG organ koji je nadležan za slanje zahtjeva za uzajamnu pomoć, za odgovaranje na te zahtjeve i za izvršavanje tih zahtjeva.

Pravosudni organi postupaju po Zakonu o međunarodnoj pravnoj pomoći u krivičnim stvarima, pa i kada se radi o krivičnim djelima iz oblasti sajber kriminala, na isti način kao što to čine i za drugu vrstu krivičnih djela.

Predočavajući materijalno i procesno nacionalno zakonodavstvo u Crnoj Gori može se reći da računarski kriminal ili visoko tehnološki kriminal je nov pojavni oblik kriminaliteta, da je država preduzela značajne i odlučne korake u tom pravcu prvenstveno usvajanjem određenih materijalnih i procesnih zakona, koji predstavljaju dobar osnov za krivično gonjenje počinilaca ovih krivičnih djela. Pošto je Crna Gora u procesu reforme pravosuđa koja podrazumijeva i reformu krivičnog zakonodavstva, neophodno je izvršiti analizu određenih primjedbi, preporuka stručnih lica koja se bave ovim poslovima, a sve u cilju donošenja što boljih zakonskih normi koje bi ostvarile rezultate u borbi protiv visokotehnološkog kriminala.

XI GLAVNI PRETRES

Jedan od ciljeva ovog Priručnika je da pomogne u svakodnevnom radu sudijama koji postupaju u postupcima za krivična djela iz oblasti računarskog kriminala, i to ne samo u tim, već i u svakom drugom postupku gdje se u dokaznom postupku predlažu i izvode elektronski dokazi.

Dalje, cilj Priručnika je da tužioci i sudije upoznaju dovoljno ovu problematiku, da umiju da prepoznaju šta je bitno, a šta ne, da znaju da postave prava pitanja učesnicima u svim fazama postupka, a naročito sudskim vještacima, da bi dobili odgovore koji će kasnije biti od važnosti za donošenje odluke. Ne može se i ne mora očekivati da svi razumiju do tančina ovu problematiku. Pri tome, ne smije se zaboraviti na procesnu ulogu tužilaca i sudija u krivičnom postupku, a posebno da tužioci i sudije i dalje ostaju da budu pravnici, a vještaci stručna lica, čiji nalazi i mišljenja ponekad mogu biti odlučujući za formiranje pravilne i na zakonu zasnovane odluke u krivičnopravnim stvarima koje se tiču ove oblasti.

Postizanju navedenog cilja ne treba da bude ograničavajući faktor činjenici da, kako za početnom, tako i za stalnom obukom u ovoj oblasti. Postoji ozbiljno interesovanje kod jednih, ali i potpuna nezainteresovanost, pa i nelagodnost, kod drugih, naročito onih koji ne koriste svakodnevno računar.

Nema razloga za sumnju da će se i na dalje nastaviti sa dobrom praksom organizovanja obuke, koju je i do sada na veoma kvalitetan način sprovodio Centar za edukaciju nosilaca pravosudne funkcije širom Crne Gore. U tom smislu, ovaj Priručnik treba shvatiti kao početni korak u dostizanju potrebnog nivoa znanja za uspješnu borbu protiv računarskog kriminala, uz istovremeno očuvanje i poštovanje osnovnih principa krivičnog postupka i krivičnog prava.

U dijelu Priručnika koji se bavi nacionalnim zakonodavnim okvirom, predstavljena su pojedinačno krivična djela, njihova zakonska obilježja, predmet izvršenja, objekat krivičnog djela i posljedica. Stoga će se u ovom dijelu dati prikaz pojedinih primjera iz prakse, (pretežno iz Republike Srbije, obzirom da je tamošnja sudska praksa za sada najobimnija) i eventualne teškoće sa kojima se susretala u rješavanju tih problema, kako tokom prvostepenog postupka, na glavnim pretresima, tako i pred drugostepenim sudom, sa naročitim osvrtom na izvedene specifične dokaze koji su neizbježni u ovim postupcima.

Obzirom da ćemo se, po svemu sudeći, sasvim moguće u budućim postupcima i dalje susretati sa istim situacijama, cilj prezentiranja pravnosnažno okončanih postupaka je da se postigne veća ekonomičnost i efikasnost u rješavanju predmeta.

Prilikom objašnjavanja će se koristiti naziv krivičnog djela iz Krivičnog zakonika koji je na snazi u Republici Srbiji, a u zagradama će se numerički navoditi odgovarajući član Krivičnog zakonika koji je na snazi u Crnoj Gori. Pri tome treba imati u vidu da se zakonski naziv i/ili opis djela u nekim slučajevima razlikuju, što će biti obilježeno znakom *, kako bi se na to skrenula pažnja i uticalo da se čitalac vrati na dio Priručnika koji se bavi nacionalnim zakonodavstvom.

11.1. Oštećenje računarskih podataka i programa (čl.349 KZ)

Primjer za krivično djelo oštećenje računarskih podataka i programa predstavlja postupak protiv okrivljenog koji je oglašen krivim da je neovlašćeno izmijenio računarske podatke na određenom sajtu, vlasništvu jedne agencije, na taj način što je iskoristivši propust u izradi sajta, neautorizovano preuzeo administratorska prava na tom sajtu i izmijenio podrazumijevanu adresu, tako što je postavio svoju adresu na Gmailu, a potom je od prodavca domena zahtijevao i dobio autorizacioni kod, nakon čega je izvršio preregistraciju domena kod drugog provajdera, čime je dobio apsolutnu kontrolu nad njim i učinio ga neupotrebljivim za stvarnog vlasnika domena.

Kod krivičnog djela oštećenje računarskih podataka i programa, radnja izvršenja krivičnog djela je alternativno određena. Brisanje ili izmjena podrazumijevaju potpuno uništenje računarskog programa ili podatka ili njihovo mijenjanje, ali tako da podaci postanu potpuno neupotrebljivi ili neupotrebljivi za funkciju za koju su bili namijenjeni. Oštećenjem se smanjuje upotrebna vrijednost računarskog podatka ili programa i može biti djelimično ili potpuno. Uništenjem je stvar dovedena u takvo stanje da je izgubila vrijednost i postala potpuno neupotrebljiva.

Prikrivanje podrazumijeva sklanjanje sa mjesta gde se do tada nalazio u računaru računarskog programa ili podatka i na taj način činjenje neupotrebljivim sa aspekta njegove namjene, primarnog cilja i primarnog korisnika kome je program služio.

11.2. Računarska prevara (čl.352 KZ)

U pogledu krivičnog djela računarske prevare u praksi nema previše predmeta. Kao jedan primjer je predmet u kojem je okrivljeni lažnim prikaziva-

njem podataka uticao na rezultat elektronske obrade i prenosa podataka u namjeri da sebi pribavi protivpravnu imovinsku korist i time prouzrokovao štetu preduzeću Telekom, na taj način što je u više navrata neovlašćeno pristupao ormarićima navedenog preduzeća sa telefonskim instalacijama u određenim zgradama, vršio je neovlašćenu konekciju na telefonske priključke fiksnih brojeva, čiji su korisnici bili druga lica, sa tih brojeva je pozivao telefonski servis za dopune mobilnih telefona, na kome je računar automatski registrovao fiksni broj, identifikovao je i korisnika a zatim je okrivljeni putem tastature mobilnog telefona unosio prethodno pribavljene korisničke šifre, čime se računarskom programu za obradu podataka lažno predstavio kao zakoniti korisnik usluga i na taj način dopunjavao stanje kredita na računu mobilnog telefona u različitim iznosima. Raspon dopune je sa otprilike od 30 eura pa sve do 760 eura na račun jednog korisnika. Za navedeno krivično djelo prvostepenom presudom, osuđen je na kaznu zatvora u trajanju od 2 godine. Navedena presuda je iz 2010. godine, kada se rigoroznije odlučivalo u pogledu kazni u ovakvim predmetima. Navedeno lice je bilo u pritvoru koji mu je produžen do pravnosnažnosti presude, a razlog tome se može tražiti i u tome što se radilo o produženom krivičnom djelu sa 25 pojedinačnih radnji.

11.3. Neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (čl.353 KZ)*

Za krivično djelo neovlašćen pristup računarskom sistemu, ovdje će se navesti primjer okrivljene kojoj je izrečena sudska opomena što se u više navrata neovlašćeno uključila u računarsku mrežu jedne firme na taj način što se sa svog kućnog računara konektovala na internet i pristupajući sa IP adrese bila je dodijeljenja korisniku-njenom suprugu, pristupila internet adresi firme nakon čega je prekršila mjere zaštite uspostavljene od strane firme, unijela korisnička imena i lozinke za dvoje zaposlenih u toj firmi i sa svog računara neovlašćeno pregledala sadržaje njihove elektronske pošte.

Drugi primjer, ali za kvalifikovan oblik, je predmet u kojem je okrivljeni sa svog računara unošenjem prethodno pribavljenih šifri u polje za unos korisničkog imena i lozinke neovlašćeno pristupio serveru za pružanje usluge obrade elektronskih podataka, izbrisao postojeće podatke, unio podatke po svojoj volji, usljed čega je došlo do zastoja i navedeni veb sajt je u vrijeme trajanja napada bio nedostupan, nakon čega je zbog masovnih napada NN lica navedena internet prezentacija uklonjena.

Prvostepena presuda je ukinuta rješenjem drugostepenog suda, obzirom da su ocijenjeni osnovanim žalbeni navodi branioca da se masovni napadi od strane velikog broja lica ne mogu pripisati krivici okrivljenog, a činjenica

o masovnim napadima je bila unijeta u izreku presude, kao radnja izvrše--nja okrivljenog. Drugostepeni sud je skrenuo pažnju da u konkretnom slučaju okrivljeni može da odgovara jedino za svoje radnje i svoje postupke. Osim navedenog, drugostepeni sud je našao da prvstepena presuda nema razloga o odlučnim činjenicama. Naime, prvostepeni sud ne navodi razloge zbog kojih smatra da je okrivljeni izvršio kvalifikovani oblik krivičnog djela a da pri tome prethodno nije utvrdio da je samom radnjom okrivljenog zaista došlo do blokade sistema.

11.4. Ugrožavanje sigurnosti (čl.168 KZ)

Što se tiče krivičnog djela ugrožavanja sigurnosti, jedan od primjera je predmet u kome je izvršilac ugrozio sigurnost više lica – osoba koje namjeravaju da učestvuju na manifestaciji Parada ponosa, i to prijetnjom da će napasti na život i tijelo tih lica, tako što je na internet prezentaciji društvene grupe Facebook, u okviru jedne grupe čiji se naziv navodi, a čiji je okrivljeni član, sa svog profila uputio prijeteću poruku upućenu svim eventualnim učesnicima navedenog događaja.

Drugostepeni sud je najprije postupao tako što je prvostepene presude koje su bile oslobađajuće, potvrđivao ovakve presude, nalazeći da su pravilno prvostepeni sudovi našli da u konkretnom slučaju nije došlo do individualizacije pasivnog subjekta kod koga se kao posledica krivičnog djela ugrožavanja sigurnosti javlja upravo njegova konkretna sigurnost, koja se manifestuje u njegovom ličnom osjećaju nesigurnosti. Kako je stavljeno na teret da je okrivljeni ugrozio sigurnost više lica koja namjeravaju da učetsvuju u navedenoj manefestaciji dakle u vrijeme kada se nije ni znalo da li će se održati manifestacija, te da je njegova prijetnja bila upućena svim eventualnim učesnicima, pri čemu je bilo nemoguće individualizovati pasivni subjekat, drugostepeni sud je tada smatrao da je pravilno prvostepeni sud našao da radnje koje su okrivljenom stavljene na teret ne predstavljaju krivično djelo.

Međutim, nakon zauzimanja stava Vrhovnog kasacionog suda Srbije, došlo je do izmjene prakse, u postupcima su saslušavani svjedoci koji su izjavili da su pročitali poruku na Facebook-u koju je okrivljeni ostavio, da su o toj poruci obavijestili administratora Facebook-a, da su organizatori manifestacije to prijavljivali policiji, da su se svjedoci osjetili ugroženim, da su i sami bili učesnici na toj manifestaciji, da su osjetili strah za ličnu bezbjednost i da su takve navode shvatili kao direktan poziv na nasilje.

Prenosimo u integralnoj verziji Pravno shvatanje VKS Srbije:

„O potrebnim elementima za optužni predlog kod krivičnog dela ugrožavanje sigurnosti iz člana 138 stav 2 u vezi stava 1 KZ

Za postojanje krivičnog djela iz člana 138. stav 2. KZ, potrebno je da se zna na koja lica se odnosi pretnja i čija je lična sigurnost ugrožena, ali to ne znači da identitet tih lica mora biti tačno određen u optužnom aktu, već je dovoljno da je ta lica moguće odrediti – identifikovati prema nekoj okolnosti koja stoji u vezi sa upućenom pretnjom.

Kod krivičnog djela ugrožavanje sigurnosti iz člana 138. st.2. u vezi st.1. KZ, često se pojavljuje dilema da li je uopšte neophodno precizno imenom i prezimenom označiti pasivnog subjekta – oštećenog ili je za optužni predlog dovoljno da je on odrediv, tj. da se iz dispozitiva zna na koja lica se odnosi prijetnja kojom se prijeti zlom, a što ima za posljedicu stvaranje nespokojstva, straha i narušavanja pravne i fizičke nesigurnosti, tj. lične slobode.

Kad je pretnja upućena direktno, neposredno, onda nema dileme na koga se odnosi. Međutim, kada je prijetnja upućena većem broju neidentifikovanih lica, preko internet prezentacije društvene mreže „Facebook" ili kakvog drugog preciznog sredstva elektronske komunikacije koje je dostupno svima jer je pristup toj mreži neograničen, onda je za optužni akt dovoljno da su pasivni subjekti odredivi, a koja su njihova imena i prezimena i da li su za pretnju saznali je stvar dokazivanja u krivičnom postupku". http://www.vk.sud.rs/pravno-shvatanje-o-potrebnim-elementima-za-optuzni-predlog-kod-krivicnog-dela-ugrozavanje-sigurnosti-iz-clana-138.-stav-2. -u-vezi-stava-1.-kz.html

U praksi sudova u regionu prisutna su navedena krivična djela koja su izvršena na taj način što je ugrožena sigurnost najviših državnih funkcionera ili su prijetnje upućivane određenim licima u pojedinim državnim institucijama.

Izvjesno je da se veliki broj krivičnih djela ugrožavanje sigurnosti vrši preko Facebooka društvene mreže, pa tako navodimo i primjer gdje je izvršilac krivičnog djela sa svog korisničkog profila na korisnički profil oštećenog poslao prijeteće poruke "mrtav si, odrobijaću te", a potom i na svom korisničkom profilu postavio sliku na kojoj se nalazio oštećeni sa zaokruženom glavom na kojoj je sastavljen tekst "poslednji pozdrav" i navedeno ime oštećenog, zatim primjer gde je okrivljeni oglašen krivim (presuda je potvrđena od strane drugostepenog suda) da je okrivljena sa svog kućnog računara ugrozila sigurnost više lica, sa korisničkog profila Facebooka, koji je kreirala pod imenom koji ne odgovara njenom imenu i prezimenu uputila na korisnički profil maloljetne oštećene. Prijetnje koje se odnose na maloljetnu oštećenu i njenu majku, gde poruke obiluju psovkama ali i prijetnjama da će napasti na njihov život i tijelo , što je ovdje bilo bitno. U dokaznom postupku između ostalih izvedenih dokaza, pročitane su odštampane poruke sa Facebooka.

Dodatni Protokol uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju djela rasističkih ksenofobične prirode izvršenih preko računarskih sistema ima za cilj da se inkriminišu i kazne navedena

ponašanja bez obzira da li se njime širi mržnja ili se činjenice predstavljaju na neistinit način.

11.5. Pravljanje i unošenje računarskih virusa (čl.351 KZ) i prevara (čl.244 KZ)

Što se tiče krivičnog djela pravljanje i unošenje računarskih virusa u postupku koji je vođen pred Višim sudom u Beogradu, a zatim i pred Apelacionim sudom u Beogradu, potvrđena je prvostepena presuda u kojoj je osim navedenog krivičnog djela okrivljeni oglašen krivim za krivično djelo pravljenje i unošenje računarskih virusa i za krivično djelo prevara u pokušaju.

U izreci koja je zaista opširna, ne i neopravdano, (kojoj ćemo ovdje dati dosta prostora kako bi se čitaoci upoznali do detalja) navedeno je da je okrivljeni na svom personalnom računaru, pomoću programske aplikacije Visual basic napravio računarski virus IC Trojanac, a u namjeri njegovog unošenja u tuđe računare, koji je imao funkcije slikanja aktivnog monitora zaraženih računara drugih korisnika, tzv. Screenlogger, snimanje kucanja karaktera na tastaturi Keylogger, postavljanje sadržaja na zaražene računare drugih korisnika, kao i skidanje sadržaja sa tih računara (*funkcije upload i download*), oformio dvije sobe za razgovor *(chat rooms)* koje je koristio kao mjesto i sredstvo za zadavanje komandi i vršenje kontrole nad zaraženim računarima i prijem odgovora, navedeni virus unio u računare 70 korisnika, prouzrokovao štetu po zaražene računare i njihove korisnike, na taj način što je nezavisno od volje korisnika vršio snimanje sadržaja aktivnog monitora, snimanje elektronskih sadržaja koje korisnik unosi putem tastature koji podaci su potom bez znanja i pristanka korisnika zaraženih računara slati na server koji je bio pod kontrolom okrivljenog, i to sve tako što je predstavljajući se različitim imenima sa različitih adresa na elektronske adrese korisnika slao elektronsku poštu u kojoj se kao prilog (attachment) poruke nalazio računarski virus, dok je u poruci navodio da treba da pogledaju šta se u prilogu nalazi, a po otvaranju priloga pokretala se instalacija virusa na računar, virus se kopirao u programski registar, pravio je sistemski zapis, što je dalje omogućavalo da se virus aktivira svakim podizanjem operativnog sistema.

Sličan primjer predstavlja radnja izvršenja okrivljenog koji je napravio i unio virus u tuđe računare, a zatim virusu slao i zadavao komande preko tekstualnih poruka i na taj način prikupljao lične, poslovne i druge podatke korisnika zaraženih računara, pa je tako unio virus u računare tri njemačka državljanina, prikupljao podatke o njihovim bankovnim računima i to za online transakcije a zatim u namjeri da pribavi sebi protivpravnu imovinsku korist i lažnim prikazivanjem činjenica doveo u zabludu jednog od njemačkih državljanina i službenike njemačke banke, kako bi ih naveo da na štetu

imovine klijenata isplati iznos od 2. 600 eura.

Na navedeni način, okrivljeni je prikupio podatke u vezi ovog državljanina koje se tiču ne samo imena i prezimena već i broja fiksnog telefona, broja mobilnog telefona, broja bankovnog računa korisničko ime, ali i ono što je bitno PIN broj *(personal identification number- numerička lozinka koja služi sistemu za identifikaciju korisnika),* zatim je saznao i njegov TAN broj *(transaction authentication number- jednokratna numerička lozinka)* koji se koristi za potvrdu online transakcije.

Osim toga okrivljeni je doveo u zabludu istog državljanina lažnim prikazivanjem činjenica da je od svoje banke dobio poklon u iznosu od 1300 eura, i tako što je u Frontpage- u u HTML jeziku, izradio lažnu internet stranicu banke na kojoj je na njemačkom jeziku naveo tekst kojim se potvrđuje da navedeni državljanin njemačke dobio kao poklon od banke za uspješno poslovanje iznos od 1300 eura i to trgovanje/ poslovanje sa trgovinom hartija od vrijednosti.

Tako pripremljenu stranicu je postavio na hard disk njegovog računara i sačekavši da se uloguje kako bi provjerio stanje svog računa aktivirao je Keylogger kako bi nadgledao koje podatke unosi sa tastature, snimio je broj za online transakcije, doveo u zabludu kako službenike banke da na štetu imovine klijenta, a u korist faktički okrivljenog, na račun otvoren u banci u Srbiji na ime majke okrivljenog, putem online transakcije uplate iznos sa lažnom svrhu pomoć prijatelju, koju transakciju je banka konačno stopirala obzirom da je provjerom posumnjala da se radi o rizičnoj transakciji.

Okrivljeni je u svojim odbranama, što je jako bitno navesti, do detalja iznosio odbranu, što je za prvostepeni i drugostepeni sud bilo od značaja da lakše sagleda način izvršenja navedenih krivičnih djela sa kojima se do sada nije susretalo puno sudija.

U toku dokaznog postupka pročitan je dopis CERT *(computer emergency response team-nacionalni tim za monitoring i brzu reakciju na prijetnje)* zemlje oštećenog državljanina dostavljen domaćoj banci, iz kog je utvrđeno koji je tip virusa u pitanju, da se radi o Trojancu, kakve funkcije on ima, kakve su funkcije postavljanja sadržaja na zaraženi računar, kako su zadavane komande, odakle i kako je vršena kontrola, te prijem i odgovor od strane zaraženih računara. U dokazom postupku izvršen je pregled hard disk računara, uz pomoć forenzičkog softverskog alata, izvršena je aktivizacija podataka korišćenjem Forensic toolkit, pregledom sadržaja utvrđeno da je računar korišćen za pristup internetu i u druge svrhe, da su pronađene izvjesne datoteke koje su dostavljene sudu u prilogu i one su obično na CD-R mediju.

Pred sudom je vršen uvid u sadržaj dostavljenih diskova i tada je utvrđeno da se na sadržajima snimljenim sa hard diska laptopa oduzetog od okrivljenog, između ostalog, nalaze, i vidljivi su, snimci aktivnih ekrana računa-

ra oštećenog stranog državljanina, na kojima se vidi stanje na računu itd.

Prvostepeni sud je našao da posljedica krivičnog djela unošenje računarskih virusa jeste nastupanje štete ali za razliku od tumačenja okrivljenog i branioca tokom postupka, sud nalazi da se šteta može manifestovati u bilo kom obliku, dakle ne nužno, da je došlo do imovinske štete, već je dovoljno da je unošenje virusa imalo posljedice koje se mogu ogledati i "samo u usporavanju rada računara, u padanju sistema ili njegovom ponovnom podizanju ili pokretanju na svakih nekoliko minuta, usporavanje internet konekcije i slično" pri čemu se šteta može posmatrati i kao neimovinska, obzirom da je povređeno pravo na privatnost i zaštita povjerljivih podataka korisnika tako zaraženih i kompromitovanih računara.

Posebno je interesantno da se u konkretnom slučaju radilo o sticaju sa krivičnim djelom prevare (u klasičnom smislu) u pokušaju. Ovo stoga što je prvostepeni sud pravilno našao da je okrivljeni kao sredstvo za izvršenje krivičnog djela prevare koristio računar, računarske programe i pristup internetu, odnosno sredstva koja po mišljenju suda jesu podobna za izvršenje predmetnog krivičnog djela.

Što se tiče dokaza potrebno je utvrditi da li je računarski virus, unijet direktnim pristupom računaru ili je to učinjeno u okviru mreže internog karaktera uz pomoć drugog računara kao dijela te mreže ili je to učinjeno putem interneta. Karakteristično je za ovo krivično djelo da izvršioci su obična lica koja nemaju samo osnovno poznavanje rada na računaru već u mnogo kvalitetnijem nivou poznaju i način rada operativnog sistema, način funkcionisanja pojedinih djelova i međusobne povezanosti i operativnog sistema, osnove programiranja, izrade računarskih programa uz pomoć nekog od postojećih i poznatih programskih jezika ili alata.

11.6. Prevara (čl.244 KZ)

Sa gore navedenim primjerom dobro je odmah navesti sljedeći primjer samostalnog krivičnog djela prevare, u pokušaju, dakle opet krivičnog djela koje nije iz posebne glave Krivičnog zakonika koje se bavi krivičnim djelima računarskog kriminala.

Naime, okrivljenom u ovom postupku je stavljeno na teret da je dovodio građane, lažnim prikazivanjem činjenica, u zabludu i navodio ih da mu na štetu svoje imovine isplate iznos u vrijednosti koja je ukupno prešla iznos od 1.500.000, 00 dinara, tako što je kod internet provajdera registrovao domen na kome je postavio internet prezentaciju pod nazivom "Apel za pomoć licu... " na kojoj se predstavio kao otac teško oboljelog osamnaestomjesečnog dječaka kome je nephodno potrebna hitna medicinska pomoć. Pomoć je podrazumijevala operaciju, presađivanja matičnih ćelija, koja je

navodno zakazana u bolnici u inostranstvu i čije izvođenje košta 145.000 eura, pri tom je postavio preko stotinu fotografija na kojima se nalazilo neidentifikovano dijete zajedno sa roditeljima za koje je okrivljeni na ovoj stranici tvrdio da se radi o slikama njegovog oboljelog sina. Na toj prezentaciji pozvao je sve koji žele da mu novčanim prilozima pomognu, uplaćaju svoje priloge na račune koje je otvorio u dvije banke, a zatim putem interneta kontaktirao sa administratorom sajta čije se ime navodi i lažno se predstavio na isti način. Zatim je spisak sajtova koji su akciju podržali, postavio na svom domenu, nakon čega su mu od strane više lica uplaćena novčana sredstva koja je on potom podigao.

U toku dokaznog postupka pročitani su izvještaji provajdera *(kompanija koje pružaju usluge pristupa Internetu fizičkim i pravnim licima)*, utvrđeno je da je okrivljeni uplatio iznos na ime registracije domena, na ime tromjesečnog hostinga, da je otvorio domen, tačno vrijeme i datum kada je to učinio, svoje osnovne podatke, brojeve telefona i email adrese koje je unio u formulare za registraciju, da je istog dana, nakon par časova podignut veb sajt na kome je predstavljena njegova internet prezentacija sa IP adrese koja je inače bila u vlasništvu Telekoma. Na isti način iz dopisa Interenet provajdera utvrđeno je da su zabeležene 2 konekcije na naloge elektronske pošte, koja je pripadala okrivljenom sa IP adrese koje su bile dodijeljene korisniku – okrivljenom, da su ostvarene putem ADSL veze koja je instalirana na fiksnom telefonskom priključku a to je bio upravo broj telefona koji je okrivljeni naveo u formularu za registraciju domena. Radilo se o priključku čiji je pretplatnik bila majka okrivljenog, a ADSL se vodio na ime okrivljenog.

11.7. Falsifikovanje isprave (čl.412 KZ)

Sljedeći primjer tiče se krivičnog djela falsifikovanje isprave. Naime, okrivljenom iz ovog postupka stavljeno je na teret da je nabavio radi upotrebe lažne isprave, to su dva kladioničarska tiketa, tako što je NN lice na računaru kladionice na navedenom uplatnom mjestu, sa optičkog diska pokrenuo program koji je omogućio da se zaobiđe informacioni sistem kladionice, da se izvrši modifikacija kladioničarskog tiketa koji se već nalaze u bazi i čiji je datum kreiranja validan, te da se na njih potom unesu rezultati već odigrane utakmice sa već poznatim ishodom. Nakon toga, uz pomoć programa kladionice za evidenciju tiketu, pregledana je grupa tiketa koji još nijesu poslati u centralu kladionice, koji su već uplaćeni, otkucani u vremenskom periodu prije početka odigranih mečeva. Uz pomoć navedenog programa napravljena su dva dobitna tiketa tako što je izmijenjen sadržaj postojećih tiketa u bazi podataka kladionice, u njih su unijeti podaci u vidu poznatih ishoda, već odigranih utakmica, koje je potom otštampao koristeći tikete kladionice i na taj način uticao na rezultat elektronske obrade podataka, potom tako sačinjene tikete koji su prepoznati kao dobitni, predao okrivlje-

nom koji ih je upotrebio kao prave, donio na naplatu na uplatno mjesto, pri čemu je jedan od tiketa i isplaćen.

11.8. Zloupotreba službenog položaja (čl.416 KZ)

Jedan od zanimljivijih primjera je postupak (koji jedini primjer u ovom Priručniku koji još nije pravnosnažno okončan), u kojem se radi se o službenom licu koje je zaposleno u MUP-u i koje je prema navodima optužnice iskorišćavanjem svog službenog položaja i ovlašćenja, prekoračenjem granica svog službenog položaja, pribavio korist drugookrivljenom, na način što je na njegov zahtjev, nakon što mu je drugookrivljeni dao određene brojeve mobilnih telefona (za koje se utvrdilo da pripadaju djevojci drugookrivljenog) zatražio da mu pribavi listing obavljenih razgovora preko mobilnih telefona tih brojeva, pribavio drugookrivljenom izvještaje o telekomunikacionom saobraćaju za navededne telefonske brojeve, zatim ih snimio na fleš memoriju koju je predao drugookrivljenom, a sve to, prema navodima optužnice, iskorišćavanjem svog službenog položaja.

11.9. Neovlašćeno iskorišćavanje autorskog djela ili predmeta srodnog prava (član 234 KZ)

U pogledu krivičnog djela neovlašćeno iskorišćavanje autorskog djela ili predmeta srodnog prava, najčešći oblik izvršenja ovog krivičnog djela sastoji se u tome što je izvršilac neovlašćeno umnožavao i stavljao u promet različita autorska djela: filmove u DVH ili DVD formatu, muziku u MP3 formatu, kompjuterske programe i igre, enciklopedije i druge multimedijalne sadržaje. Na taj način, neovlašćeni izvršilac je razmjenom i posredstvom interneta prethodno nabavljao kopije autorskih djela koje je smještao u memoriju svog računara i na optičke diskove CD-R i DVD-R, potom oglašavao njihovu prodaju putem svojih internet stranica, ostavljajući kao kontakt svoju elektronsku adresu. Putem elektronske pošte zainteresovanim kupcima slao je katalog sa pojedinačnim naslovima autorskih djela, čije je kopije nakon pristazanja narudžbine na svom računaru dalje umnožavao, zatim ih pakovao i tako pripremljene grupisao po narudžbinama koje je kupcima dostavljao lično, a drugima preko poštanskih uputnica, ostvarujući na taj način protivpravnu imovinsku korist za sebe.

Drugi vid je neovlašćeno umnožavanje i stavljanje u promet računarskih softvera, pa tako na primjer karte za GPS uređaje, koji predstavlja autorsko djelo, Garmin čiji nosilac autorskih prava je preduzeće, koje je ovlašćeni zastupnik za određenu teritoriju. Ovo djelo vršeno je tako što je u štampanim izdanjima i na internetu oglašavano pružanje usluga instaliranja

računarskih softvera, Garmin mapa. Izvršilac je ostavljao svoje brojeve mobilnih telefona za kontakt i dogovor i adresu elektronske pošte, nakon čega po dogovoru, navedene softvere i mape dostavljao i instalirao kupcima za određenu cijenu i na taj način ostvario protivpravnu imovinsku korist.

Specifičnost za navedeno krivično djelo je i činjenica da se bez obzira na broj primjeraka autorskih djela koje se odnose na filmski, muzički i multimedijalni sadržaj, svi pojedinačno moraju navesti, pa praksa, u regionu, bilježi situaciju u kojoj postoji prvostepena presuda, koja na prvoj i drugoj strani ima uvod, lične podatke okrivljenog, izreku u kojoj je naveden način izvršenja, a zatim počinje nabrajanje primjeraka autorskih djela, u vidu filmskih sadržaja, računarskih programa, muzičkih sadržaja do 176 strane, potom pravna kvalifikacija i odluka o krivičnoj sankciji, nakon koje slijedi obrazloženje, koje, u najvećem broju, posebno zbog velikog broja priznanja izvršenja ovih krivičnih djela, nije duže od dvije – tri strane. U praksi se u prvo vrijeme nijesu navodili svi navedeni podaci ali je nakon odluke najvišeg suda praksa izmijenjena tako da u činjeničnom opisu optužnice a samim tim i buduće presude mora da bude navedeno da autorsko djelo predstavlja određen broj npr. kompakt diskova sa snimljenom muzikom i/ili DVD-a sa snimljenim filmovima uz obavezno navođenje i identifikaciju o kojim muzičkim djelima i filmovima se radi, ko je njihov autor, odnosno ko je lice koje je nosilac autorskog prava ili lice na koje je prenijeto autorsko pravo. U suprotnom bi se došlo u situaciju da radnja izvršenja predmetnog krivičnog djela nije bliže određena objektom djela, odnosno nazivom autorskog djela i subjektom autorskog prava, u kom slučaju bi nedostajao bitan element za postojanje krivičnog djela neovlašćeno korišćenje autorskog i drugog srodnog prava i slijedom toga bi se morao zauzeti stav da djelo koje je predmet optužbe nije krivično djelo.

Jedna od interesantnih odbrana je ona u kojoj okrivljeni ističe da je kolekcionar, da skuplja već dvadeset godina pojedina izdanja, da je počeo da prebacuje sa VHS na DVX format, da je lično pravio omote za filmove, na taj način sačinio je diskove koji su veoma slični originalu, ali koje ne prodaje. U konkretnom slučaju, iz izvještaja o vještačenju utvrđeno je da je forenzičkom analizom hard diskova pronađen veći broj omota za diskove elektronskog formata, veći broj kataloga diskova u elektronskom formatu, kao i programi koji bi mogli da se koriste za pripremu i štampanje kao što su NERO burning rom i slično. Ono što je opredijelilo tužioca, da krene u postupak a potom i sud da okrivljeni bude oglašen krivim, su dva oglasa u kojem se nudila, osim profesionalnog presnimavanja totalna rasprodaja DVX diskova istih naslova, bez ograničavanja broja primjeraka, navedena je cijena i broj telefona okrivljenog na koji su se zainteresovani mogli obratiti.

11.10. Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka, krivično djelo računarska sabotaža, krivično djelo pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnog djela protiv bezbjednosti računarskih podataka, pravljenje i unošenje računarskih virusa - STICAJ

Jedan od takođe zanimljivih pravnosnažno okončanih predmeta je postupak protiv okrivljenog koji je prvim stavom izreke oglašen krivim za krivično djelo neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka, krivičnog djela računarska sabotaža i krivično djelo pravljenja, nabavljanja i davanja drugom sredstava za izvršenje krivičnog djela protiv bezbjednosti računarskih podataka a drugim, trećim i četvrtim stavom izreke je oglašen krivim za krivično djelo neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka i krivično djelo računarska sabotaža, a stavom pet presude je oglašen krivim za produženo krivično djelo pravljenje i unošenje računarskih virusa i jedno produženo krivično djelo pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnog djela protiv bezbjednosti računarskih podataka.

Okrivljeni se kršeći mjere zaštite neovlašćeno uključio u računarsku mrežu, neovlašćeno pristupio elektronskoj obradi podataka, na taj način što je prethodno koristeći anonimne servise – usluge raznih pružaoca takvog načina pristupa internet mreži, a u cilju anonimnog korišćenja interneta, radi prikrivanja svog djelovanja, kao što su hotspot, wireless, koja omogućava izlazak na internet kroz otvorene bežične mreže pristupa, svojeručno mijenjajući takozvane MAC adrese *(Media Access Control Address- jedinstven broj kojim se vrši identifikacija uređaja)* mrežne kartice računara koje je koristio a koja adresa služi za identifikaciju mrežnog uređaja, tj. računara u mrežnom okruženju, pri tom koristeći nekoliko Socks 5 protokola konekcija *((Internet protokol koji usmjerava mrežne pakete između klijenta i servera preko proksi servera i obezbjeđuje autentifikaciju tako da samo ovlašćeni korisnici mogu da pristupe serveru, koji omogućavaju da se IP (internet protokol) adresa korisnika prikrije, tj. da se komunikacija sa drugim računarom odvija preko udaljenih računara (servera) za opsluživanje drugih računara, a koji nasumice dodjeljuju IP adrese iz bilo kog opsega adresa, pri čemu se prava IP adresa korisnika ne otkriva))*

Okrivljeni je neovlašćeno pristupio zaštićenoj računarskoj mreži, centralnom serveru za kontrolu svih internet prezentacija jednog preduzeća za pružanje usluga pristupanja internetu na čijem serveru je bila smještena internet prezentacija državnog organa. Koristeći pseudonim unio je, uništio, izbrisao i izmijenio sadržaj i na taj način učinio neupotrebljivim računarske podatke i programe. Namjera je bila da onemogući i

znatno omete postupak elektronske obrade podatke koje su od značaja za državni organ, na taj način što je u elektronskom zapisu centralnog kontrolnog servera izbrisao takozvane administrativne, tj. upravljačke korisničke pristupne podatke *(korisničko administrativno ime i lozinku za otključavanje – omogućavanje pristupa uređivanju prezentacije).* Onemogućio je dalji pristup, od strane ovlašćenih lica kontroli podataka i samoj interenet prezentaciji, nakon čega je te kontrolne podatke, tj. korisničko ime i šifru svojeručno promijenio, upisujući takozvane "standardne vrijednosti" Koristeći ime i šifru admin-admin, proslijedio je podatke drugom na upotrebu radi izvršenja krivičnog djela neovlašćen pristup zaštićenom računaru, mreži ili elektronskoj obradi podataka, tako što je navedene podatke odmah distribuirao putem različitih socijalnih i komunikacionih mreža na internetu drugim licima, radi nastavka neovlašćenog pristupa i izmjene sadržaja navedene inernet prezentacije.

Navedeni primjer na vrlo jasan način prikazuje koliko je neophodno da se unapređuju znanja sudija i tužilaca iz procesnog i materijalnog krivičnog prava i savladaju osnovni pojavni oblici računarskog kriminala.

U stavu 2 izreke presude, ponavlja se na bezmalo jednak način izvršenje krivičnog djela i to različito samo u pogledu toga što je pristupao centralnom serveru za kontrolu svih internet prezentacija, intenet servis provajdera, a na kojim serverima su bile inernet prezentacije različitih državnih ograna, javnih službi, ustanova, preduzeća i drugih subjekata, koristeći pseudonime, unosio, uništio, izbrisao, izmijenio, oštetio, prikrio ili na drugi način učinio neupotrebljivim računarske podatke tako što je mijenjao korisničke pristupne podatke, a nakon toga u elektronske baze podataka internet prezentacija svojeručno unosio izmjene sadržaja tekstva, fotografija i drugih elektronskih podataka ili u potpunosti brisao internet prezentaciju i podatke, umjesto čega je u elektronske baze koje su bile javno dostupne unosio prethodno pripremljene sopstvene prezentacije koje su imale razne poruke, pa je tako neovlašćeno pristupio a zatim onemogućio ili znatno omeo postupak elektronske obrade i prenosa podataka na internet prezentacijama, između nekoliko fakulteta, sudova različitog ranga, zatim je pristupao internet prezentacijama različitih političkih stranaka, medijskih kuća, agencija, ministarstva, sajtu koji je bio posvećen parlamentarnim izborima i dr.

Tačkom 5 izreke, okrivljeni je oglašen krivim da je napravio računarski virus u namjeri unošenja u tuđe računare i računarske mreže. Okrivljeni je na svom kućnom računaru napravio računarski virus potom na većem broju hakerskih internet sajtova objavio svoj računarski virus, (program za protivpravni pristup i kontrolu računara) kome je dao određeni naziv i koji bi se kada bi ga neki korisnik preuzeo i iskoristio, njemu vraćao u formi novog PHP Shell *(koristi za administraciju i održavanje sajta, za raspakivanje i pomjeranje velikih fajlova)* i obavještenja gdje i na koji način je virus prisutan i na

koji tačno način zaraženi računar može biti kontrolisan, a zatim na jednoj adresi elektronske pošte posjedovao tako pribavljenih preko 600.000 šelova a na drugoj adresi elektronske pošte 176.000, pri čemu je dakle jedan šel služio sa pristup jednom sajtu ili nalogu.

Ovo govori da je imao pristup na svaki zaražen računar, koji je neko drugo lice koristilo, a da to lice nije ni svjesno da mu je računar zaražen i time je izvršiocu bilo omogućeno da pristupa ostalim internet sajtovima koji su se nalazili na serverima, preko takozvanog backdoor pristupa. Tako pribavljenih oko 776.000 PHP Shell, izvršioc je kasnije unosio u tuđe računare i računarske mreže na internet prezentacijama koje je izmijenio, čime je imaocima tih prezentacija pričinio štetu u vidu nemogućnosti pristupa i korišćenja internet prezentacija i time istovremeno pričinio i materijalnu štetu u neutvrđenom iznosu.

Ono što je zanimljivo da je u konkretnom slučaju okrivljeni, koji je učenik srednje "Elektrotehničke škole", priznao izvršenje svih krivičnih djela, neoženjen, bez djece, krivična djela je, a bilo ih je ukupno 12, izvršio u periodu od godinu i nešto više dana.

Njegova odbrana je unijeta u integralnoj verziji na 6 strana. Iz takve odbrane se može steći slika o tome na koji način ovi mladi ljudi razmišljaju, šta ih motiviše i na koji način vrše ova krivična djela, a ono što je još važnije i na koji način sud može da preduzme radnje koje sadrže sva bitna obilježja krivičnog djela iz oblasti računarskog kriminala.

Kod dokazivanja bitno je pribaviti izvještaj od Internet provajdera koji je pružao usluge hosting svakoj pojedinoj web stranici, kako o logovima pristupa serveru za prezentaciju "napadnutih" sajtova tako i sadržaj prezentacije prije i posle napada.

11.11. Zloupotreba platnih kartica (čl.260KZ)* i prikrivanje (člana 256 KZ)

Izvršilac koji je mlađe punoljetno lice je neovlašćeno, u više navrata upotrijebio poverljive podatke koji jedinstveno uređuju prave platne kartice u platnom prometu i to sa jedanaest različitih platnih kartica čiji su izdavaoci banke iz Sjedinjenih Američkih država. Okrivljeni je pribavio sebi protivpravnu imovinsku korist, na taj način što je koristeći elektronski nalog za elektronske naručivanje i plaćanje preduzeća Card servis na internet stranici navedenog preduzeća, koristio dvije lažne adrese elektronske pošte, lažno se predstavljajući drugim imenom, upotrebio povjerljive podatke sa jedanaest platnih kartica, navedenih banaka, u ukupno 98 navrata, tako što je u polja predviđena za popunjavanje podataka o platnim karticama, unosio prethodno pribavljene podatke o platnim karticama, ime i prezi-

me korisnika, vrijeme validnosti i broj platne karitice. Okrivljeni je kupovao karte za muzičke koncerte poznatih svjetskih izvođača, nakon čega je šifre naručenih karata predavao drugookrivljenom, koji ih je potom predao trećeokrivljenom, koji je podizao karte za koncerte na biletarnici gde je saopštavao šifre rezervisanih karata, a potom su karte pribavljene na taj način prodavali.

Prema njemu je kao prema mlađem punoletnom licu, on je inače 1992 godište, student Računarskog fakulteta, izrečena vaspitna mjera pojačanog nadzora od strane organa starateljstva, koja može trajati najmanje 6 mjeseci, a najduže 2 godine. Izrečena mu je posebna obaveza da se osposobljava za zanimanje koje odgovara njegovim sposobnostima i sklonostima, kao, obaveza se izriče u trajanju do 1 godine, a sud može njeno izvršenje izmijeniti ili obustaviti. Navedeno mlađe punoljetno lice je između ostalog u svojoj odbrani navelo da intenet koristi više od 9 godina, da se registrovao na jednom internet forumu, da je vidio reklamu za internet sajt na kome se prodaju podaci o platnim karticama, da se na tom sajtu registrovao, otvorio nalog, sačuvao ga sa šifrom na svom računaru, tako da se pri svakoj konekciji otvarao njegov nalog, zatim je na tom sajtu kupio podatke o platnim karticama, za vrijednost od 200 američkih dolara, podaci su prebačeni na njegov nalog i sadržavali su podatke o kartici i datum isteka, Cvv2 broj. Potom je ušao na sajt koncertne dvorane, rezervisao karte, najpre radi probe, pa kako se ispostavilo da funkcioniše, stizalo mu je obavještenje da je karta uspješno rezervisana. Dobio je broj pomoću kojeg se karta može podići, te brojeve je zapisivao, davao drugom okrivljenom uz dogovor da ih uz pomoć rezervacije on podiže, ali ne i da ih prodaje. Prilikom konekcije, okrivljeni je za internet koristio računar koji se nalazio u prostorijama škole koju je ranije pohađao i to u sali za računare koja ima internet konekcije. On je tvrdio je da nije imao namjeru pribavljanja protivpravne imovinske koristi, da nije želio da izvrši krivično djelo, već da vidi da li će to da funkcioniše.

Drugokrivljeni, njegov drug, je objasnio da mu je mlađe punoletno lice reklo da će mu proslijediti šifre i jedan dio je poslao na njegovu email adresu koja je navedena, a drugi dio na njegov Facebook nalog, preko četa na ICQ na njegov laptop. Poslao mu je šifre za rezervaciju za preko 250 karata, neke mu je usmeno diktirao, pa ih je zapisao na papiru.

Pregledom hard diska, od jednog lica koja su bili procesuirana, pronađeni su korisnički email nalozi, imena sa lozinkama za logovanje na internet sajtove, koji su označeni u opisu radnje, zatim je izvršen uvid u listing izvršenih transakcija na prodajnom mjestu sa potvrdama banaka iz Amerike o falsifikatu i kopijama slipova izvršenih transakcija. Sud je utvrdio detalje tih sumnjivih transakcija, ime i prezime i koje karte su kupljene, kao činjenicu da je banka izdavalac Visa kartica u dopisima upućenim lokalnoj banci potvrdila da su upotrijebljene platne kartice falsifikovane, a imena kupaca koja se pojavljuju i imena vlasnika kartica nijesu jednaki. Izvršen je i uvid u

izvještaj o korisniku IP adrese, pa je utvrđeno da je kao korisnik registrovana jedna osnovna škola. U postupku pregleda i analize sadržaja dva hard diska, utvrđeno je da su pronađene izvjesne tekstualne datoteke kao i Skype komunikacija, telefonski imenik i Facebook live chat, da je sačinjen zapisnik u službenim prostorijama MUP-a da je konstatovano da je u prisustvu branioca i osumnjičenog mlađeg punoljetnog lica izvršeno otvaranje i započet proces očitavanja digitalnih otisaka iz tri laptop računara, da su branilac i okrivljeni napustili prostorije MUP-a RS dok je postupak još uvijek trajao a da nijesu imali primjedbi na dio postupka kome su prisustvovali.

Zatim je izvršen uvid u izvještaje službe za specijalne istražne metode, odjeljenja za elektronski nadzor o vještačenju mobilnog telefona i SIM kartice, pa je tom prilikom ostvaren uvid u imenik, u listu poziva iz telefona, SMS poruke na osnovu čije sadržine je utvrđeno da su dva lica iz postupka imala komunikaciju, da se pojavljuju šifre pored imena Elton, da postoje i tekstualne poruke u telefonu koje su zavedene u statusu unsent, a gdje se takođe pojavljuje ime jednog od izvođača sa koncerta i brojevi šifri rezervisanih karata.

Kod krivičnog djela falsifikovanje i zloupotreba platnih kartica, važno je utvrditi da li je učinilac ovog krivičnog djela postupao u saizvršilaštvu ili je imao pomagače, obzirom da prema načinu izvršenja, radnja izvršenja vrlo često obuhvata više lica koja imaju različita zaduženja kao što su nabavka blanko kartica, nabavka uređaja, nabavka kodova, izrada lažnih platnih ili preinačenje pravih platnih kartica, neposredna upotreba u prometu ili distribucija radi upotrebe u prometu. Važno je kod preinačenja prave platne kartice utvrditi namjeru da se takva kartica upotrebi kao prava.

Sljedeći predmet je pokazatelj da je u nelegalnom poslu učestvovalo više lica. Optuženi AA je u periodu od nekoliko mjeseci organizovao kriminalnu grupu koja je imala za cilj vršenje krivičnih djela falsifikovanje i zloupotreba platnih kartica radi sticanja finansijske koristi. Kriminalna grupa je postojala određeno vrijeme, njeni pripadnici su djelovali sporazumno, svjesno prihvatajući aktivnosti grupe i manifestujući ovu pripadnost izvršavanjem unapred određenih zadataka. Optuženi AA posjedovao je opremu za izradu platnih kartica – uređaj za čitanje i pisanje po magnetnoj pisti platnih kartica, računar i laserski štampač, kupovao je putem interneta identifikacione podatke za izradu lažnih platnih kartica, organizovao je plaćanje za kupljene podatke preko "Western union" službe. Izrađivao je lažne platne kartice i pronalazio vlasnike, odnosno radnike na prodajnim mjestima koji su omogućavali da se na POS terminalima instaliranim u prodajnim objektima upotrebljavaju lažne platne kartice kao prave. Optuženi BB imaoje zadatak da izrađuje i upotrebljava lažne platne kartice kao prave, a optuženi II je imao zadatak da upotrebljava lažne platne kartice kao prave.

U toku postupka nesumnjivo utvrđeno na osnovu nalaza i mišljenja vještaka koji je naveo da datoteka računara (koji je oduzet od optuženog AA) sa-

drži gotove podatke za izradu 10 magnetnih pista platnih kartica i 11 lažnih platnih kartica koje su pronađene prilikom lišenja slobode optuženih EE i VV, a koje predstavljaju predmete i materijale korišćene za izradu lažnih platnih kartica, te da hard disk i USB memorije sadrže podatke koji potencijalno mogu da se koriste za pravljenje lažnih platnih kartica ili pak za neovlašćenu trgovinu sa ukradenim podacima o platnim karticama, da 5 mini kompakt-diskova (koji su oduzeti od optuženog AA) koji predstavljaju instalacione diskove za uređaj "mini 123" i "mini 400" . Po mišljenju vještaka ovi urađaji imaju funkciju čitača i pisača po magnetnoj pisti plastičnih kartica, a takođe da su folije na karticama koje su pronađene prilikom lišenja slobode optuženih EE i VV odštampane laserskim štampačem koji je pronađen i oduzet od optuženog AA. Prema mišljenju ovih vještaka pronađeni kablovi služe za povezivanje računara i uređaja "mini 123" i "mini 400" jer sa jedne strane, SS imaju serijski broj RS 232 DBS PORT koji ide na računar, a sa druge strane mini USB port koji je istog profila kao kabl iz uputstva.

Prvostepeni sud je dovodeći u vezu iznijetu sadržinu ovih dokaza sa sadržinom razgovora koje su optuženi AA i BB vodili, a što je utvrđeno iz transkripta, nesumnjivo utvrdio, bez obzira na činjenicu da uređaj za pisanje po magnetnoj pisti platnih kartica nije pronađen, da je optuženi AA posjedovao svu potrebnu opremu za izradu falsifikovanih platnih kartica, te da su optuženi AA i BB pravili lažne platne kartice. Optuženi AA i BB su napravili više lažnih platnih kartica i to tako što su identifikacione podatke upisane u magnetni zapis originalne platne kartice čiji su korisnici strana fizička lica – broj platne kartice, datum važenja platne kartice i druge sigurnosne podatke, koje je optuženi AA kupovao putem interneta na forumima od NN lica, pomoću računara i uređaja za čitanje i pisanje po magnetnoj pisti platnih kartica nanosili na preštampanu bijelu plastiku, koju je nabavio optuženi VV i predao optuženom BB. Okrivljeni su zatim preko iste preljepljivali providnu plastičnu foliju na koju su laserskim štampačem naštampali lažno ime i prezime lica korisnika kartice, broj kartice i predavali ih članovima kriminalne grupe koji su u prodajnim objektima upotrebljavali lažne platne kartice kao prave, plaćajući robu i usluge.

Kako je brojnost ovih krivičnog djela u porastu, navešće se i ostali oblici zlouupotrebe platnih kartica: zloupotreba kod plaćanja bez fizičkog prisustva kartice (plaćanje preko interneta, plaćanje preko mobilnih telefona), krađa identiteta, zloupotreba od strane korisnika kartice (kod plaćanja preko interneta-poricanjem da je izvršeno plaćanje, zloupotreba od strane članova porodice), unutrašnje zloupotreba (od strane službenika banaka, izrada fiktivnih kartica, kopija kartica, otkrivanje PIN-a), indirektna zloupotreba (pranje novca, finansiranje terorizma).

11.12. Prikazivanje, pribavljanje i posjedovanje pornografskog sadržaja i iskorišćavanje maloljetnog lica za pornografiju (čl.211KZ)* u sticaju sa krivičnim djelom prinude (čl.165 KZ)

Najveći broj predmeta, koje smo koristili u procesu pripreme ovog Priručnika, tiču se računarskog kriminala i odnose se na navedeno krivično djelo. U pogledu ovog krivičnog djela količina oduzetog materijala se kreće od nekoliko desetina fotografija do 1 Terabajta (*1 TB = 1024 GB, ilustracije radi, ako je jedna slika je oko 1MB, onda je 1TB oko jedan milion slika, mala slika može biti 100KB, onda je 1TB = 10 miliona slika, ili 300 sati video zapisa*) nedozvoljenih sadržaja.

Interesantan je primjer ovog krivičnog djela u sticaju sa krivičnim djelom prinude. Naime, oglašen je krivim da je u više navrata iskoristio maloljetnu oštećenu za proizvodnju slika i audio vizualnih zapisa pornografske sadržine i prikazivao joj audio video zapise iste sadržine, koristeći internet servis Skype, koji funkcioniše kao P2P mreža *((peer to peer mreža-vrsta decentralizovane i distribuirane mrežne arhitekture u kojoj pojedini čvorovi u mreži (pod nazivom"peer") djeluje i kao izvor i potrošač. U peer-to-peer mreži datoteke ili streaming audio/video se dijele između više međusobno povezanih "peers" čiji su već sačuvani fajlovi u svakom od računara direktno na raspolaganje drugim učesnicima te mreže, bez potrebe za centralizovane koordinacije od strane servera) mreža preko koje se pruža usluga internet telefonije, prenosa snimaka sa veb kamera u realnom vremenu i razmjena tekstualnih poruka))* i to tako što je stupio u komunikaciju sa maloletnom oštećenom, koristeći korisnički profil čije ime je navedeno. Okrivljeni se lažno predstavljao da je njen vršnjak. Tražio je da se pred kamerom skida u više navrata i to sve snimao, a potom kada to više nije željela da čini, prijetio da će postojeće video fajlove pokazati njenim prijateljima, porodici i postaviti na Facebook.

Prilkom obrazlaganja osuđujućih presuda treba imati na umu da distribucija, u smislu Konvencije o zaštiti djece od seksualne eksploataciji i seksualnog zlostavljanja, podrazumijeva aktivno i redovno dostavljanje nedozvoljenih pornografskih sadržaja drugim osobama uz upotrebu računarskih mreža. Izraz pribavljanja za sebe ili za drugo lice obuhvata pribavljanje materijala putem „skidanja" (download) sa interneta ili kupovine filmova ili fotografija sa nedozvoljenim sadržajem. Posjedovanje obuhvata posjedovanje nedozvoljenih sadržaja bilo u štampanom materijalu ili fotografijama i/ili video snimcima kao i čuvanje takvih podataka na računaru.

U pojedinim zakonodavstvima već sam pristup web sajtovima sa dječijom pornografijom putem računarskih tehnologija nije dozvoljen, ima za cilj da inkriminiše onlajn pristup nedozvoljenim sadržajima čak i bez „skidanja"(download) sa interneta i čuvanja na optičkim medijima.

11.13. Računarska sabotaža (čl.350 KZ)*

Predmet je zanimljiv utoliko što je okrivljeni u svojstvu glavnog analitičara za informisanje i izvještavanja sa računara za koji je bio zadužen i koji se nalazio u službenim prostorijama izbrisao računarske podatke koji su se na njemu nalazili u namjeri da onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za njegovu službu i to preko 5000 dokumenata koji su imali oznaku „službene tajne" ili „za internu upotrebu".

U ovom predmetu je pribavljen izvještaj, a zatim je na glavnom pretresu saslušan vještak, po struci inženjer informatike, koji je detaljno objasnio, postupak prilikom uzimanja imidža, odnosno kopije hard diska. Vještak je objasnio da se prilikom klasičnog brisanja, podaci nikada trajno ne skidaju sa računara, već se samo briše informacija da je podatak postojao, da je izvršen povraćaj podataka sa imidža hard diska i sa računara. Vršeno je generisanje otiska SHA256, (*Secure Hash Algorithm*) i utvrđeno je vrijeme brisanja dokumenata.

Primjer dobrog postupanja: Navedeno je da je vještak pozvao odgovorno lice, načelnika odjeljenja koji je bio prisutan sve vrijeme tokom vještačenja, da je sačinjen zapisnik, da je prije započetog vještačenja, računar bio zapečaćen, da je brisanje u konkretnom slučaju nastalo putem običnog brisanja, dakle da hard disk nije bio formatiran.

Vještak dalje objašnjava šta se zapravo dešava kada se formatira disk, pa navodi da za korisnika nestaju sve datoteke koje su se nalazile na hard disku, ne postoji ni operativni sistem, a u konkretnom slučaju utvrđeno je da su brisana dokumenta iz nekoliko direktorijuma sa ekstenzijom .doc i .exl, dakle Excel tabele i Word dokumenti. Vještak je opovrgao tezu odbrane tako što je naveo da prisustvo virusa nije moglo da dovede do brisanja ovih foldera, jer nijesu obrisana sva dokumenta sa navedenim ekstenzijama.

Pročitan je izvještaj o vještačenju MUP RS Službe za specijalne istražne metode, Odsjeka za prikupljanje i obradu digitalnih podataka. Objašnjeno je na koji način je izvršena aktivizacija podataka, šta je zatečeno u računaru, da je korišćen uređaj Logikub Talon, da je korišćen softverski alat forenzik tul kit, i da je sadržaj hard diska fiksiran generisanjem digitalnih otisaka SHA 256, pa se navodi dugačak niz cifara i slova. Sve je to snimljeno na disk koji je dostavljen sudu i vršen je uvid u sadržinu navedenog diska na glavnom pretresu. Prvostepeni sud je zaključio da je nalaz i mišljenje dato od strane stručnjaka koji je kvalifikovan za oblast u kojoj je vještačio i da je dakle koncipiran tako da logično slijedi iz utvrđenih činjenica.

Kod krivičnog djela računarske sabotaže objekat krivičnog djela su računar i drugi uređaji za elektronsku obradu i prenos podataka. Prema Krivičnom zakoniku Crne Gore, ovo krivično djelo postoji ukoliko je izvršeno prema

bilo kom računaru, a kada se radi o računarima koji su od posebnog značaja za državne organe, javne službe, ustanove, preduzeća i druge, oni su obuhvaćeni kvalifikovanim oblikom ovog krivičnog djela.

XII DRUGOSTEPENI POSTUPAK

12.1. Navedeni **primjer** je dobar i sa aspekta sljedećeg dijela Priručnika – razmatranje navoda odbrana kojima se najčešće osporava prvostepena presuda u drugostepenom postupku.

Žalbama se napadaju odluke suda po svim zakonskim osnovima, a ovde ćemo predstaviti neke:

- osporava se ličnost vještaka u smislu njegove stručnosti za ovu oblast, reference, broj do sada obavljenih vještačenja,
- ističe se da se presuda zasniva na dokazu na kojem se po odredbama ZKP-a ne može zasnivati, (nedozvoljeni dokaz) poziva se na odredbu ZKP o tome ko može biti vještak, pa tako da lice prema kome je krivično djelo učinjeno, ne može biti određeno za vještaka, a ako jeste onda se na njegovom nalazu i mišljenju ne može zasnivati sudska odluka, pa stim u vezi zaposlenost kod oštećenog predstavlja razlog za njegovo izuzeće. (U konkretnom slučaju oštećen je MUP i izvještaj o vještačenju je potpisao policijski narednik koji se kasnije u postupku tretira kao sudski vještak. Vještačenje povjereno ustanovi – Odsjeku za prikupljanje i obradu digitalnih dokaza MUP-a, koje se nalazi u resoru unutrašnjih poslova) (*-u drugostepenoj presudi je odgovoreno na takav žalbeni navod, da se vještačenje može povjeriti ustanovi koja se nalazi u resoru unutrašnjih poslova, kada resor raspolaže takvom stručnom službom, te po nalaženju drugostepenog suda vještačenje nije bilo u suprotnosti sa odredbama ZKP-a koje regulišu oblast vještačenja. Drugostepeni sud je dalje našao da je pravilno prvostepeni sud u potpunosti prihvatio izvještaj o vještačenju MUP, službe za specijalne istražne metode - Odsjeka za prikupljanje i obradu digitalnih dokaza, obzirom da je dat od strane stručnjaka koji je kvalifikovan za oblast u kojoj je vještačio, a koncipiran je tako da logično slijedi iz utvrđenih činjenica, te je predmetno vještačenje obavljeno u skladu sa odredbama ZKP-a*)
- da je presuda nerazumljiva, obzirom da se u izreci ponavljaju izrazi na stranom jeziku (*file, Recycle Bin i dr.).* Suštinski dio presude sadrži pojmove na engleskom jeziku, u žalbi se citira član koji u skladu sa Ustavom i zakonom predviđa jezik u službenoj upotrebi u krivičnom postupku,
- pravilnost utvrđenog činjeničnog stanja, u presudi se ne navode obe-

ležja računara sa kojeg su podaci izbrisani, kako bi bio individualizovan računar, vještak se poziva na takozvani SHA-256 broj, ali u presudi nema podataka o serijskom broju jedinice, čvrstog diska, njegovom proizvođaču, kapacitetu i drugim podacima na osnovu kojih bi se tačno utvrdilo na kojim predmetima informatičke opreme je preduzeta inkriminisana radnja izvršenja, da li je okrivljeni bio zadužen računarom sa kog su navedeno podaci obrisani. (Stim u vezi treba ponoviti iz prvog dijela Priručnika da izvještaj o pregledu hard diska mora da sadrži podatke o proizvođaču i modelu računara, serijskom broju, proizvođaču diska, modelu hard diska, serijskom broju hard diska, kapacitetu, vrijeme izvršenja krivičnog djela, te da li je okrivljeni tada imao pristup računaru.

- Osporava se nalaz i mišljenje vještaka navođenjem odbrane da je tehnički nemoguće da se stotine dokumenata izbriše u istom satu, istom minutu ili tačno određenoj sekundi pa čak i da se pretpostavi da su bili grupisani i raspoređeni bili bi hronološki brisani jer brisanje podrazumijeva makar jedan klik na tastaturi ili na mišu,
- Nema krivičnog djela, jer je okrivljeni podatke koje je obrisao, presnimio na svoj eksterni disk, te dakle on samim tim nije izbrisao službenu dokumentaciju, ona je samo bila prebačena na fleš memoriju, dakle, da nije izbrisao ili učinio neupotrebljivim podatke.
- Slijed od trenutka oduzimanja predmeta pa do prezentiranja dokaza pred sudom, obzirom da iz pismenih dokaza proizilazi da su računar i eksterni nosač memorije predati drugim službama, da niko prije vještačenja nije znao gde se nalazi kompjuter, ko ga je odnio, kada je vraćen.
- Prvostepeni sud je propustio da utvrdi da li je postojala mogućnost manipulacije sa računarom koji nije pregledan i vještačen više mjeseci od dana kada je oduzet.
- Prvostepeni sud nije utvrdio kako je brisanje tih dokumenata skupno i pojedinačno uticalo na postupak elektronske obrade i prenosa podataka oštećenog, odnosno da li su svi ti podaci čuvani i na nekim drugim računarima u okviru iste službe, čime bi se isključila mogućnost da je služba trpela i da je bila onemogućena u radu
- Konstatuje se da nije u prisustvu branioca ili okrivljenog uzet SHA broj sa hard diska,
- Pretpostavlja se da je neko mogao da promijeni vrijeme u BIOS-u, (*Basic Input-Output System, pronalazi i učitava operativni sistem u radnu memoriju (RAM*) *i sadrži programe koji omogućuju rad tastature i monitora*) što je vještak dozvolio kao mogućnost .
- Upitno je da li se računari čuvaju neobezbijeđeno, da li se zaključavaju lozinkom, da li se pristupne šifre nalaze nalijepljene na kućište kompjutera ili uopšte negdje na vidnom mjestu, dostupne svima, da

li je svako mogao da uđe u prostoriju posle radnog vremena i uključi kompjutere.

- Nepotpuno utvrđeno činjenično stanje, obzirom da prvostepeni sud nije zatražio knjigu posjeta zgradi gde se nalazi ovaj računar, niti je saslušao obezbjeđenje na ulazu, i što kao jedan od elektronskih dokaza nije pregledao snimke sa kamera sa ulaza u zgradu gde se nalazio računar sa kojeg je izvršeno brisanje.
- U jednoj od žalbi u predmetu dječje pornografije, branilac postavlja tvrdnju da se jedino na osnovu ličnih dokumenata može utvrditi da li je neko lice maloljetno, odnosno mlađe od 18 godina, te da u konkretnom slučaju identifikacija lica koja se nalaze na materijalu koji je pronađen u računaru okrivljenog je izostala, nepoznato je ko su lica za koje sud utvrđuje da su maloljetna. Prema navodima žalbe to nije moguće utvrditi samo posmatranjem, jer akteri nekih od tih fajlova nijesu očigledno djeca, već tjelesno i polno formirana lica, pa je jedan od prijedloga branioca da se identifikacija mogla izvršiti preko proizvođača ili distributera filma, putem prepoznavanja ili putem međunarodne pravne pomoći, ili da se mora pribaviti nalaz i mišljenje vještaka antropologa ili drugih medicinskih stručnjaka, koji bi na osnovu naučnih metoda procijenio starosnu dob spornih lica u tim fajlovima.
- Osporava se presudom izrečena mjera bezbjednosti oduzimanja stvari – predmeta tj. računara, jer da je time okrivljenom uskraćeno pravo na širu društvenu komunikaciju.
- U žalbama se ističe nepostojanje umišljaja pa se u jednoj navodi da je okrivljeni koristeći softver E-mule u polja pretrage ubacivao „XXX“, što je oznaka za pornografiju, pa je onda skidao zipovane fajlove (*ZIP-format je format za kompresiju fajlova. Jedan ZIP-fajl može sadržati jedan ili više fajlova*). Dakle, nije mogao da zna sadržinu iste, pa kada bi ih „otpakovao“ i vidio šta je, brisao je one fajlove koji su sadržavali dječiju pornografiju, da se dešavalo da okrivljeni uopšte ne pogleda skinuti materijal već ga je direktno kopirao na diskove, da se iz dosadašnje prakse u gonjenju ove vrste krivičnih djela utvrdilo da osobe koje ciljano tragaju za pornografskim sadržajem nastalim iskorišćavanjem maloljetnih lica, u polja pretrage unose poseban termin tj. PTHC (*Preteen hard core)* a takvih pretraga kod okrivljenog nije bilo pa je trebalo primijeniti insitut in dubio pro reo, jer on nije ciljano tražio taj sadržaj.
- Osporeno je utvrđeno činjenično stanje pa se u jednoj žalbi navodi da je Izvještajem vještaka ustanovljeno da je određeni inkriminisani materijal (video klipovi koji mu se upravo i stavljaju na teret) koji je pronađen u računaru okrivljenog u FLV formatu (*Flash video je format datoteke koji se koristi za isporuku videa preko Interneta),* a da su vještaci konstatovali da računar okrivljenog ne posjeduje program koji bi mogao da otvori te foldere. S obzirom na tu činjenicu, postavljeno je pitanje kako je moguće nekom staviti na teret posjedovanje zabra-

njenog audio-video materijala, ako se taj materijal zbog nepostojanja adekvatnih alatki, odnosno programa, ne može koristiti.

- Ističe se žalbama da se presuda zasniva na dokazima na kojima se ne može zasnivati, pa tako u jednoj ističu da je prvostepeni sud u dokaznom postupku pročitao izvještaj Kancelarije za međunarodne poslove, Odjeljenja za unutrašnju bezbjednost SAD i da je iz tog izvještaja utvrdio da je lice sa teritorije Republike Srbije, pod korisničkim imenom koji je naveden u izreci presude, pristupao domenu, odnosno oglasnoj tabli na internetu, pod nazivom koji se navodi i utvrdio je da je ovaj domen bio specijalno namijenjen distribuciji slika i video zapisa zloupotrebe djece u svrhu pornografije. Na prvoj stranici ovog izvještaja se navodi da je Homeland Security Investigations istraživao prsten širom svijeta rasprostranjene eksploatacije djece, da je moguće da je osumnjičeni državljanin učestvovao u kriminalnoj aktivnosti, da se nadležnom MUP-u dostave imena srpskih državljanina koji koriste određene IP adrese, te da će ta kancelarija dostaviti više informacija i paket dokaza nakon prijema imena od strane MUP-a. Konačno, stav branioca da taj izvještaj ne može biti korišćen kao dokaz, iz jednostavnog razloga što je vidljivo da su u periodu do slanja ovog izvještaja tajno snimane komunikacije raznih korisnika različitih sajtova i to van teritorije Republike Srbije, da se nalogom da se osumnjičenom odredi pritvor dok se ne otkriju dokazi, koji su inače sadržani u izvještaju Homeland Security Investigations, krše osnovna prava čovjeka i građanina, a samim tim i pravo na odbranu.

Potencira se da istražni sudija nije donio rješenje kojim se odobrava praćenje i snimanje komunikacija korisničkog imena koje se navodi u izreci presude koje je koristio okrivljeni sa raznih IP adresa, pa je dokaz pribavljen suprotno Zakoniku o krivičnom postupku, zbog čega se smatra da je načinjena bitna povreda postupka. Nejasno je dalje da li se radi o sajtu ili oglasnoj tabli u okviru sajta, obzirom da se navodi da internet sajt sa nazivom označenim bio namijenjen za distribuciju slike i video zapisa nastalim dječijom zloupotrebom. Ako se radi o sajtu, onda je svakom dozvoljen i omogućen pristup takvom sajtu, a ako se radi o oglasnoj tabli u okviru sajta, onda to podrazumijeva članstvo koje je kategorizovano u više kategorija.

Osporeno je i da je materijal u AVI formatu uopšte pronađen u računaru okrivljenog. Branilac se pozivao da je bilo neophodno da se obavi nezavisno vještačenje kako bi se otklonile neke protivrječnosti, kako bi se utvrdilo tačno vrijeme preuzimanja materijala, zatim mogućnosti manipulacije administratora sajta sa korisničkim imenom, pa upoređivanje obima preuzetog materijala, stavljanje u korelaciju sa mjesečnom potrošnjom okrivljenog kod provajdera, kao i provjera tvrdnje da sav pronađeni materijal potiče iz aktivnog dijela hard diska računara okrivljenog.

Ovo je tipičan primjer problema koji se javljaju u praksi, kako prilikom

otkrivanja tako i procesuiranja i konačnog donošenja, na zakonu zasnovane, sudske odluke, a odnosi se na neophodnu prekograničnu saradnju, iz već ranije pomenutih razloga, za uspješnu borbu protiv visokotehnološkog kriminala. Može se dogoditi da se ospori način pribavljanja dokaza kada se elektronski dokaz nalazio u računaru na području druge nadležnosti, pod tim se ne misli samo na mjesnu nadležnost u okviru jedne države, već nasuprot, bilo gdje u svijetu.

- Osporava se sadržina transkripta, da nijesu izgovorene koje se navode u njima, da je pogrešno otkucano
- Osporava se da je glas okrivljenog na snimcima pribavljenim putem mjera tajnog nadzora.

12.2. Osim navedenih, već viđenih žalbenih navoda, treba se podsjetiti još nekih okolnosti o kojima sud, kako u prvostepenom tako i u drugostepenom postupku mora imati na umu tokom celog krivičnog postupka.

Pored nesumnjivog utvrđivanja kad, kako i gdje je krivično djelo izvršeno, ponekad je potrebno u sklopu odbrane, a radi njene provjere utvrditi stepen tehničkog znanja koji je bio potreban za uspješno izvršenje djela, jer ukoliko su preduzete radnje prefinjenije broj potencijalnih izvršilaca je manji.

Dalje, potrebno je kod pojedinih oblika krivičnih djela gdje se kao izvršilac javlja službeno lice, obuhvatiti i potreban nivo i dostupnost poznavanja okolnosti kao što su lozinke, šifre, kripto ključevi, organizacija podataka i sl., koji je bio neophodan za izvršenje krivičnog djela, što često može ukazati da li je krivično djelo izvršeno od strane nekog od zaposlenih ili od nekog spolja. Tada treba obratiti pažnju i na spisak zaposlenih koji, prema opisu posla, imaju mogućnost da budu izvršioci krivičnog djela. Ponekad je važno na pretresu utvrditi moguće motive za izvršenje krivičnog djela, važno je ispitati svedoke i to upravo prema njihovom poznavanju činjenica koje su bitne a potom kao i uvijek ocijeniti njihovu uvjerljivost, pouzdanost i dr. U tom slučaju, ponekad, je od značaja da se utvrde i postojeće slabosti u sistemu zaštite i kome su one bile poznate, zatim sva lica koja mogu biti potpuno obaviještena u pogledu izvršenog krivičnog djela.

Kako bi se postiglo bolje razumijevanje ove problematike, u situaciji kada sud mora primijeniti pravo u oblasti koja je za sada još nedovoljno poznata, vještak mora biti spreman da u pismenom nalazu i mišljenju ili prilikom usmenog izlaganja na glavnom pretresu, pruži sve relevantne informacije o oduzetom računaru, mrežnoj konfiguraciji, perifernim uređajima, korišćenim operativnim sistemima, softverima za upravljanje bazama podataka, programskim jezicima, nosiocima podataka i organizaciji podataka na njima, programima koje je koristio prilikom zrade nalaza i sl. Sudije i tužioci moraju biti spremni da bez oklijevanja postave sva potrebna pitanja čiji odgovori će razjasniti sve nedoumice.

Jako bitno je da postoji posebna opreznost kada se ocjenjuju pribavljeni podaci o nosiocima podataka, kao što su listinzi, magnetne trake, diskovi itd. Najprije je jako bitno utvrditi da je ono što je dobijeno zaista i ono što je traženo, da odgovara zahtjevima "autentičnosti" i najboljeg dokaza. Pri tome se pod dokazivanjem autentičnosti podrazumijeva podnošenje prihvatljivih dokaza da je ponuđeni dokument zaista generisan na tačno određenom računaru i to u tačno određeno vrijeme od strane određenog programa.

Sve češće ćemo se susretati sa korišćenjem računara kao sredstva izvršenja krivičnih djela i djela iz ostalih glava Krivičnog Zakonika, sa različitim zaštitnim subjektom (neovlašćena proizvodnja, držanje i satvljanje u promet opojne droge -čl.300 KZ, zloupotrebe djece, trgovina ljudima čl.444 KZ, posredovanje u vršenju prostitucije-čl.210 KZ, za korišćenje sistema za elektronski transfer novca, pranje novca-čl.268 KZ, iznuda-250 KZ, ucjena-čl.251 KZ, falsifikovanje novca-čl.258 KZ, oglašavanje na internetu prodaje škodljivih proizvoda - u vezi čl.297 KZ, terorizam- čl.447 KZ i dr.).

Značajno je i povećanje broja maloljetnih izvršilaca ovih krivičnih djela. Sve je veći broj mladih koji tokom svog školovanja u osnovnim i srednjim školama stiču osnovna informatička znanja, i predstavljaju ogroman potencijal za sve vrste zloupotrebe kompjutera.

Vještačenje dokaznog sredstva čiju je dokaznu vrijednost, sud ovlašćen da slobodno cijeni na osnovu savjesne i brižljive ocjene svih okolnosti, sud ima obavezu da podvrgne logičkoj analizi mišljenja vještaka, nije vezan tim istim nalazom i mišljenjem, pa iako nema stručno znanje postoji mogućnost da mišljenje vještaka ne prihvati kada nađe da iznijeti stavovi ne mogu odoljeti kritici, zasnovano je na pravilima logičkog zaključivanja i iskustva. Ukoliko prvostepeni sud ili uopšte sud posumnja u rezultate vještačenja ovlašćen je da preduzme sve što je potrebno da se takva sumnja otkloni ili da se odredi novo vještačenje.

U nekim složenijim predmetima teško je vršiti efikasnu kontrolu rada vještaka. U ovim postupcima prvostepeni sud nije vezan za službenu listu vještaka, u smislu da bi ona predstavljala ograničenje njegove slobode u izboru ovog, posebno u situaciji kada za predmete koji se tiču računarskog kriminala, a imajući u vidu količinu materijala koje je potrebno izvještačiti, nema dovoljan broj vještaka. Odredba čl.137 st.4 ZKP je upravo primjenjiva u takvim slučajevima kako vještak uvijek mora da da svoje mišljenje i da ga obrazloži. Postoji naravno i pravo da se vještaku neposredno postavljaju pitanja. To pravo imaju kako stranke u postupku tako i sudije, pa i članovi sudskog vijeća.

Vještak je dužan da ukoliko je stranka stavila određene i to konkretne primjedbe na nalaz i mišljenje nije dovoljno da se odgovori samo uopšteno. Sa druge strane stranka ne može samo paušalno da tvrdi da je mišljenje

nestručno ili da je nalaz nepotpun ili da je vještak pristrasan. Treba imati i u vidu da će se vještak pozvati da se neposredno izjasni ali samo ukoliko stranke stave određene, kvalitetne primjedbe, a ne i onda kada se ocijeni da to vodi samo prolongiranju postupka. Prilikom ocjene nalaza i mišljenja sud treba da vodi računa i o tome da li je rješenje o vještačenju – naredba, bila potpuno jasna, da li je sadržala određen i precizan zahtjev.

12.3. Treba imati u vidu i odnos suda prema priznanju okrivljenog koji je definisan Zakonikom o krivičnom postupku. U praksi će se rijetko desiti da okrivljeni sveobuhvatno prizna izvršenje krivičnog djela, već to priznanje obično prate i izvjesne rezerve i ograde, radnja izvršenja krivičnog djela koja mu je stavljena na teret se opisuje drugačije od načina kako je to opisano u optužnom aktu, a u ovim predmetima i samo neznatno drugačije opisan način izvršenja može uveliko stvoriti probleme za dokazivanje navoda iz optužnog akta.

Sve odredbe koje se tiču pretresanja stana i lica, privremenom oduzimanju predmeta i postupanje sa sumnjivim stvarima, moraju biti ispoštovana obzirom da će se u izvjesnom broju predmeta to pojaviti kao žalbeni navod. Ranije je već detaljno opisano postupanje prilikom primjene ovih odredbi ZKP-a. Okrivljeni može osporavanjem zakonitosti tih procesnih radnji osporiti i dokaze pribavljene tom procesnom radnjom, o čemu treba voditi računa.

Dokazi kojima se zadire u privatnost a koji se u krivičnom postupku izvode, će često biti osporavani. Takvi dokazi pribavljeni putem primjena mjera tajnog nadzora cijene se kao i svi drugi dokazi u postupku. Postaviće se pitanje tehničke ispravnosti i korektnosti samog snimka, šta je garancija da na snimku nije bilo intervencija, da nije bilo montiranja, da nije bilo dodavanja ili "uklapanja" izgovorenih riječi, osporavaće se da je na audio zapisu upravo glas okrivljenog. Upravo je u tom dijelu važna uloga vještaka radi utvrđivanja da li se na snimku nalazi glas lica za koga se tvrdi da je njegov glas.

Treba imati u vidu da se glas može vještačiti, u takvim situacijama će se uzimati i snimati glas okrivljenog lica kao nesporan uzorak, ali se može pojaviti problem da okrivljeni odbija da govori. Tehničke mogućnosti pojedinih sudnica omogućavaju snimanje kompletnog pretresa, pa se na taj način može doći do nespornog snimka glasa okrivljenog. Tokom vještačenja se radi akustička analiza kvaliteta glasa, fonetsko-lingvistička analiza, računarska analiza glasa, komparativna analiza nespornog uzorka, analiza spornog uzorka i poređenje sa nespornim a zatim se utvrđuje stepen pouzdanosti prema klasifikaciji IAI (International Association of Identification) koja ima 11 nivoa. (*Stim u vezi korisno je pomenuti i presudu Evrpskog suda za ljudska prava broj 44787/8 (PGJH protiv Ujedinjenog kraljevstva od 25.09.2001. godine, gdje sud vezano sa predstavku povrede prava na pravično suđenje zbog priba-*

vljanja nespornog glasa osumnjičenih putem prikrivenog isljednika u zatvorskoj ćeliji, zaključuje da snimljeni dokazi nijesu bili jedini dokazni materijali protiv okrivljenih, te da su okrivljeni imali mogućnost osporavanja autentičnosti i upotrebe tih snimaka, a postupajući sud i mogućnost da isključi takav dokaz ukoliko bi ustanovio da bi njegovo prihvatanje dovelo do značajne nepravičnosti).

12.4. U vezi sa već pominjanom odredbom člana 21 Konvencije koja se bavi takozvanim presretanjem podataka, uglavnom će se postaviti i pitanje povrede prava na privatnost kao i prava na prepisku. Ovdje je značajno reći da pored toga što postoje garancije u međunarodnim dokumentima o ljudskim pravima i slobodama, dozvoljava se da postoji mogućnost da dođe do zloupotrebe ovlašćenja državnih organa, ali i situacija kada do takve zloupotrebe nije došlo, ali se odbrana poziva da jeste. Osporavaće se i sloboda na izražavanje odnosno dosegnuti standardi u razvijenim demokratskim zemljama.

Razvoj računarske tehnologije omogućava brzi protok elektronskih podataka, ali se stim u vezi pojavljuje i problem u takozvanom prekograničnom protoku informacija. Stoga je važno pomenuti i postojanje Konvencije o zaštiti prava pojedinca u vezi sa automatskom obradom ličnih podataka. Treba skrenuti pažnju i na činjenicu da je u današnje vrijeme ostvarivanje prava pojedinaca sve češće podrazumijeva i prikupljanje i čuvanje podataka lične prirode, pa tako u okviru medicinske zaštite – podaci o zdravstvenom stanju pojedinaca. Stoga je se kao izvršioci pojedinih krivičnih djela iz ove oblasti mogu javiti lica koja imaju pristup ovim informacijama i krivičnim postupkom treba onemogućiti bilo kakvu zloupotrebu tako pribavljenih podataka.

Branioci će se i pozivati na član 8 Evropske konvencije o zaštiti ljudskih prava i osnovanih sloboda kojim je propisano da svako ima pravo na poštovanje svog privatnog života i korespedencije, te da se državni organi i druga javna tijela mogu umiješati u korišćenje ovog prava samo u skladu sa zakonom i kada je to neophodno radi očuvanja interesa nacionalne ili javne bezbjednosti, radi sprječavanja nereda ili zločina ili radi zaštite prava i sloboda drugih lica. Direktiva 2006/24/EU Evropskog parlamenta i Savjeta ili Direktiva o čuvanju podataka sadrži i kategorizaciju podataka koji se čuvaju. To su uglavnom podaci potrebni za pronalaženje identifikacije izvora komunikacije, dakle podaci o prometu i lokaciji pravnih i fizičkih lica i podatke koji su vezani za identifikaciju pretplatnika ili registrovanog korisnika ali ne i na podatke u pogledu sadržaja elektronske komunikacije kao ni na informacije do kojih se dolazi korišćenjem mreže elektronske komunikacije.

U krivičnim postupcima, što se tiče fiksne i mobilne telefonije pribaviće se, po potrebi, podaci kao što su telefonski broj priključka sa kojeg poziv dolazi, ime i adresa registrovanog korisnika ili pretplatnika, podaci o dodije-

ljenom korisničkom imenu vezano za pristup internetu, odnosno elektronskoj pošti ili internet telefoniji, korisničko ime i telefonski broj dodijeljen komunikaciji kojom se stupa u javnu telefonsku mrežu, te ime i prezime, ime i adresa pretplatnika ili registrovanog korisnika kome je u trenutku komunikacije dodijeljena adresa internet protokola, korisničko ime, telefonski broj, podaci potrebni za otkrivanje odredišta komunikacije kao što su u slučaju elektronske pošte internet telefonije, korisničko ime i telefonski broj primaoca, kome je namijenjen poziv preko internet telefonije – skype, ime i prezime pretplatnika ili registrovanog korisnika i korisničko ime primaoca prema kome je komunikacija usmjerena.

Treba ipak obratiti pažnju da na ovakav način dobijeni sačuvani podaci treba da sadrže datum, vrijeme i trajanje komunikacije i u tom smislu dakle datum i vrijeme prijave i odjave pristupa internetu prema određenoj vremenskoj zoni, IP adresa, kako statička tako i dinamička, koju je u komunikaciji dodijelio davalac usluga pristupa internetu, korisničko ime pretplatnika i registrovanog korisnika, datum i vrijeme prijave i odjave od usluge elektronske pošte ili internet telefonije opet prema određenoj vremenskoj zoni. *(Kao izvori elektronskih dokaza mogu se, pored već pomenutih računara i mobilnih telefona, pojaviti i skeneri, štampači, telefonske „sekretarice", digitalni fotoaparati, kamere, fax aparati, fotokopir aparati, GPS uređaji, digitalni časovnici)*. Ovo može imati odlučan značaj za potvrđivanje ili opovrgavanje odbrane okrivljenog u pogledu vremena izvršenja krivičnog djela, njegovog prisustva na mjestu gde se nalazio računar, i sl.

Može se utvrditi identifikacija komunikacijske opreme korisnika, prilikom komunikacije putem mreže mobilne telefonije čuvaju se telefonski brojevi sa kojih se poziva, brojevi koji se pozivaju, međunarodni identitet mobilnog pretplatnika koja poziva i koja prima poziv, međunarodni identitet mobilnog uređaja (IMEI *International Mobile Station Equipment Identity*) stranke koje poziva i prima poziv, u slučaju pripejd korisnika datum i vrijeme početka upotrebe usluge i lokacijska oznaka – identitet bazne stanice sa koje je usluga aktivirana. Što se tiče interneta čuvaju se podaci o telefonskom broju sa kojeg se poziva u svrhu telefonskog pristupa, dial up pristupa ili digitalna pretplatnička linija ADSL ili druga krajnja tačka lica koje započinje komunikaciju. U pogledu fiksne ili mobilne telefonije veliki broj sudija se u svojim predmetima već susretao sa takvim listinzima, pa se time nećemo dublje baviti.

Ponekad će se kao jedna od specifičnosti za krivična djela računarskog kriminala uočiti sa jedne strane, da je za izvršioca potrebno specifično znanje i iskustvo u oblasti informacionih tehnologija, o čemu smo već govorili, ali sa druge strane, vrlo često će se raditi o licima koja nemaju visoko obrazovanje ili koja su toliko mlada da su po prirodi stvari završili srednju školu, pa čak i lica koja imaju samo osnovnu školu. Pri tome se primjećuje da ta lica bez izuetka, konstantno prate razvoj tehnologije i za koje nema tajni u

oblasti telekomunikacionih tehnologija.

Kada se bavimo problemima koji mogu da proisteknu iz postupka pronalaženja i analize sadržaja uskladištenog ili memorisanog u oduzetim predmetima, mora se podsjetiti da su između ostalih, osnovna ljudska prava, pravo na nepovredivost stana i pravo na tajnost komunikacija.

Nesumnjivo, krivični postupak u odnosu na krivična djela kojim se bavi ovaj Priručnik, ponekad duboko zadire u privatnost lica protiv kojeg se vodi postupak ali ne samo njega već i lica sa kojima je on/ona komunicirao putem elektronske pošte, putem drugih servisa, Facebook i sl. Dokazi se nalaze u memoriji računara računarskih mreža ili drugih uređaja u kojima se pored onih činjenica koje su bitne za dokazivanje u pojedinom krivičnom postupku često dolazi i do podataka i informacija koje nijesu u vezi sa predmetnim krivičnim djelom koje se otkriva.

Važno je reći da postoji i zauzet stav da ukoliko neko svojom voljom učini dostupnim neke svoje lične podatke ili podatke tajne prirode ne može se kasnije pozivati na to da mu je povrijeđena privatnost.Ukoliko se u toku vođenja postupka dođe do takvih podataka, naravno ne treba uopšte smetnuti sa uma obavezu čuvanja prikupljenih podataka kao službene tajne. Bitno je voditi računa i o otklanjanju mogućnosti da je neko drugo lice a ne okrivljeni koristio predmetni oduzeti računar, a iznad svega važan je princip provjerljivosti odnosno nezavisnom potvrđivanju. Dokazi moraju biti takvi da mogu biti provjerljivi od strane drugog vještaka ili nezavisne ekspertske institucije.

Važno je imati na umu da je garant zakonitog postupanja princip upravo sudske kontrole. Sud će voditi računa o svim radnjama dokazivanja i njihovoj zakonitošću, kako u pogledu pretresanja stana i lica, ovlašćenja za privremeno oduzimanje predmeta, radnji uviđaja i rekonstrukcije, vještačenju, traženoj i pruženoj međunarodnoj pravnoj pomoći.

Odredba koja propisuje da se sudska odluka ne može zasnivati na dokazima koji su pribavljeni povredama ljudskih prava i osnovnih sloboda zajemčenih Ustavom ili potvrđenim međunarodnim ugovorima, ili na dokazima koji su pribavljeni povredama odredaba krivičnog postupka, kao i drugim dokazima za koje se iz njih saznalo, niti se takvi dokazi mogu koristiti u postupku, će sigurno biti veoma često sadržana u žalbama na odluke prvostepenih sudova.

Međutim, prema slovu ZKP sud i državni tužilac postojanje ili nepostojanje činjenica, na kojima zasniva odluku, cijeni po svom slobodnom uvjerenju. Da bi se ono pravilno formiralo neophodno je imati određeni stepen poznavanja ove materije, čemu bi prema početnoj ideji, ovaj Priručnik i u dijelu koji se odnosi na glavni pretres i drugostepeni postupak, morao da pruži izvjestan doprinos.

XII RAČUNARSKI IZRAZI

Aplikativni softver (Application software)
Predstavlja opšti naziv za računarske programe kao što su za računovodstvo, obradu teksta, finansijske analize, kompjuterske igrice, itd.

Bekap (Backup)
Pravljenja kopije podataka uskladištenih na disk ili drugi uređaj za skladištenje, za zaštitu od gubitka podataka ako postoji oštećenje na primarnoj kopiji.

Bejzik (BASIC)
Programski jezik opšte namjene, često se koristi u računarima.

Baud Rate (Baud Rate)
Mjerenje brzine kojom se podaci prenose između dva računara, broj signala u sekundi koji se prenose.

Bajt (Byte)
Grupa od osam bitova, tj. znakova koji mogu biti nule (0) i jedinice (1), kojim se na osnovnom programskom nivou bilježe podaci.

Katodna cijev (CRT - Catode Relay Tube)
Drugi termin za računarski ekran - monitor.

CD-ROM medijum i jedinica (CD-ROM)
Mali disk ili uređaj na koji ili pomoću koga se može uskladi štit i velika količina podataka.

Centralna procesorska jedinica (CPU)
Dio računara koji se nalazi na matičnoj ploči i koji služi za matematičku logičku i aritmetičku obradu podataka.

Čip (Chip)
Zajednički termin za male silikonske pločice na kojima su odštampana elektronska kola. Koristi se za izradu mikroprocesora, elektronske memorije i drugih kompjuterskih internih elektronskih komponenti.

Komunikacioni program (Communication Software)
Kompjuterski program koji sadrži instrukcije koje omogućavaju računaru da šalje podatke kao i da i prima u podatke sa drugog računara.

Kursor (Cursor block)
Grafički simbol na ekranu – monitoru kojim se ukazuje ili pokreće određena aplikacija.

Sistem za upravljanje bazama podataka (DBMS)
Računarski program koji omogućava da podaci se pohranjuju na organizovani i unaprijed logički predviđen način radi kasnije upotrebe.

Demonstracioni program (Demo program)
Nepotpuna verzija programa koja se koristi za demonstraciju karakteristika i mogućnosti kompletnog programa. Često se besplatno daje potencijalnim kupcima, ili prodaje po niskoj cijeni.

Dokumentacija (Documentation)
Štampano uputstvo za rad koje prati računar ili softver.

Eternet (Ethernet)
Vrsta mrežne interfejs kartice koja povezuje individualni računar sa mrežom. Računari na Internetu koji koriste TCP / IP protokole su često povezani sa Internetom preko Eternet linka.

Faksmodem (Fax modem)
Uređaj za povezivanje računara na telefonsku liniju za slanje faks poruke.

Fajl (File)
Zbir povezanih bajtova podataka koji postoje na uređaju za skladištenje podataka i koji čine logičku i informatičku cjelinu određene namjene.

Harddisk (Hard Disk - Hard Drive)
Uređaj za skladištenje velike količine podataka koji može biti interni (u računaru) ili eksterni (van računara, povezan sa istim preko određene kablovske ili druge veze)

Hardver (Hardware)
Fizički djelovi računara.

Ink – džet štampač (Ink-jet printer)
Računarski dodatni uređaj koji štampa na raznim vrstama papira koristeći tehnologiju otiska zagrejanog voska u monohromatskom ili kolornom opsegu.

Kilobajt (Kb - Kilobyte)
Jedinica za mjerenje memorije računara i skladišnih kapaciteta, otprilike jednaka 1.000 znakova ili bajtova podataka. Jedan Kilobajt sadrži 1024 bajtova.

Laserski štampač (Laser printer)
Računarski dodatni uređaj koji štampa na raznim vrstama papira koristeći tehnologiju otiska grafitnog praha pod uticajem laserskih zrakova u monohromatskom ili kolornom opsegu.

LCDmonitori (LCD - Liquid Crystal Display)
Ekrani za prikaz slike koju generiše računar, visokog kvaliteta.

Intranet (Intranet)
Lokalna mreža

Megabajt (Megabyte)
1024 Kilobajta

RAM Memorija (RAM Memory)
Termin se obično odnosi na elektronska memorijska kola u obliku pravougaonih pločica koje se postavljaju u posebne za to određene slotove, tj. Mjesta na matičnoj ploči računara, i služe za privremeno brzo skladištenje podataka koji se izvršavaju.

Meni lista (Menu list)
Sastavni dio programa u grafičkom obliku koji pruža izbor odabira određene opcije programa za dalje izvršavanje.

Modem (Modem)
Zastarjeli uređaj koji omogućava povezivanje računara i njihovu komunikaciju i razmjenu informacija sa drugim računarima putem telefonske linije. Moguća je podjela na „interne", tj. priključene na matičnu ploču računara ili eksterne u posebnim kućištima koja stoje pored računara.

Kablovski modem (Cable modem)
Moderan uređaj za međusobno povezivanje računara kao i korišćenje Interneta koji koristi koaksijalne ili optičke kablove, najčešće postavljene od strane Internet servis provajdera ili preduzeća za kablovsku televiziju.

Operativni sistem (Operation System)
Program koji služi za upravljanje svim djelovima sistema, uključujući kako hardver tako i softver. Najpoznatiji su „MS Windows", Linux kerneli kao što su "Ubuntu", "Red Hat", "Fedora" itd., IOS, BSD i drugi.

PCMCI (PCMCI)
Specifični format fizičke kartice za povezivanje računara i računarskih uređaja. Najviše se koristi kod mobilnih računarskih platformi.

Periferije
Dodatni hardverski uređaji koji se koriste u kombinaciji sa računarom kao što su štampač, monitor, razne vrste diskova, čitača, skeneri itd.

ROM memorija (ROM)
Memorijski uređaj (obično elektronsko memorijsko kolo) koji može biti pročitan od strane računara. Za razliku od RAM memorije, podaci smješteni u ROM memoriju su stalna (non-volatile) i ne gube se, tj. ne brišu se kada je računar isključen. Ipak, postoji način da se i sadržaj ROM memorije izbriše ili „resetuje".

Zaštitnik napona struje (Surge Protector)
Elektronski uređaj za zaštitu računara ili drugih povezanih elektronskih uređaja od štetnog dejstva oštrih promjena i napona u električnoj mreži.

Uslužni softver
Razni računarski programi za rukovanje i organizaciju podataka na računaru kao I održavanju istih, koji smanjuju potrebu za direktnom kontrolom od strane korisnika raznih procesa koji se obavljaju na računaru, kao što su brisanje datoteka starih podataka, kopiranje diskova, štampa direktorijum informacije sačuvane na disku, itd.

VAN (Wide Area Network)
Mreža računara i računarskih sistema koja obuhvata šire prostorno ili geografsko okruženje.

Obrada teksta (DTP - Desk Top Publishing)
Upotreba računara i programa za unošenje, obradu i štampanje teksta.

Internet adresa (IP adress)
Individualizovana slovna ili brojčana oznaka identifikacije računara korisnika koja se koristi u mrežnim komunikacijama radi prenosa poruke za odredjenju osobu ili računar.
‚Internetprotokol' adresa računara se sastoji iz četiri ili osam grupa elektronskih serijskih brojeva.
IP adresa može izgledati kao, "202.3.104.55" ili kao "21:DA:D3:02:F3:B2" "AA:FF:FE:28:9C:5A„ zajedno sa tačkom ili separatoram.
Svaki računar, mobilni telefon i uređaj koji pristupa Internetu je dobio najmanje jednu IP adresu za svrhu praćenja. Gdje god da pretražujete, kad god poslali e-mail ili instant poruke i kad god ste preuzeli neki fajl, vaša IP adresa se ponaša kao identifikacija uređaja koji je koristi.

Veb čitač (Browser)
Računarski program koji može biti isporučen uz operativni sistem ili samostalno preuzet radi pretraživanja (surfovanja) Internet sadržaja.

Keš memorija (Cache)
Mašinski ili programski adresiran (odredjen) prostor najčešće na hard disku, ponekad i na drugim jedinicama za odlaganje podataka, gdje se privremeno upisuju podaci koji se često koriste ili ponavljaju od strane programa koji je trenutno u upotrebi radi brzog pristupa bez pretrage.

Čet soba (chat room *или* chatline)
IRC (Internet Relay Chat) programski određena funkcija koja omogućava korisnicima koji imaju instaliran program i koji koriste Internet da se virtuelno „okupe" u „sobama", tj. posebnim privremenim programskim okruženjima u kojima mogu putem tekstualnog unosa i prikaza na ekranu računara, komunicirati sa drugim osobama u realnom vremenu.

Kolačić - kuki (COOKIE)
Manji tekstualni fajl koji se automatski preuzima i skladišti u računaru, najčešće prilikom upotrebe Interneta i brauzera, i koji omogućava indeksiranje ili omogućavanje prava pristupa korisnika odredjenim sadržajima na Internetu.

Domen sistemsko ime (DNS - Domain Name System)
Jedinstvena identifikacija grupe računara koji koriste isti mrežni (DNS IP) opseg na internim ili eksternim mrežama, i koji po određenom pravilu pripada nad-korisniku (kompaniji, instituciji, udruženju itd.).

"Skidanje sadržaja" (Download)
Postepeno preuzimanje djelova programa putem učitavanja pojedinačnih paketa korišćenjem HTTP protokola, koji nakon preuzimanja formira jedinstveni program tj. datoteku, koji je spreman za dalju upotrebu.

ISDN (Integrated Services Digital Network) i ADSL (Asymmetric Digital Subscriber Line) konekcija
Tehničke mogućnosti korišćenja većeg i bržeg protoka podatka putem telefonskih linija.

Elektronska pošta (e-mail)
Program koji omogućava slanje poruka između računara putem POP3 i SMTP programskih rutina. E-mail predstavlja elektronsku poštu u najširem smislu tih riječi. E-mail se obično dijeli na takozvane "web mailove" (npr. Gmail ili Yahoo), ili mailove koji koriste takozvane"mail servere" upotrebom određenih softverskih paketa.

Kompresija fajlova
Programski proces koji korišćenjem specifičnih matematičkih algoritama smanjuje fizički prostor koji određeni fajl tj. program zauzima u jedinici za skladištenje.

Finger program
Program koji se koristi da bi se provjerilo nečije prisustvo na računarskoj mreži. Takođe se može iskoristiti za otkrivanje punog naziva fajla.

Fajervol - vatreni zid (Firewall)
Program čija je primarna namjena odbrana računara ili računarskog sistema od neželjenih i nedozvoljenih provjera i upada. Može biti programski tj. softverski, ili fizički, tj. kao poseban uređaj koji je priključen na računar ili računarsku mrežu koju štiti.

Flejming (Flaming)
Društveni fenomen na Internetu koji predstavlja svojevrsnu zloupotrebu komunikacionih mogućnosti putem vređanja ili omalovažavanja drugih korisnika.

Friver (Freeware)
Računarski programi koji su po pravilu besplatni za upotrebu.

FTP transfer podataka (FTP - File Transfer Protocol)
Računarski protok podataka između računara ili mreža kojim se, po pravilu, prenose veće količine podataka.

Fotografija u .gif formatu (GIF)
Pored JPG formata, najčešći programski format za prikazivanje grafičkog sadržaja na Internetu.

Početna strana (Home Page)
Naslovna, tj. uvodna stranica web prezentacije na Internetu koja vodi ka daljim sadržajima same prezentacije ili drugim prezentacijama putem Internet veza, tzv."hajper linkova".

HTML (Hyper Text Markup Langauge)
Računarski programski jezik koji se koristi za kreiranje takozvanih "hajpertekst" dokumenata, koji se dalje koriste za kreiranje Internet prezentacija.

HTTP protokol (Hyper Text Tranfser Protocol)
Programski jezik - protokol, na osnovu koga funkcioniše protok podataka na Internetu.

Link
Hajpertekst veza koju je moguće "kliknuti" u okviru jednog dokumenta, tj. prezentacije, i koja radnja će dovesti do preusmjeravanja na drugi sadržaj.

Internet
Globalna računarska mreža zasnovana na TCP/IP protokolu.

Internet provajderi (ISP)
Komercijalni ili nekomercijalni entiteti - preduzeća koji omogućavaju pristup Internetu i/ili nekim servisima koji su bazirani na Internet tehnologijama.

Prijava na sistem (Log in)
Proces identifikacije i prijave početka rada na računaru ili određenom Internet servisu. Uobičajeni važeći uslovi su korisničko ime i lozinka.

Odjava sa sistema (Log off)
Postupak odjavljivanja tj. prekidanja rada sa određenim programom ili na odeđenom računaru.

Elektronska mailing lista
Diskusione grupe koje su povezane sa relativno malom grupom korisnika u okviru određenog zajedničkog interesa.

Multimedija
Dokumenti ili platforme koje kombinuju različite vrste podataka (tekst, video, grafika, audio).

Njuzgroup (Newsgroup)
Grupa korisnika koja je okupljena radi kreiranja i praćenja vijesti u određenoj oblasti.

Onlajn (On-line)
Označava prisustnost na mreži, aktivnost računara i programa sa drugim računarima ili programima. Najčešće označava aktivnost na Internetu.

PDF fajl (PDF file - Portabl Document File)
Standardni tekstualni fajl koji se koristi na Internetu i predstavlja rezultat rada kompanije "Adobe". U osnovnom obliku je besplatan i pristupačan svima. Napredne opcije se naplaćuju.

Politika privatnosti (Privacy Policy)
Skup pravila koje primjenjuju web sajtovi i kojima se opisuju informacije koje mogu biti ili jesu prikupljenje o korisniku usluge. Po pravilu politika privatnosti mora obuhvatati mogućnost izbora tj. prihvatanja određenih zahtjeva ili ne.

Skripta (Script)
Manji računarski program koji služi za automatizaciju određenih rutina tj. komandi koje se ponavljaju.

Spam
Opšta oznaka za sav neželjeni sadržaj koji se bez znanja i volje korisnika upućuje na njegov računar. Obuhvata neželjenu poštu, reklame, lažne proizvode, promocije itd.

Telnet program, telnetovanje.
Program koji omogućava jednom korisniku da se prijavi za rad na udaljenom računaru i da ga stavi pod svoju dozvoljenu ili nedozvoljenu kontrolu.

Aplоad (Upload)
Slanje fajla tj. podataka sa sopstvenog računara na drugi računar ili računarski sistem.

URL adresa (Universal Resource Locator)
Adresa prezentacije ili stranice prezentacije na Internetu.

Virus
Program ili dio programskog koda koji se instalira tj. ubacuje u drugi program radi izazivanja neočekivane i obično nepoželjne posljedice, kao što su brisanje ili oštećenje fajlova.

Veb server
Računar koji je povezan na Internet radi skladištenja i upravljanja Internet dokumentima. Veb server obrađuje zahtjeve od drugih računara i isporučuje tražene dokumente.

Sajt
Grupe povezanih stranica, slika i datoteka na Veb server.

Web (www)
Jedna od nekoliko karakteristika Interneta. Predstavlja u svojoj ukupnosti svu povezanost svih računarskih i programskih resursa na Internetu i šire. Internet je ogromna "interkonekcija računarskih mreža" koja obuhvata cijelu planetu. Ona se sastoji od miliona računarskih uređaja koji razmjenjuju velike količine informacija. Desktop računari, mejnfrejm računari, GPS jedinice, mobilni telefoni, auto alarmi, video igre, konzole, pa čak i kućni aparati jesu ili mogu biti povezani putem veba na Internet.
Internet je počeo u kasnim 1960-im, kao američki vojni projekat, da bi od tada evaluirao u masovni i javni Veb. Nijedna organizacija ne posjeduje, niti može reći da kontoliše Internet.
Internet sadrži više slojeva informacija, gdje je svakom sloju posvećena različita dokumentacija. Ovi različiti slojevi se nazivaju „protokoli". Najpopularniji protokoli su www, FTP, Talent, Gopherspace, instant poruke, e-mail i sl Najpopularniji veb brauzeri u 2013. godini, su bili: Google Chrome, Firefox, Internet Explorer и Safari.

Blogovi i bloging
Blog predstavlja kolumnu tzv. „modernih online pisaca". Amaterski i profesionalni pisci objavljuju svoje blogove u vezi bilo koje potencijalno interesantne teme: njihovog hobija, interesa, njihovih mišljenja o zdravstvenoj zaštiti, foto blogova omiljenih slika, tehnoloških savjeta o korišćenju raznih programa ili uređaja i sl.
Apsulutno svako može pokrenuti blog, a neki ljudi mogu postići razumne prihode od prodaje reklame na svojoj blog stranici. Blogovi se razlikuju u kvalitetu, od vrlo amaterskih do veoma profesionalnih. Započinjanje bloga je besplatno.

Društveni mediji
Predstavljaju širok pojam za bilo koji online alat koji omogućava korisnicima da komuniciraju sa hiljadama drugih korisnika. Instant poruke i ćaskanje su česti oblici društvenih medija, kao što su blogovi sa komentarima, diskusioni forumi, video šering i razmjena fotografija itd. Facebook, Instagram, Twitter i sl. su primjeri savremenih društvenih medija.

Social Bookmarking
Social Bookmarking je specifičan oblik društvenih medija. Social Bookmarking predstavlja mjesta gdje korisnici komuniciraju, preporučujući sajtove jedni drugima („označavanje lokacije")

Daunload (Download)
Označava preuzimanje raznih sadržaja sa interneta i opisuje način pravljenja lične kopije određenog sadržaja koji ste pronašli na Internetu ili Vorld Vide Veb.

Malver (Malware)
Malver je širok pojam koji opisuje bilo koji zlonamjerni softver dizajniran od strane hakera. Malver obuhvata: viruse, trojance, kilogere, retverove, zombi programe i bilo koji drugi softver koji ima za cilj da postigne:

- ometanje računara
- krađu informacija
- preuzimanje kontrole nad računarom
- u druge svrhe radi manipulacije

Malver programi mogu predstavljati tzv. tempirane bombe.

Ruter (Router)
Ruter, ili u mnogim slučajevima ruter-modem kombinacija, je hardverski uređaj koji služi za usmjeravanje mrežnih signala. Ruter može služiti za žičnu ili bezžičnu vezu, kao i za obje.

Ključne riječi i oznake (Bookmarks)
Ključne riječi su termini za pretragu koje se koriste za pronalaženje dokumenata. Ključne riječi su osnova za katalogizaciju Veba.

Teksting/Ćaskanje
Teksting je kratak način da se prenese „tekst poruka", tj. slanje kratkih elektronskih bilješki obično putem mobilnog telefona ili ručnog elektronskog uređaja. Teksting je popularan među mlađom populacijom koja koristi mobilne uređaje češće nego standardne računare.
U 2010, unos teksta je izazvao kontroverznu naviku pod nazivom"Seksting", koji predstavlja slučajeve kada mladi ljudi šalju seksualno eksplicitne fotografije drugim korisnicima mobilnih telefona.

I. M. (Instsant messaging)
IM predstavlja slanje i primanje instant poruka, najčešće bez naknade, kao oblik savremenog komuniciranja putem Interneta.
Trenutno najpopularniji programi za ovu vrstu komunikacije su "Whatsapp", "Vine", "BBM" i sl.

P2P (Peer to peer)
P2P fajl šering, tj. dijeljenje, predstavlja direktnu razmjenu fajlova između dva i više računara.

E-trgovina (e-commerce)
E-trgovina predstavlja transakcije u svrhu prodaje i kupovine dobara na mreži.

Socijalni inžinjering (Social engineering)
Proces prikupljanja podataka o određenoj osobi na osnovu raspoloživih informacija na Internetu u okviru različitih servisa, socijalnih grupa i medija itd.

Trojanac
Trojanac prestavlja vrstu malvera koji se oslanja na korisničku radnju u cilju aktiviranja. Trojanci su projektovani da na programskom nivou maskiraju kao legitiman fajl ili softverski program. Ponekad će izgledati bezazleno kao muzički ili filmski fajl, ili instaler koji pretenduje da bude iskorišćen upravo za borbu protiv virusa.

Cloud computing и softver
Klaud kompjuting je termin koji opisuje način korišćenja računarskih programa na Internetu, za razliku od standardnog načina korišćenja putem instaliranja na računaru.
Veb bazirani servisi elektronske pošte su najčešći primjeri ovog savremenog načina pohranjivanja i korišćenja podataka.

Apps-apleti
Aplikacije i apleti su softverske aplikacije koje su dizajnirane da budu mnogo manje od redovnog računarskog softvera, ali i dalje pružaju veoma korisne funkcije. U posljednje vrijeme aplikacije su veoma popularne na mobilnim telefonima i mobilnim platformama.

Šifrovanje i autentifikacija
Šifrovanje je matematičko kodiranje podataka. Šifrovanje koristi složene matematičke formule-algoritmove.
Autentifikacija je u direktnoj vezi sa šifrovanjem. Autentifikacija je složen način da računarski sistemi potvrde svoj mašinski identitet.

Portovi i Port Forvarding
Svaki računar na programskom i operativnom nivou ima 65.536 portova, preko kojih se razmjenjuju podaci.

LITERATURA

- *Konvencija o visokotehnološkom kriminalu Savjeta Evrope (CETS 185)*
- *Dodatni protokol na Konvenciju o visokotehnološkom kriminalu Savjeta Evrope o sprječavanju krivičnih djela rasizma i ksenofobije*
- *Eksplanatorni izvještaj uz Konvenciju o visokotehnološkom kriminalu*
- *Direktiva Savjeta Ministara Evropske Unije 2013/40/EU*
- *Zakon o autorskim i srodnim pravima. (Službeni list Crne Gore br. 37/2011)*
- *Zakon o patentima (Službeni list Crne Gore br. 66/08, 40/10, 40/2011)*
- *Mr Snežana Šaboh "Zaštita softvera patentima – regulative i iskustva SAD-a i zemalja Evropske unije" www.singipedija.com maj 2011 godina*
- *Doc. dr Adis Balota "Zakonska zaštita softvera pravima intelektualne svojine" Časopis udruženja sudskih vještaka Crne Gore - Expertus forensic. Broj 21, oktobar 2013. godina Podgoprica*
- *Džodi R. Vestbi "Međunarodni vodič za borbu protiv kompjuterskog kriminala" Američka advokatska komora, Čikago, USA.*
- *http://www.fbi. gov/hq/cid/fc/ec/about/about_scf. htm*
- *Strategija sajber bezbjednosti 2013-2017 Crne Gore http://www.gov. me/biblioteka/strategije*
- *Arhiva Posebnog tužilaštva za visokotehnološki kriminal Srbije*
- *Konvencija o zaštiti djece protiv seksualne eksploatacije i seksualnog zlostavljanja (CET 201)*
- *Okvirna odluka Savjeta Evrope 2005/222*
- *Okvirna odluka Savjeta Evrope 32000D375*
- *Regionalna deklaracija o strateškim prioritetima u borbi protiv visokotehnološkog kriminala*
- *"IT forensic" Nigel Jones Great Britain*
- *Jakša Backović, specijalistički rad "Itraživački alati u mrežnoj forenzici"*
- *www.epo.org*
- *www.wipo.int*
- *www.first.org*
- *www.europa.eu.int*
- *www.cirt.me*


9 789940 500153