УДРУЖЕЊЕ ЈАВНИХ ТУЖИЛАЦА И
ЗАМЕНИКА ЈАВНИХ ТУЖИЛАЦА СРБИЈЕ

PRIRUČNIK ZA TRENING TUŽILACA I SUDIJA U OBLASTI VISOKOTEHNOLOŠKOG KRIMINALA

aecid

PRIRUČNIK ZA TRENING TUŽILACA I SUDIJA U OBLASTI VISOKOTEHNOLOŠKOG KRIMINALA

Izdavač:
Udruženje javnih tužilaca i
zamenika javnih tužilaca Srbije

Lektura i korektura:
Vesna Komar

Tehničko uređenje:
Siniša Lekić

Štampa:
ATC, Beograd

Tiraž:
2300

PRIRUČNIK ZA TRENING TUŽILACA I SUDIJA U OBLASTI VISOKOTEHNOLOŠKOG KRIMINALA

УДРУЖЕЊЕ ЈАВНИХ ТУЖИЛАЦА
И ЗАМЕНИКА ЈАВНИХ ТУЖИЛАЦА СРБИЈЕ

Curriculum za obuku sudija, tužilaca i pripadnika policije iz oblasti visokotehnološkog kriminala

Opšti cilj:

Obezbediti da sudije, javni tužioci i pripadnici policije steknu neophodna znanja i veštine za efikasnu primenu mera borbe protiv visokotehnološkog kriminala (VTK).

Posebni ciljevi:

– pružiti učesnicima obuke osnovne informacije o pojmu visokotehnološkog kriminala i pojmovno ga razgraničiti;

– obučiti pripadnike pravosudnih organa i policije da razlikuju krivična dela iz oblasti visokotehnološkog kriminala, međusobno i sa delima iz drugih vrsta kriminala;

– upoznati učesnike obuke sa kategorijama i pojavnim oblicima visokotehnološkog kriminala;

– upoznati učesnike sa domaćim pravnim i institucionalnim okvirom za borbu protiv visokotehnološkog kriminala;

– upoznati učesnike sa pojavnim oblicima, statistikama i trendovima visokotehnološkog kriminala u Srbiji i u drugim zemljama i napraviti poređenje;

– približiti učesnicima značaj međunarodnih instrumenata i odnosa ljudskih prava sa visokotehnološkim kriminalom i u sklopu gonjenja za krivična dela iz oblasti visokotehnološkog kriminala.

Metode:

Prezentacija prilikom upoznavanja učesnika obuke sa novim informacijama; rad po grupama – radioničarski rad i studije slučaja kada je potrebno produbljivanje postojećih znanja i analiza određenog problema sa više aspekata.

Sredstva:

ppt prezentacija, projektor, flipchart.

Trajanje:

dva dana.

PRVI DAN

1. Pojam visokotehnološkog kriminala, osnovni pravni i tehnički pojmovi vezani za visokotehnološki kriminal

Svrha:

Pružiti učesnicima obuke osnovne informacije o pojmu visokotehnološkog kriminala, kao i o osnovnim pravnim i tehničkim pojmovima vezanim za visokotehnološki kriminal.

Sadržaj:

– pojam i definicija visokotehnološkog kriminala,
– pojmovno razgraničenje od drugih vrsta kriminala,
– osnovni pravni i tehnički pojmovi vezani za visokotehnološki kriminal,
– odnos sa drugim vrstama kriminala.

Metod:

Radionica na kojoj će učesnici na osnovu svog dosadašnjeg iskustva, kao i u odnosu na to kojoj ciljnoj grupi koja je treningom obuhvaćena pripadaju, doći do definicije pojma visokotehnološkog kriminala. Učesnici podeljeni u tri grupe odgovaraju na pitanja određivanja pojma i definicije visokotehnološkog kriminala, pojmovnog razgraničenja od drugih vrsta kriminala, osnovnih pravnih i tehničkih pojmova vezanih za visokotehnološki kriminal, kao i odnosa sa drugim vrstama kriminala. Stavove grupe učesnici prezentuju u plenumu. Radionica je posebno korisna fasilitatorima da procene nivo predznanja učesnika treninga. Nakon rada u grupi sledi diskusija u plenumu, kao i prezentacija predavača.

Sredstva:
flipchart (za grupni rad i rad u plenumu), ppt i projektor (za predavača).

Trajanje:
60 minuta.

Obrazloženje:
Pre prelaska na druge teme obuhvaćene obukom, neophodno je jasno pojmovno odrediti i razgraničiti pojam visokotehnološkog kriminala, kao i osnovne pojmove koji su za njega vezani.

2. Kategorije krivičnih dela koja se mogu smatrati delima visokotehnološkog kriminala – u užem i širem smislu; uporednopravna praksa u ovoj oblasti

Svrha:
Upoznati učesnike obuke sa kategorijama krivičnih dela koja se mogu smatrati delima visokotehnološkog kriminala.

Sadržaj:
– visokotehnološki kriminal u užem smislu, koji je prvenstveno usmeren na kompjuterske mreže i uređaje i njegovi pojavni oblici,
– visokotehnološki kriminal u širem smislu, koji samo koristi kompjuterske mreže i uređaje za činjenje krivičnih dela i njegovi pojavni oblici.

Metod:
Prezentacija o različitim kategorijama oblicima visokotehnološkog kriminala i uporednopravnoj praksi iz ove oblasti. Nakon prezentacije, učesnici podeljeni u gru-

pe učestvuju u radionici. Grupe dobijaju opise slučajeva i imaju zadatak da ih klasifikuju prema podeli koja je data tokom prezentacije. Nakon završetka rada, grupe ukratko predstavljaju svoje zadatke i nalaze, posle čega sledi diskusija.

Sredstva:
ppt prezentacija i projektor (za predavača), flipchart (za rad po grupama).

Trajanje:
60 minuta.

Obrazloženje:
Neophodno je napraviti razliku između ove dve kategorije visokotehnološkog kriminala.

3. Granični slučajevi visokotehnološkog kriminala; uočavanje obeležja koja određenim delima daju svojstvo visokotehnološkog kriminala; uporednopravna praksa u ovoj oblasti

Svrha:
Predstaviti granične slučajeve visokotehnološkog kriminala i time približiti učesnicima obuke konkretna obeležja koja određenim krivičnim delima daju svojstvo visokotehnološkog kriminala.

Sadržaj:
– ključna obeležja (karakteristike) visokotehnološkog kriminala,
– predstavljanje uporednopravne prakse u ovoj oblasti,
– predstavljanje graničnih slučajeva iz oblasti visokotehnološkog kriminala.

Metod:

U prvom delu sledi prezentacija o ključnim obeležjima ove vrste kriminala, uporednoj praksi iz ove oblasti i graničnim slučajevima iz ove oblasti. Nakon toga sledi radionica, na kojoj se učesnicima u kratkim crtama predstave slučajevi. Učesnici, uz diskusiju, imaju zadatak da odgovore i obrazlože da li konkretan slučaj spada u domen visokotehnološkog kriminala.

Sredstva:

ppt i projektor (za prezentaciju), flipchart (za radionicu).

Trajanje:

60 minuta.

Obrazloženje:

Za uspešnu borbu protiv visokotehnološkog kriminala neophodno da učesnici mogu da ovladaju sposobnošću razlikovanja da li jedno konkretno krivično delo spada u domen visokotehnološkog kriminala ili ne.

4. Domaći propisi koji regulišu borbu protiv visokotehnološkog kriminala

Svrha:

Upoznati učesnike obuke sa domaćim sistemom za borbu protiv visokotehnološkog kriminala (sa posebnim osvrtom na aktere, institucije i procedure).

Sadržaj:

– zakonodavstvo (propisi iz ove oblasti),

– institucionalni akteri u borbi protiv visokotehnološkog kriminala (sudstvo, javno tužilaštvo, policija),
– odnos institucionalnih aktera u borbi protiv visokotehnološkog kriminala.

Metod:

U prvom delu sledi prezentacija o propisima, institucionalnim akterima i odnosima između institucionalnih aktera u borbi protiv visokotehnološkog kriminala. U daljem toku se održava radionica. Učesnici su podeljeni, prema organizacijama kojima pripadaju, u grupe (sudstvo, tužilaštvo, policija) i u radionici imaju cilj da definišu najvažnije uloge druge dve grupe u borbi protiv visokotehnološkog kriminala. Na ovakav način učesnici se bolje upoznaju sa ulogama drugih aktera u ovom sistemu. Nakon rada u grupi, učesnici u plenumu predstavljaju svoje zaključke.

Sredstva:

ppt prezentacija i projektor (za predavača), flipchart (za rad po grupama).

Trajanje:

90 minuta.

Obrazloženje:

Neophodno je da učesnici obuke dobro upoznaju ne samo svoju ulogu u borbi protiv visokotehnološkog kriminala već i ulogu i značaj drugih aktera.

DRUGI DAN

1. Međunarodni instrumenti na polju borbe protiv visokotehnološkog kriminala, sa posebnim osvrtom na aktivnosti EU

Svrha:

Upoznati učesnike sa međunarodnim instrumentima i postavljenim standardima u oblasti borbe protiv visokotehnološkog kriminala, sa posebnim osvrtom na dokumente i aktivnosti EU.

Sadržaj:

– međunarodni instrumenti Saveta Evrope – Konvencija o sajber kriminalu,
– aktivnosti UN na polju borbe protiv sajber kriminala,
– Evropska konvencija o sajber kriminalu i delatnost EU na ovom polju,
– predlozi međunarodnih dokumenata iz ove oblasti, izrađeni od strane međunarodnih eksperata.

Metod:

Kratka prezentacija međunarodnih dokumenata iz ove oblasti. U drugom delu, učesnici su podeljeni po grupama (u odnosu na organizacije kojima pripadaju) i imaju dva zadatka: 1) da iz predstavljenih međunarodnih dokumenata izdvoje deo koji se odnosi na njihovu organizaciju i 2) da u predstavljenim međunarodnim dokumentima, na osnovu prethodnog segmenta o domaćim propisima i institucijama, izdvoje one delove koji su u skladu sa međunarodnom praksom, kao i one koje treba menjati. Nakon grupnog dela i prezentacije zaključaka grupa, sledi kraća diskusija.

Sredstva:
ppt i projektor (za predavača), flipchart (za radionicu).

Trajanje:
60 minuta.

Obrazloženje:
S obzirom na prirodu visokotehnološkog kriminala, neophodno je da učesnici obuke upoznaju i međunarodne instrumente na polju borbe protiv visokotehnološkog kriminala, kao i instrumente i aktivnosti EU, koja predstavlja dugoročno strateško opredeljenje naše zemlje.

2. Procesnopravni i drugi problemi pri gonjenju za počinjena dela visokotehnološkog kriminala, sa osvrtom na odnos ljudskih prava i ove vrste kriminala

Svrha:
Upoznati učesnike obuke sa procesnopravnim i drugim problemima za počinjena dela visokotehnološkog kriminala, sa posebnim osvrtom na pitanje ljudskih prava.

Sadržaj:
– definisanje procesnopravnih i drugih problema pri gonjenju za počinjena dela visokotehnološkog kriminala,
– odnos ljudskih prava i visokotehnološkog kriminala,
– analiza domaćih propisa i iskustava,
– uporedna iskustva i moguća normativna rešenja.

Metod:

Radionica. Učesnici, podeljeni u grupe prema organizacijama kojima pripadaju, imaju zadatak da, na osnovu već stečenih znanja o domaćem pravnom okviru za borbu protiv visokotehnološkog kriminala i međunarodnim standardima i iskustvima iz ove oblasti, definišu po pet najvećih procesnopravnih i drugih problema u domaćem sistemu gonjenja počinilaca krivičnih dela ove vrste kriminala. Grupe predstavljaju u plenumu svoje zaključke i bira se pet najznačajnijih problema. Fasilitatori oblikuju i po potrebi adaptiraju ove probleme. U drugom delu, svaka grupa ima zadatak da predloži po jedno određeno normativno rešenje za svaki problem. Nakon ovog dela, ponovo se radi u plenumu. Predstavnici grupa predstavljaju svoja rešenja, a predavač, način na koji su data pitanja rešena u drugim pravnim sistemima.

Trajanje:

90 minuta.

Sredstva:

flipchart (za rad po grupama), ppt i projektor (za predavača).

Obrazloženje:

Kroz metod radionice, učesnici, na osnovu prethodnog i do ove faze obuke stečenog znanja, identifikuju postojeće probleme i daju moguća rešenja.

3. Dosadašnja iskustva Srbije na suzbijanju VTK – najznačajniji slučajevi, statistički podaci, pravci daljih aktivnosti u ovoj oblasti

Svrha:

Upoznati učesnike obuke sa pojavnim oblicima, statistikama i trendovima i najvažnijim slučajevima iz oblasti visokotehnološkog kriminala u Srbiji.

Sadržaj:
– pojavni oblici visokotehnološkog kriminala u Srbiji,
– rasprostranjenost određenih krivičnih dela iz ove oblasti,
– statistike i trendovi,
– najznačajniji slučajevi.

Metod:
prezentacija.

Sredstva:
ppt, projektor.

Trajanje:
60 minuta.

Obrazloženje:
Neophodno je upoznati učesnike sa konkretnom situacijom u pogledu visokotehnološkog kriminala u Srbiji.

4. Studija slučaja

Svrha:
Produbiti i proširiti naučeno primenom stečenih znanja na konkretne relevantne studije slučaja.

Sadržaj:
– studija slučaja.

Metod:

Učesnici će, podeljeni u grupe prema organizaciji kojoj pripadaju, učestvovati u studiji relevantnog slučaja iz određenog pravnog sistema. Oni će imati zadatak da slučaj „rešavaju“ u skladu sa domaćim propisima. Nakon toga, učesnicima će biti prezentovan tok i ishod slučaja u datom stranom pravnom sistemu.

Sredstva:

flipchart (za grupe), ppt i projektor (za predavača).

Trajanje:

60 minuta.

Obrazloženje:

Učesnici će imati priliku da primene postojeća znanja u rešavanju konkretnog slučaja, kao i da steknu informacije o slučajevima koji su postavili standarde tumačenja i postupka u ovoj oblasti.

Ciljevi treninga

Opšti cilj treninga je da se obezbedi da sudije, javni tužioci i pripadnici policije steknu neophodna znanja i veštine za efikasnu primenu mera borbe protiv visokotehnološkog kriminala (VTK).

Posebni ciljevi treninga su:

– pružiti učesnicima obuke osnovne informacije o pojmu visokotehnološkog kriminala i pojmovno ga razgraničiti;

– obučiti pripadnike pravosudnih organa i policije da razlikuju krivična dela iz oblasti visokotehnološkog kriminala, međusobno i sa delima iz drugih vrsta kriminala;

– upoznati učesnike obuke sa kategorijama i pojavnim oblicima visokotehnološkog kriminala;

– upoznati učesnike sa domaćim pravnim i institucionalnim okvirom za borbu protiv visokotehnološkog kriminala;

– upoznati učesnike sa pojavnim oblicima, statistikama i trendovima visokotehnološkog kriminala u Srbiji i u drugim zemljama, i napraviti poređenje;

– približiti učesnicima značaj međunarodnih instrumenata i odnosa ljudskih prava sa visokotehnološkim kriminalom i u sklopu gonjenja za krivična dela iz oblasti visokotehnološkog kriminala.

Metode treninga:

Prezentacija kao metod se koristi kada je učesnike obuke potrebno upoznati sa novim informacijama.

Rad po grupama – koristi se kada je potrebno produbljivanje postojećih znanja i analiza određenog problema sa aspekata mesta u sistemu borbe protiv visokotehnološkog kriminala iz koga učesnici dolaze i njihovog prethodnog iskustva; trener-

fasilitator daje zadatak grupama i stoji im na raspolaganju ukoliko ima dodatnih pitanja; takođe, ukoliko neka grupa u svom radu zapadne u teškoće, trener treba aktivno da interveniše.

Studija slučaja – u poslednjem segmentu treninga treba da pomogne učesnicima da aktivno primene svoja znanja.

Sredstva:

1. kompjuter,
2. projektor,
3. flipchart,
4. markeri u boji,
5. sat.

Trajanje:

dva dana.

Raspored treninga:

Dan 1	
9:00 – 9:30	Uvodni deo
9:30 – 10:30	Pojam visokotehnološkog kriminala
10:30 – 11:00	Pauza za kafu
11:00 – 12:00	Kategorije krivičnih dela visokotehnološkog kriminala
12:00 – 12:15	Pauza
12:15 – 13:15	Granični slučajevi visokotehnološkog kriminala; svojstva koja krivičnim delima daju obeležje visokotehnološkog kriminala
13:15 – 14:15	Pauza za ručak
14:15 – 15:45	Domaći propisi za borbu protiv visokotehnološkog kriminala

Dan 2	
9:00 – 10:00	Međunarodni instrumenti na polju borbe protiv visokotehnološkog kriminala
10:00 – 10:30	Pauza za kafu
10:30 – 12:00	Procesnopravni i drugi problemi pri gonjenju za dela visokotehnološkog kriminala
12:00 – 12:15	Pauza
12:15 – 13:15	Dosadašnja iskustva Srbije na suzbijanju visokotehnološkog kriminala
13:15 – 14:15	Pauza za ručak
14:15 – 15:45	Studija slučaja
15:45 – 16:15	Evaluacija

Pravila treninga:

1. budite tačni,
2. aktivno učestvujte u radu,
3. ukoliko imate pitanja, možete ih postavljati u svakom trenutku,
4. budite slobodni da osporite tuđe mišljenje,
5. primenite sva svoja dosadašnja znanja i iskustva.

Pojam VTK

1. Visokotehnološki kriminal se može definisati kao radnja koja se preduzima uz upotrebu računara i drugih sredstava informacionih tehnologija, a koja je usmerena na:

– neovlašćen pristup zaštićenom računaru,
– neovlašćeno presretanje elektronskih podataka koji su upućeni sa računara ili ka drugom računaru,
– uništavanje, izmenu i brisanje elektronskih podataka,
– ometanje ili onemogućavanje funkcionisanja računarskog sistema putem oštećenja, brisanja, menjanja ili umetanja elektronskih podataka,
– distribuciju nedozvoljenih sadržaja,
– stvaranje i širenje virusa i malicioznog softvera.

(Ranko Jerković, „Borba protiv visokotehnološkog kriminaliteta u Srbiji“, *http://www.telekomunikacije.rs/aktuelni_broj/ranko_jerkovic:_borba_protiv_visokotehnoloskog_kriminaliteta_u_srbiji_.161.html*)

2. Visokotehnološki kriminal je vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku.

(Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala.)

3. Visokotehnološki kriminal se može definisati kao kriminalna aktivnost koja koristi infrastrukturu vezanu za informacione tehnologije i uključuje neovlašćen pristup, neov-

lašćeno presretanje podataka (tehničkim sredstvima, iz ili unutar kompjuterskog sistema), intervenciju na podacima (neovlašćeno oštećenje, brisanje, menjanje), sistemsko mešanje (neovlašćene intervencije u pogledu funkcionisanja kompjuterskog sistema, ubacivanjem, prenošenjem, oštećenjem ili menjanjem kompjuterskih podataka), zloupotrebu uređaja, krivotvorenje (ID *theft*) i elektronsku prevaru.

(Paul Taylor, „Hackers: Crime in the Digital Sublime" (November 3, 1999 ed.). Routledge; 1 edition. pp. 200. ISBN 0415180724.)

4. Visokotehnološki kriminal predstavlja svako neautorizovano ponašanje koje uključuje automatsku obradu podataka ili njihov prenos. Ono predstavlja poseban vid inkriminisanih ponašanja kod kojih se računarski sistem (shvaćen kao jedinstvo hardvera i softvera) pojavljuje ili kao sredstvo ili kao objekt krivičnog dela, ukoliko se delo na drugi način ili prema drugom objektu uopšte ne bi moglo izvršiti ili bi ono imalo bitno drugačije karakteristike.

(Prof. Đorđe Ignjatović u „Visokotehnološki kriminal", Denis Bećirović, Bilten Okružnog suda u Beogradu, br. 7/2005.)

5. Kompjuterski kriminal je kriminalna aktivnost koja se obavlja korišćenjem kompjutera i interneta. Ovo pokriva dug niz aktivnosti, od nelegalnog „skidanja" muzičkih fajlova sa internata, do krađe miliona dolara sa onlajn bankovnih računa. Ova vrsta kriminala takođe uključuje i nenovčane prekršaje, kao što su stvaranje i prenošenje virusa na druge kompjutere ili postavljanje poverljivih poslovnih informacija na internet.

(*http://www.techterms.com/definition/cybercrime*)

Kategorije krivičnih dela iz oblasti VTK

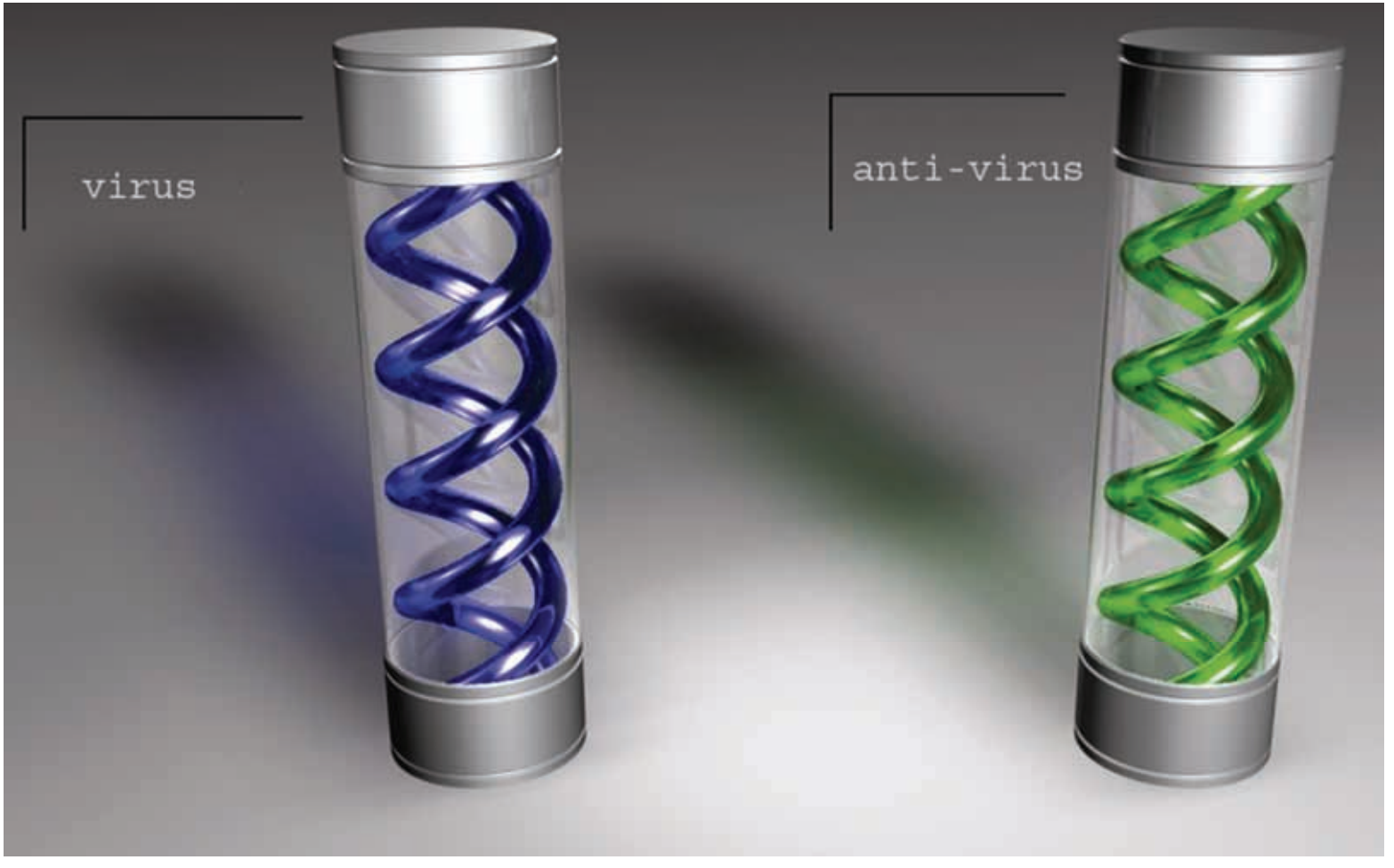
U odnosu na činjenicu da li se računar, sistem ili mreža koriste kao sredstvo za izvršenje dela ili su objekat na kome se delo izvršava, ponekad se koriste različiti izrazi da bi se definisala kriminalna delatnost koja se vrši upotrebom računara:

1. klasičan kompjuterski kriminal kod koga je računar ili računarski sistem sredstvo izvršenja ili objekat napada;

2. internet kriminal kod koga je zloupotreba mreže određujući faktor (posedovanje i distribucija dečje pornografije, raspirivanje nacionalne i rasne mržnje, neovlašćena distribucija autorskih dela i predmeta intelektualne svojine);

3. e-kriminal koji se vezuje za zloupotrebu komunikacionih uređaja i uređaja za skladištenje elektronskih podataka (npr. prevare vezane za platne kartice ili podizanje gotovog novca).

(Ranko Jerković, „Borba protiv visokotehnološkog kriminaliteta u Srbiji“, *http://www.telekomunikacije.rs/aktuelni_broj/ranko_jerkovic:_borba_protiv_visokotehnoloskog_kriminaliteta_u_srbiji_.161.html*)


virus
anti-virus

Spamming, Cookies, Adware/Spyware

Slanje neželjene elektronske pošte (*spam*) najčešće funkcioniše tako što *spammer*-i nabavljaju na ilegalnom tržištu liste sa velikim brojem imejl adresa ili ih sami pribavljaju korišćenjem programskih alata, koji se popularno zovu *spambots.*[1] Nije redak slučaj da se te liste imejl naloga nabavljaju od hakera, koji ih preuzimaju „provalom“ u veb servere ili baze podataka sa lokalnih mreža. Dešava se i da sam korisnik, svojom nepažnjom, omogući da se njegova imejl adresa nađe na nekoj od pomenutih lista, tako što se prilikom registracije na neke internet veb portal sajtove saglasi sa tom opcijom, ne pročitavši pažljivo tekst procedure registracije.

Kao što se može videti, *spam* poruke imaju najčešće marketinški aspekt. U principu, slanje ove vrste pošte najjeftiniji je način reklame, i čak se i procentualno mali odaziv na te poruke meri desetinama hiljada odgovora. Može se desiti da se uz *spam* poruku pošalje, u vidu priloga imejlu, i neki virus (*malware)*. U tom slučaju se susrećemo sa situacijom koja nije više u sivoj zoni graničnih slučajeva, već biće krivičnog dela iz člana 300 Krivičnog zakonika Srbije, Pravljenje i unošenje računarskih virusa.

*Cookie*s (kolačići) svoj naziv duguju kolačićima sudbine (*fortune cookies*),[2] gde se unutar „kolačića” nalazi skrivena poruka. Možda je ovo i najbolje objašnjenje šta su to „kolačići”. Naime, internet prezentacije, a pogotovo one sa aktivnim sadržajem, koje imaju registracione forme i baze svojih korisnika, smeštaju na računar posetioca malu tekstualnu datoteku sa jedinstvenim identifikacionim brojem (na veb serveru internet prezentacije se nalazi aplikacija koja prepoznaje ove brojeve) i

Cookies (kolačići) svoj naziv duguju kolačićima sudbine (fortune cookies), gde se unutar „kolačića” nalazi skrivena poruka.

[1] Izvor: *http://en.wikipedia.org/wiki/Spambot*, 01.05.2009.

[2] Izvor: *http://www.wisegeek.com/what-are-computer-cookies.htm*, 01.05.2009.

imenom internet prezentacije. Retke su prilike da „kolačići" sadrže i neke privatne informacije o korisniku, koje je on pružio prilikom registrovanja ili posete nekoj internet prezentaciji. Namera je da se prilikom sledeće posete korisniku omogući nesmetan nastavak rada iako su internet pretraživač *(web browser*) ili računar u međuvremenu bili isključeni. „Kolačići" mogu da budu privremeni (smeštaju se u radnu memoriju računara, koja se prazni prilikom njegovog gašenja) ili trajni, kada se nalaze na hard disku računara.[3]

Treba napomenuti da se mogu javiti slučajevi kada neke „kolačiće" može da koristi više kompanija, koje prate, recimo, šta ste kupovali preko interneta i na taj način „špijuniraju" i prate vaše kretanje kroz internet, što ulazi u sfere nedozvoljenog ponašanja. U to ime, svi internet pretraživači imaju mogućnost da „kolačiće" restriktivno prihvataju, ili čak i isključe, uz napomenu da vam neke internet prezentacije u ovom slučaju neće raditi.

Adware/Spyware. – Termin *adware* se odnosi na programe koji: „automatski puštaju, prikazuju ili preuzimaju reklame, nakon instalacije tog programa ili kada je aplikacija u upotrebi".[4] *Spyware* aplikacije se instaliraju na računaru *bez znanja korisnika*, zatim, koristeći internet vezu, dakle resurse korisnika, šalju informacije o kretanju korisnika na internetu, menjaju konfiguraciju internet pretraživača, usporavaju rad računara...

Moguće su i situacije da ti programi šalju i informacije o korisniku računara, koje možemo tumačiti kao privatne (ime i prezime, brojeve telefona, lozinke, korisnička imena...), čime se već može prepoznati ozbiljan problem privatnosti na internetu. Što se tiče *adware* programa, česte su situacije da programeri da bi omogućili masovnu upotrebu njihovih proizvoda i na taj način dospeli do više korisnika, omogućavaju besplatno preuzimanje sa interneta njihovog programa, uz saglasnost koris-

Termin adware se odnosi na programe koji: „automatski puštaju, prikazuju ili preuzimaju reklame, nakon instalacije tog programa ili kada je aplikacija u upotrebi". Spyware aplikacije se instaliraju na računaru bez znanja korisnika, zatim, koristeći internet vezu, dakle resurse korisnika, šalju informacije o kretanju korisnika na internetu, menjaju konfiguraciju internet pretraživača, usporavaju rad računara...

[3] Izvor: *http://www.wisegeek.com/what-are-computer-cookies.htm*, 01.05.2009.
[4] Izvor: *http://en.wikipedia.org/wiki/Adware*, 01.05.2009.

nika da će prilikom korišćenja aplikacije biti izložen reklamnim porukama, dok eventualno ne plati za taj *software*. Na ovaj način se programeru vraća uloženo, kroz zaradu od ustupanja reklamnog prostora u kodu aplikacije. Mnoge kompanije koje koriste *adware* u svrhe reklamiranja ne prihvataju da se njihovi programi zovu *spyware*, pa je iz *McAfee*-a (proizvođači bezbednosnih aplikacija) proizašao termin PUP (*Potentially Unwanted Program*),[5] što u prevodu znači potencijalno neželjeni program. Pored osnovnog značenja *spyware* programa, koji se vezuju uz *adware* i reklamni *software*, postoji i definicija koja ih tumači kao „tehnologiju koja pomaže u sakupljanju informacija o osobi *bez njenog znanja*,"[6] gde se, pri tom, *spyware* ubacuje u računar na netransparentan način, ili kao deo nekog virus programa i može, a često i služi, da obezbedi hakerima korisne informacije da bi upadali u računarske sisteme (koji je operativni sistem u upotrebi?, „provala" datoteke SAM (*Security Account Manager* – kod *Windows* operativnih sistema), baze sa korisničkim šiframa itd.). Takvi programi su, na primer, *key logger* (programi koji pamte šta se kuca na tastaturi), zatim *dialer* (programi koji uspostavljaju vezu sa drugim mrežama, koristeći korisnikov modem i telefonsku liniju, a pre svega korisnikovu nepažnju). U vezi sa temom *adware* programa treba pomenuti i *pop-up* prozore, koji se pojavljuju kada je neki *adware* program aktivan, a mnogo češće prilikom „krstarenja" internetom, i to kao iskačući prozori-reklame. Treba biti obazriv prilikom reagovanja na ove prozore (čak i kada je namera da se ugase) zato što se pogrešnim „klikom" omogućava instalacija *spyware* ili nekih drugih malicioznih (*malware*) programa. Na kraju, pored obazrivosti, protiv *spyware* programa mogu da se koriste i neki besplatni programi sa interneta, na primer *Spybot Search & Destroy*.[7]

---

[5] Izvor: *http://searchsecurity.techtarget.com/loginMembersOnly/1,289498,sid14_gci1066761,00.html*, 01.05.2009.

[6] Izvor: *http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214518,00.html*, 01.05.2009.

[7] Izvor: *http://www.safer-networking.org/index2.html*, 01.05.2009.

Zakonski okvir

Zakonodavna rešenja vezana za oblast visokotehnološkog kriminala u zakonodavstvu Republike Srbije mogu se razvrstati u tri grupe. Prvu grupu čini Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala,[8] propis statusnog karaktera kojim se vrši uspostavljanje organizacije i nadležnosti državnih organa u borbi protiv visokotehnološkog kriminala. Drugu grupu čine propisi materijalnopravne prirode, kojima je predviđeno koje radnje predstavljaju društveno neprihvatljivo ponašanje, čime se narušavaju ili povređuju određeni zaštitni objekti, i kao takve se po mišljenju zakonodavca smatraju krivičnim delima ili osnovom za prekršajnu odgovornost ili odgovornost za privredne prestupe. Treću grupu čini Zakonik o krivičnom postupku,[9] koji uspostavlja procesnopravne okvire kojima su predviđeni mehanizmi i ovlašćenja državnih organa u postupcima otkrivanja, prikupljanja dokaza, krivičnog gonjenja i suđenja učiniocima krivičnih dela visokotehnološkog kriminala.

U vezi sa *Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala* važno je istaći da je donošenjem ovog zakona i osnivanjem posebnih organa za borbu protiv visokotehnološkog kriminala načinjen veliki korak, što predstavlja izraz razumevanja rizika koji sa sobom nosi izvršenje krivičnih dela iz ove oblasti i doprinos uspostavljanju visokotehnološke bezbednosti. Činjenica da su informacione i komunikacione tehnologije postale nezamenljive u funkcionisanju modernih društava nametnula je potrebu da se u svetskim okvirima uspostave mere i mehanizmi za zaštitu društava i pojedinaca od visokotehnološkog

[8] „Službeni glasnik RS“, br. 61/05.
[9] „Službeni glasnik RS“ br. 58/04,... 49/07.

kriminala usvajanjem odgovarajućih zakonodavnih rešenja i unapređenjem međunarodne saradnje. Rezultat takvih napora je, između ostalog, i donošenje Konvencije o sajber kriminalu Saveta Evrope,[10] koja uspostavlja minimum standarda koje je neophodno, po mišljenju međunarodne zajednice, da ispune nacionalna zakonodavstva u cilju efikasne borbe protiv visokotehnološkog kriminala. S druge strane, pitanje organizacije pravosudnog sistema svake države u pravcu stvaranja pretpostavki za uspešnu borbu i suzbijanje novih pojavnih oblika kriminala, u ovom slučaju visokotehnološkog, pitanje je koje uvek nameće niz nedoumica na koje nije lako dati odgovor. Da li se opredeliti za sveobuhvatnu sistemsku promenu, koja se ogleda u promeni i usklađivanju niza propisa kako bi se stvorio adekvatan zakonski okvir koji bi omogućio državnim organima efikasno delovanje, ili se odlučiti za delimičnu izmenu pojedinih zakonskih odredaba u pravcu izmene postojećih ovlašćenja ili nadležnosti, ili uspostavljanja novih, do tada nepostojećih, organa koji bi bili „umetnuti“ u već postojeći i uvreženi sistem delovanja, pitanje je čiji odgovor mora da pomiri niz različitih zahteva i mogućnosti. S jedne strane, odabir prve varijante pruža mogućnost da se odgovori svim potrebnim zahtevima, ali, sa druge strane, zahteva angažovanje velikih materijalnih i ljudskih resursa, postavljanje sistema na potpuno novim osnovama za šta je potrebna snažna politička volja ali i društvena svest o neophodnosti takvih promena. Izbor druge varijante pruža mogućnost bržih promena bez zadiranja u osnove sistema i uz angažovanje mnogo manje sredstava, ali, s druge strane, može da nametne niz drugih problema kao što su preplitanje nadležnosti starih i novih organa, odnosno nerešeno pitanje nadležnosti za pojedina krivična dela, kolizija novih zakonskih rešenja sa postojećim u pogledu novih ovlašćenja, pitanje neprihvatanja, odnosno saradnje sa novim organima koji remete već ustaljene i uobičajene načine saradnje.

[10] Convention on Cybercrime, Budapest, 23. XI 2001. (ETS No. 185).

U Okružnom javnom tužilaštvu u Beogradu formirano je Posebno tužilaštvo za borbu protiv visokotehnološkog kriminala, dok je u okviru Okružnog suda u Beogradu formirano Veće za borbu protiv visokotehnološkog kriminala, a u okviru Ministarstva unutrašnjih poslova osnovana je posebna služba radi obavljanja poslova organa unutrašnjih poslova u vezi sa ovim krivičnim delima. Teritorijalna nadležnost navedenih organa uspostavljena je na celoj teritoriji Republike Srbije. Iako ovakvo zakonsko rešenje pruža dobar osnov za uspešnu borbu protiv visokotehnološkog kriminala, problem nastaje s obzirom na način kako je formulisana stvarna nadležnost pomenutih organa. Naime, član 3 Zakona propisuje da se ovaj zakon primenjuje radi otkrivanja, gonjenja i suđenja za krivična dela protiv bezbednosti računarskih podataka i krivična dela protiv intelektualne svojine, imovine i pravnog saobraćaja kod kojih se kao objekat ili sredstvo izvršenja javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj autorskih dela prelazi 500 ili nastala materijalna šteta prelazi iznos od 850.000 dinara. Ovako određena stvarna nadležnost posebnih organa za borbu protiv visokotehnološkog kriminala ne obuhvata krivična dela koja se odnose na dečju pornografiju i zloupotrebu platnih kartica. Naime, krivična dela prikazivanje pornografskog materijala i iskorišćavanje dece za pornografiju iz člana 185 Krivičnog zakonika Republike Srbije i falsifikovanje i zloupotreba platnih kartica iz člana 225 istog zakona ne spadaju u korpus krivičnih dela u čijem postupanju su nadležni posebni organi.

Drugu grupu propisa u zakonodavstvu Republike Srbije koji se tiču visokotehnološkog kriminala čine propisi materijalnog karaktera. To je pre svega *Krivični zakon Republike Srbije*[11] kojim su propisana krivična dela iz oblasti visokotehnološkog kriminala, kao i sva druga krivična dela koja se odnose na opšti i organizovani kriminal. Danom stupanja na snagu ovog zakonika, 1. januara 2006. godine, prestali

[11] „Službeni glasnik RS“, br. 85/05, 88/05, 107/05.

su da važe Krivični zakon Republike Srbije i Osnovni krivični zakon (bivši Krivični zakon Savezne Republike Jugoslavije). Pomenutim zakonom predviđena su krivična dela vezana za oblast visokotehnološkog kriminala, koja su bila predviđena i ranijim zakonima – Krivičnim zakonom Republike Srbije, s tim što su propisana i neka nova krivična dela koja ranije nisu postojala kao krivično delo, a to je neovlašćeno korišćenje računara ili računarske mreže iz člana 304 Krivičnog zakonika, dok su krivična dela iz glave XX Krivičnog zakonika – protiv intelektualne svojine, preneta iz Zakona o autorskim i srodnim pravima, u kome su ostale predviđene kaznene odredbe, u članu 187 za privredni prestup i u članu 188 za prekršaj. Prema važećem Krivičnom zakoniku, odredbe koje se odnose na oblast visokotehnološkog kriminala sadržane su pre svega u opštem delu Zakonika u članu 112, u delu koji se odnosi na značenje izraza u smislu krivičnog zakonodavstva. Na ovaj način je propisano šta se smatra računarskim podatkom, računarskom mrežom, računarskim programom, računarskim virusom. Računarskim podatkom se smatra predstavljena informacija, znanje, činjenica, koncept ili naredba, koji se unosi, obrađuje ili pamti ili je unet, obrađen ili zapamćen u računaru ili računarskoj mreži. Računarskom mrežom smatra se skup međusobno povezanih računara koji komuniciraju razmenjujući podatke. Računarskim programom smatra se uređeni skup naredbi, koji služi za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara. Računarski virus je računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu, koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka. Navedeno predstavlja deo definicija pojedinih pojmova koji se koriste u Krivičnom zakoniku i njihovo značenje u smislu odredaba ovog zakonika, a koji su vezani za oblast visokotehnološkog kriminala, na šta upućuje i odredba člana 2, stav 2 Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, kojim je propisano da izrazi koji se koriste u ovom zakonu imaju značenje u smislu odredaba

Računarski virus je računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu, koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka.

Krivičnog zakona. Konkretna krivična dela, propisana krivičnim zakonodavstvom, pre svega su ona koja se odnose na bezbednost računarskih podataka. Navedena krivična dela sadržana su u Konvenciji o sajber kriminalu, u domaćem zakonodavstvu propisana su u glavi XXVII Krivičnog zakonika i obuhvaćena članom 3, stav 1 Zakona o organizaciji i nadležnosti državnih organa u borbi protiv visokotehnološkog kriminala, kao krivična dela koja spadaju u isključivu nadležnost ovih organa.

To su oštećenje računarskih podataka i programa iz člana 298 Krivičnog zakonika, računarska sabotaža iz člana 299, pravljenje i unošenje računarskih virusa iz člana 300, računarska prevara iz člana 301, neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka iz člana 302, sprečavanje i ograničavanje pristupa javnoj računarskoj mreži iz člana 303 i neovlašćeno korišćenje računara i računarske mreže iz člana 304.

Sledeća grupa krivičnih dela propisana Konvencijom o sajber kriminalu sadržana je u Krivičnom zakoniku, i to su krivična dela protiv intelektualne svojine – glava XX, krivična dela protiv imovine – glava XXI i krivična dela protiv pravnog saobraćaja – glava XXXII, a članom 3, stav 2 Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala određeno je da ova krivična dela spadaju u nadležnost organa za borbu protiv visokotehnološkog kriminala pod određenim kumulativno i alternativno određenim uslovima, odnosno ukoliko se kao objekat ili sredstvo izvršenja javljaju računari, računarske mreže, računarski

podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, i ako broj primeraka autorskih dela prelazi 500 ili nastala materijalna šteta iznos od 850.000 dinara.

U grupu krivičnih dela protiv intelektualne svojine, koja su kao posebno propisana i obuhvaćena Konvencijom i stoga i ovde posebno navedena, spadaju povreda moralnih autora i interpretatora iz člana 198 Krivičnog zakonika, neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199, neovlašćeno uklanjanje ili menjanje elektronske informacije o autorskim i srodnim pravima iz člana 200, povreda pronalazačkog prava iz člana 201, neovlašćeno korišćenje tuđeg dizajna iz člana 202.

Pored navedenih krivičnih dela, treba pomenuti i krivična dela prikazivanje pornografskog materijala i iskorišćavanje dece za pornografiju iz člana 185 i falsifikovanje i zloupotreba platnih kartica iz člana 225, koja su prema odredbama Konvencije svrstana u grupu krivičnih dela protiv visokotehnološkog kriminala i koja po svojoj prirodi to i jesu, ali u domaćem pravu i dalje se nalaze u okviru organa opšte nadležnosti.

Pored Krivičnog zakonika i *Zakonom o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine*[12] regulisana je jedna od oblasti koja spada u visokotehnološki kriminal – zaštita intelektualne svojine. Navedenim propisom predviđena je odgovornost za privredne prestupe i prekršajna odgovornost pravnih lica za povredu prava intelektualne svojine i data su ovlašćenja pojedinim ministarstvima kroz službe inspekcije (ministarstvo nadležno za poslove trgovine, turizma i usluga, preko tržišne inspekcije i turističke inspekcije, ministarstvo nadležno za poslove finansija, preko poreskih inspektora i poreske policije i sl.) da sprovode mere iz svoje nadležnosti u pravcu kontrole proizvodnje, prometa, upotrebe i držanja robe i pružanja usluga kojima se povređuje pravo intelektualne svojine.

[12] „Službeni glasnik RS“, broj 46/06.

Zakonik o krivičnom postupku kao treća vrsta propisa u zakonodavstvu Republike Srbije sadrži odredbe procesnopravnog karaktera kojima su predviđeni procesni mehanizmi i ovlašćenja svih učesnika u krivičnom postupku u pogledu otkrivanja učinilaca krivičnih dela, prikupljanja dokaza, procesuiranja i suđenja. Navedeni zakonik, osim posebne glave koja se odnosi na krivična dela organizovanog kriminala, sadrži i odredbe opšteg karaktera koje se odnose na sve vrste krivičnih dela, pa i krivična dela visokotehnološkog kriminala. U okviru procesnih odredaba, posmatrano u odnosu na krivična dela visokotehnološkog kriminala, poseban značaj imaju odredbe kojima se reguliše prikupljanje i obezbeđivanje dokaza. U vezi sa izvršenjem krivičnih dela visokotehnološkog kriminala pojavljuje se jedna posebna vrsta dokaza koji se po svojoj prirodi razlikuju od tzv. klasičnih dokaza, koji se pojavljuju u vezi sa izvršenjem krivičnih dela opšteg kriminala, a to su elektronski dokazi. Jedan od nedostataka važećeg Zakonika o krivičnom postupku jeste što ne daje definiciju dokaza, a samim tim ni definiciju elektronskog dokaza. Elektronski dokaz jeste informacija ili podatak od značaja za istragu, smešten ili prenet putem računara. Pomenuti dokazi imaju istu vrednost kao i svi drugi materijalni dokazi i za njih važe potpuno ista procesna pravila kao i za sve ostale dokaze. Međutim, ono što se nikako ne sme gubiti iz vida u pogledu elektronskih dokaza jeste specifičnost elektronskih dokaza, koja proizlazi iz njihove prirode, a to je da su veoma osetljivi, odnosno vrlo lako se mogu izmeniti, obrisati ili na bilo koji drugi način uništiti. Takođe, elektronski dokazi mogu da budu smešteni na pojedinačnom računaru, računarskoj mreži ili udaljenom serveru van teritorijalne nadležnosti organa koji ih prikupljaju, mogu da budu vidljivi ili nevidljivi, što pored pomenute mogućnosti njihove lake izmene ili uništenja, kako namerno, tako i usled nestručnog rukovanja, nameće i niz specifičnosti u njihovom pribavljanju. Upravo ove specifičnosti elektronskih dokaza koje proizlaze iz njihove prirode mogu da budu od velikog uticaja na potpuno utvrđivanje činjeničnog stanja koje je, kako u fazi pretkrivičnog postupka, kroz rad policije i tužilaštva, tako i u fazi istrage kojom rukovodi istražni sudija, od vitalnog značaja

za ishod svakog krivičnog postupka. Ovo stoga što činjenično stanje predstavlja osnov za donošenje odluke o postojanju ili nepostojanju krivičnog dela, kao i o krivičnoj odgovornosti učinioca. Činjenice od značaja za krivični postupak utvrđuju se kroz radnje dokazivanja strogo propisane u Zakoniku o krivičnom postupku,[13] koji predstavlja procesni okvir kojim je regulisano postupanje svih nadležnih organa i njihova ovlašćenja. Za razliku od Konvencije o sajber kriminalu koja prepoznaje značaj i specifičnost elektronskih dokaza i upravo iz tih razloga i predviđa posebne procesne mehanizme kojima se omogućava ili olakšava prikupljanje ove vrste dokaza, Zakonik o krivičnom postupku ne predviđa posebne mehanizme i ovlašćenja državnih organa, već se primenjuju opšta procesna pravila kao i u pogledu svih ostalih dokaza. Polazeći od osnovne premise da samo činjenice prikupljene na zakonom propisan način mogu da imaju karakter dokaza u postupku i doprinesu potpunom utvrđivanju činjeničnog stanja, jasno je da specifična priroda elektronskih dokaza igra veliku ulogu u propisivanju procesnih ovlašćenja i adekvatnih mehanizama koji bi trebalo da omoguće njihovo prikupljanje u krivičnom postupku.

Prema Zakoniku o krivičnom postupku, radnje dokazivanja su: pretresanje stana i lica – čl. od 77 do 81, privremeno oduzimanje predmeta – čl. od 82 do 86, postupanje sa sumnjivim stvarima – čl. 87 i 88, saslušanje okrivljenog – čl. od 89 do 95, saslušanje svedoka – čl. od 96 do 109, uviđaj – čl. od 110 do 112 i veštačenje – čl. od 113 do 132. Navedene radnje dokazivanja primenjuju državni organi nadležni za otkrivanje krivičnih dela svih vrsta kriminaliteta i u okviru njih nije predviđeno nijedno posebno ovlašćenje niti mehanizam koji bi se odnosio na krivična dela visokotehnološkog kriminala, imajući u vidu specifičnu prirodu elektronskih dokaza koji se pojavljuju u vezi sa njihovim izvršenjem. Pored navedenih radnji dokazivanja, Zakonikom o krivičnom postupku predviđene su i specijalne istražne tehnike[14] koje su

[13] „Službeni glasnik RS“ br. 58/04,... 49/07.

[14] Kontrolisane isporuke, prikriveni islednik i sl.

ostale van domašaja organa za borbu protiv visokotehnološkog kriminala, imajući u vidu da su prema zakonskim odredbama primenjiva samo za krivična dela organizovanog kriminala. Takođe, mera tajnog audio i video-nadzora iz člana 232 Zakonika o krivičnom postupku nije primenjiva u pogledu krivičnih dela visokotehnološkog kriminala s obzirom na to da se po odredbama Zakonika može primenjivati samo u pogledu krivičnih dela protiv ustavnog uređenja i bezbednosti, krivičnih dela protiv čovečnosti i međunarodnog prava, kao i krivičnih dela sa elementima organizovanog kriminala. Jedina mera koja ostaje u okviru primene u vezi sa izvršenjem krivičnih dela visokotehnološkog kriminala jeste izdavanje naredbe istražnog sudije bankarskoj, finansijskoj ili drugoj organizaciji o dostavi podataka o stanju poslovnih ili ličnih računa osumnjičenog iz člana 234 Zakonika o krivičnom postupku. Međutim, navedena mera je primenjiva samo u pogledu krivičnih dela za koja je zakonom propisana kazna zatvora od najmanje četiri godine, što u slučaju krivičnih dela visokotehnološkog kriminala ograničava primenu na krivično delo neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199, stav 3 Krivičnog zakonika, računarske prevare iz člana 301, st. 2 i 3 Krivičnog zakonika u pogledu pojedinih težih oblika i krivičnog dela računarske sabotaže iz člana 299 Krivičnog zakonika u celosti.

Ujedinjene nacije

Rezolucija br. 55/63 o borbi protiv zloupotrebe informatičkih tehnologija

Osnovno načelo koje ističe Rezolucija jeste da bi sve države, kroz svoja nacionalna zakonodavstva, trebalo da onemoguće postojanje „sigurnih područja“ za izvršioce krivičnih dela visokotehnološkog kriminala, čime se zapravo u prvi plan ističe potreba za sinhronizovanom zakonodavnom akcijom na globalnom nivou i ukazuje na opasnost da bi one države koje propuste da pravno regulišu ovu oblast privukle na svoju teritoriju veliki broj potencijalnih izvršilaca krivičnih dela.

Dalje, navodi se da mora da postoji koordinacija, odnosno saradnja između nadležnih organa država članica, koji se bave istragom i krivičnim progonom u vezi sa zloupotrebom informatičkih tehnologija. Ovde se zapravo ukazuje na međunarodni, odnosno transnacionali karakter visokotehnološkog kriminala, zbog čega se i efikasna međunarodna saradnja postavlja u fokus.

Svaka država potpisnica treba da posveti naročitu pažnju edukaciji, odnosno savremenim metodama obuke lica angažovanih na otkrivanju i krivičnom progonu izvršilaca krivičnih dela visokotehnološkog kriminala. Na ovaj način percipira se problem koji bi mogao da nastane u sprovođenju odgovarajućih zakona usled nedovoljne obučenosti nadležnih istražitelja, tužilaca i sudija.

Takođe, potrebno je da se pravnim mehanizmina zaštite poverljivost, integritet i dostupnost računarskih podataka i sistema od neovlašćenog uništenja, izmene ili brisanja. Ovim se ukazuje na potrebu da se odgovarajuća ponašanja sankcionišu, što je većina zakonodavstava i učinila predviđajući postojanje krivičnih dela protiv bezbednosti računarskih podataka. U vezi sa navedenim je i obaveza da se pravno reguliše postupak čuvanja i brzog pristupa elektronskim podacima koji su u vezi sa

Svaka država potpisnica treba da posveti naročitu pažnju edukaciji, odnosno savremenim metodama obuke lica angažovanih na otkrivanju i krivičnom progonu izvršilaca krivičnih dela visokotehnološkog kriminala.

aktuelnim krivičnin istragama (ova obaveza uglavnom se odnosi na internet provajdere, a u Srbiji je, na primer, ovo pitanje regulisano podzakonskim aktom, što ćemo videti docnije).

Ukazuje se i na potrebu da se javnost upozna sa opasnostima koje prete iz sajber prostora, kao i na činjenicu da odgovarajuće mere prevencije mogu sprečiti izvršenje mnogih krivičnih dela ili barem uticati na njihovo blagovremeno prijavljivanje, i to u cilju efikasnog krivičnog progona. Rezultati brojnih istraživanja pokazuju da je tamna brojka visokotehnološkog kriminaliteta izuzetno visoka, mogli bismo reći i bez premca ako se uporedi sa drugim vrstama i pojavnim oblicima kriminaliteta. Razlozi tome su mnogobrojni, ali najpre treba poći od činjenice da nije jednostavno statistički „brojati“ bilo koju vrstu kriminala. Postoje tri osnovna koraka neophodna za kvantifikovanje određenog kriminalnog ponašanja. Kao prvo, neophodno je da određena delatnost bude uopšte uočena, zatim da ona bude kvalifikovana kao kriminalna delatnost i, konačno, da kao takva bude prijavljena nadležnim organima. Ukoliko bilo koja od ovih faza izostane, preduzeta kriminalna delatnost neće biti zabeležena u statistikama nadležnih organa, odnosno činiće deo tamne brojke kriminaliteta.

Konačno, Rezolucija upozorava da se u borbi protiv zloupotrebe računarskih tehnologija mora očuvati balans između individualnih prava i sloboda koje su garantovane svakom pojedincu, sa jedne, i prava države da krivično goni počinioce krivičnih dela, sa druge strane. Reč je zapravo o tome da represivne mere i ograničenja određenih prava građana u vezi sa krivičnim progonom moraju da budu restriktivni i samo u onoj meri koja je neophodna za zakonito prikupljanje dokaza i vođenje krivičnog postupka pred nadležnim sudovima.

Rezolucija 56/121 Generalne skupštine UN

Rezolucija je usvojena 23. januara 2002. godine i takođe kao predmet ima borbu protiv zloupotrebe informatičkih tehnologija.[15] Kao dopuna Rezolucije 55/63, još jednom je ukazano na potrebu da se prilikom usvajanja odgovarajućih zakona, kao i prilikom utvrđivanja politike krivičnog progona, uzmu u obzir rezultati rada Komisije za prevenciju kriminala i krivično pravosuđe te drugih relevantnih međunarodnih i regionalnih organizacija.

Rezolucija Ekonomsko-socijalnog saveta (ECOSOC) 2007/20

Rezolucija poziva države članice da ozbiljno razmotre potrebu za modernizacijom postojećeg nacionalnog zakonodavstva naročito imajući u vidu dramatičan porast transnacionalnog privrednog kriminaliteta i u vezi sa tim upotrebu modernih računarskih tehnologija kao sredstva za izvršenje ovih krivičnih dela. Ukazuje se i na potrebu da nacionalna krivična zakonodavstva, ukoliko to nisu učinila, predvide neovlašćenu upotrebi ili izradu identifikacionih dokumenata, kao i podataka o identitetu. S tim u vezi, podstiče se i šira i efikasna upotreba modernih tehnologija u prevenciji i suzbijanju kako privrednog, tako i kriminaliteta povezanog sa zloupotrebom identiteta.

Konačno, ukazuje se i na potrebu da države članice razmotre pristupanje Konvenciji Saveta Evrope o visokotehnološkom kriminalu, kao i svim drugim međunarodnim pravnim aktima koji su primenljivi kada je u pitanju privredni kriminalitet i zloupotreba identiteta i identifikacionih podataka.

Takođe, postignuta je i saglasnost da se pitanja privrednog kriminaliteta i zloupotrebe identiteta, kao posebna tema, nađu na dnevnom redu Komisije UN za prevenciju kriminaliteta i krivično pravosuđe.

[15] „Resolution A/res/56/121“, General Assembly of the United Nations, 23. januar 2002.

Ciljevi Konvencije su, pre svega, harmonizacija između nacionalnih zakonodavstava kada je reč o materijalnopravnim odredbama u oblasti visokotehnološkog kriminala; uvođenje adekvatnih instrumenata u nacionalna zakonodavstva kada je reč o procesnim odredbama, kako bi se stvorila osnova za istraživanje i procesuiranje ovih krivičnih dela; ustanovljavanje brzih i efikasnih institucija i procedura međunarodne saradnje.

Savet Evrope

Konvencija o visokotehnološkom kriminalu Saveta Evrope sa Dodatnim protokolom

Ciljevi Konvencije su, pre svega, harmonizacija između nacionalnih zakonodavstava kada je reč o materijalnopravnim odredbama u oblasti visokotehnološkog kriminala; uvođenje adekvatnih instrumenata u nacionalna zakonodavstva kada je reč o procesnim odredbama, kako bi se stvorila osnova za istraživanje i procesuiranje ovih krivičnih dela; ustanovljavanje brzih i efikasnih institucija i procedura međunarodne saradnje.[16]

Već u preambuli Konvencije naglašava se da postoji potreba za kažnjavanjem počinilaca dela vezanih za korišćenje računara i računarskih mreža, koja su specifična po mnogim činiocima, a najviše po tome što po pravilu imaju međunarodni karakter. Zbog toga je unapređenje saradnje policijskih i drugih relevantnih organa među državama sveta jedan od osnovnih zadataka razvoja mehanizama suzbijanja visokotehnološkog kriminala.

U preambuli se poziva na niz konvencija i drugih međunarodnih dokumenata koji su nastali u okviru Ujedinjenih nacija, Saveta Evrope i drugih međunarodnih organizacija, a koji ustanovljavaju određene standarde poštovanja ljudskih prava, posebno prava dece, kao i prava na privatnost i bezbednost podataka o ličnosti. Na ovaj način, tvorci Konvencije veoma jasno stavljaju do znanja da namera tog teksta nije da uruši postojeće standarde uživanja ljudskih prava putem mešanja države, odnosno policijskih i istražnih organa, u privatnost pojedinca ili poslovanje kompanija, već naprotiv da ustanovi efikasne elemente zaštite tih istih prava od neautorizovanih spoljnih invazija, od strane trećih lica.

[16] *Convention on Cybercrime – Explanatory Report*, str. 4-5. Tekst dostupan na internet adresi: *http://conventions.coe.int/Treaty/en/Reports/Html/185.htm*, 01.05.2009.

Konvencija se sastoji iz četiri poglavlja: Upotreba termina; Mere koje treba da se preduzmu na nacionalnom nivou – materijalno i procesno pravo; Međunarodna saradnja; i Završne odredbe.

Prvo poglavlje Konvencije ima samo jedan član i daje kratak pregled i definicije osnovnih termina koji su upotrebljeni u daljem tekstu. Tako se pod „računarskim sistemom“ podrazumeva grupa povezanih uređaja, od kojih najmanje jedan može da izvodi automatsku obradu podataka; „računarski podatak“ je svaka činjenica, odnosno informacija koja se nalazi u formi pogodnoj za obradu u računarskom sistemu, uključujući i programe koji se mogu upotrebljavati za vršenje određenih funkcija računara; izraz „provajder“ (davalac usluge) ima dvostruko značenje: pod njime može da se podrazumeva svako fizičko ili pravno lice koje pruža usluge omogućavanja komunikacije putem računarske mreže, ali i svako lice koje čuva, odnosno procesuira računarske podatke nastale za vreme takve komunikacije, odnosno upotrebe uređaja; konačno, izraz „podatak u saobraćaju“ podrazumeva svaki računarski podatak koji je vezan za komunikaciju unutar računarskog sistema ili je nastao kao deo takve komunikacije, i nosi informaciju o poreklu i odredištu komunikacije, njenom putu, datumu, vremenu, veličini i trajanju, ili vrsti usluge.[17]

Drugo poglavlje Konvencije podeljeno je na više delova i pokriva različite materijalnopravne i procesnopravne mere koje se države potpisnice obavezuju da će uvesti u nacionalno zakonodavstvo. Svrha materijalnopravnih odredaba je da unapredi sredstva prevencije i kažnjavanja krivičnih dela koja su izvršena upotrebom savremenih tehnologija, odnosno povezana sa upotrebom računara i računarskih mreža. Pri tom, Konvencija treba da uspostavi minimum zajedničkih standarda kada je reč o inkriminisanju tih dela. Na taj način se stvara osnova za saradnju između nadležnih organa država, kao i za razmenu iskustava. Takođe, ovakav pristup će eliminisa-

[17] Član 1 Konvencije.

ti mogućnost da se u slučaju eventualne ekstradicije počinioca stavi prigovor nedostatka dvostruke inkriminacije.[18]

Prva grupa inkriminisanih dela visokotehnološkog kriminala može da se označi kao dela protiv računara i računarskih sistema u užem smislu. Konvencija o visokotehnološkom kriminalu Saveta Evrope ovu grupu naziva „Krivična dela protiv poverljivosti, celovitosti i dostupnosti računarskih podataka i sistema“, i u nju svrstava sledeća dela[19]:

Nezakonit pristup informacijama sadržanim na računaru ili računarskom sistemu, u nameri da se te informacije prisvoje, izmene ili unište. Za ovo delo se, dakle, traži *namera*, tako da je državama potpisnicama ostavljena mogućnost da inkriminišu samo posebne radnje koje dovode do ilegalnog pristupa nekom računaru ili mreži. Tipičan primer ovakvog dela je postavljanje „trojanaca“ u nečiji računar. „Trojanci“ (engl. *trojans*) ispoljavaju se pre svega kao forma nenasilnog preuzimanja kontrole nad tuđim računarom, čega njegov vlasnik najčešće nije svestan. „Trojanac“ ne može sam da se aktivira, već to *čini korisnik računara koji je napadnut* u ubeđenju da instalira autorizovan program, ili neku drugu aplikaciju za rad na računaru (otuda analogija sa trojanskim konjem). Slično „trojancima“ deluju i „logičke bombe“, štetni programi poput virusa, ali bez mogućnosti samostalnog izvršavanja,

[18] *Convention on Cybercrime – Explanatory Report*, *loc. cit.*, str. 8.
[19] Članovi 2-6 Konvencije.

sve dok ne dobiju komandu od korisnika napadnutog računara, koja se najčešće sastoji u pokretanju određenog programa.

Nezakonito presretanje privatnih podataka koji se prenose na bilo koji način između dva računara (ili mreže). Ovde Konvencija ostavlja mogućnost državama da ovako definisano delo ograniče postojanjem namere. Kao i u prethodnom slučaju, ova činjenica je bitna pre svega zbog mogućnosti da neko bez svog znanja, ili bar bez ikakve namere, dođe u posed tuđih podataka na računarskoj mreži.

Izmena podataka (ometanje podataka i ometanje sistema) na računaru, u smislu namernog potpunog ili delimičnog oštećenja, brisanja, promene sadržine, kompresije i bilo kog drugog načina izmene originalnih podataka. Ovo delo možda na prvi pogled izgleda slično *nezakonitom pristupu*, ali se mora shvatiti pre svega kao njemu komplementarno: nelegalni pristup (u nameri da se izmene podaci) omogućava izvršenje samog dela izmene podataka. I ovde Konvencija ostavlja mogućnost sužavanja dometa inkriminacije – države mogu izmenu podataka smatrati krivičnim delom samo ako je pričinjena veća šteta. Postupci opisani u delu nelegalnog pristupa, kao što su „trojanci“ i „logičke bombe“, zapravo kao krajnji cilj imaju izmenu podataka na računaru, ili njihovo slanje autoru štetnog programa (radi dalje zloupotrebe, najčešće preuzimanja identiteta napadnutog računara).

Na delo izmene podataka nadovezuje se *upad u računarsku mrežu*, koji je na potpuno isti način definisan, ali se odnosi na sistem računara čiji se rad onemogućava ili menja nelegalnim pristupom i izmenom podataka na mreži. Ovo delo se sreće u mnogim nacionalnim zakonodavstvima kao *uskraćivanje usluga* (misli se na usluge odgovarajuće računarske mreže zbog nelegalnog upada u njene podatke).

Zloupotreba uređaja je specifično delo koje veoma dobro oslikava sa kakvim se problemima nacionalni zakonodavci ili međunarodna zajednica mogu susresti u pokušajima da definišu sva dela visokotehnološkog kriminala. Zloupotreba uređaja je složeno krivično delo, koje pokušava da pomiri načelo *nulla crimen, nulla poena, sine lege* i faktičko „bujanje“ najrazličitijih krivičnih dela koja su vezana za savre-

Izmena podataka (ometanje podataka i ometanje sistema) na računaru, u smislu namernog potpunog ili delimičnog oštećenja, brisanja, promene sadržine, kompresije i bilo kog drugog načina izmene originalnih podataka.

Zloupotreba uređaja *je specifično delo koje veoma dobro oslikava sa kakvim se problemima nacionalni zakonodavci ili međunarodna zajednica mogu susresti u pokušajima da definišu sva dela visokotehnološkog kriminala.*

mene tehnologije. Zato generalnom odredbom države potpisnice preuzimaju na sebe obavezu da kazne svaku namernu ilegalnu proizvodnju, posedovanje, upotrebu ili nabavku, prodaju, kao i svaki drugi oblik distribucije i činjenja dostupnim nekome ko na to inače nema prava, bilo kog „uređaja“ pod kojim se podrazumevaju i računarski programi, kao i bilo koji oblik podataka pomoću kojih se mogu izvršiti krivična dela navedena u prethodnim članovima Konvencije. Imajući u vidu revolucionarnost, a verovatno i neodređenost ove odredbe, pisci Konvencije, ipak, dopuštaju državama da stave rezervu na ovaj član, osim kada je reč o prodaji ili drugom obliku distribucije lozinki ili drugih računarskih podataka pomoću kojih se mogu počiniti navedena dela. Na ovaj način se „uređaji“ možda i nepravedno stavljaju u drugi plan, ali se i državama ostavlja da same odrede domašaj pomenutog principa da nema kažnjavanja bez (jasno) inkriminisanog krivičnog dela.

Ovakav pokušaj Saveta Evrope je u svakom slučaju u skladu sa rastućom opasnošću od visokotehnološkog kriminala, a istovremeno zadovoljava i kriterijume koje smo naveli – na generički način sažeti veliku grupu protivpravnih radnji u nekoliko složenih krivičnih dela, čije su inkriminacije dovoljno precizne da mogu poslužiti nacionalnim zakonopiscima, a istovremeno ostavljaju dovoljno slobode budućoj praksi da odredi granice njihovog domašaja bez stvaranja pravne nesigurnosti. Ovo možda ne može da se primeni i na pojam „uređaja“, ali je više nego jasno da je u ovom slučaju reč o maštovitom pristupu u cilju da se pravo približi realnosti i da se na neki način premosti očigledna razlika između dinamike razvoja pravnih akata i tehničko-tehnoloških mogućnosti za njihovo kršenje, koja sada postoji.

Druga grupa inkriminisanih dela mogla bi da se označi kao visokotehnološka varijanta klasičnih krivičnih dela. Ova sekcija Konvencije obuhvata dva dela: falsifikovanje i prevaru.[20]

[20] Članovi 7 i 8 Konvencije.

Falsifikovanje se odnosi samo na umišljajno, neovlašćeno ubacivanje, brisanje, izmenu ili sakrivanje računarskih podataka, koje rezultira izmenjenim sadržajem tih podataka, bez obzira na to da li oni na ovaj način dobijaju drugu svrhu i smisao, ili postaju neupotrebljivi. Državama je ostavljena mogućnost da predvide i posebnu vrstu namere da se učini prevara da bi postojalo ovo krivično delo.

Prevara je definisana kao umišljajno, neovlašćeno ubacivanje, brisanje, izmena ili sakrivanje računarskih podataka, kao i svako drugo mešanje u rad računarskog sistema, u cilju da se pribavi protivpravna imovinska korist za sebe ili treće lice.

Falsifikovanje se odnosi samo na umišljajno, neovlašćeno ubacivanje, brisanje, izmenu ili sakrivanje računarskih podataka, koje rezultira izmenjenim sadržajem tih podataka, bez obzira na to da li oni na ovaj način dobijaju drugu svrhu i smisao, ili postaju neupotrebljivi.

Prevara je definisana kao umišljajno, neovlašćeno ubacivanje, brisanje, izmena ili sakrivanje računarskih podataka, kao i svako drugo mešanje u rad računarskog sistema, u cilju da se pribavi protivpravna imovinska korist za sebe ili treće lice.

Treći segment drugog poglavlja bavi se delima koja su vezana za sadržaj komunikacije na računarskoj mreži, ali on takođe ima samo jedan član posvećen velikom problemu internet komunikacije – dečjoj pornografiji.[21]

Države potpisnice se obavezuju da kao krivično delo inkriminišu u domaćim zakonodavstvima sledeće aktivnosti: proizvodnju dečje pornografije u cilju njenog distribuiranja kroz računarski sistem; nuđenje ili činjenje dostupnim dečje pornografije kroz računarski sistem; distribuciju ili slanje dečje pornografije kroz računarski sistem; nabavljanje dečje pornografije za sebe ili drugoga putem računarskog sistema; posedovanje dečje pornografije na računarskom sistemu ili na medijumu za prenos računarskih podataka. Dakle, praktično je inkriminisano svako ponašanje vezano za dečju pornografiju, uključujući i pribavljanje i posedovanje, što čini značajnu razliku u odnosu na bića sličnih krivičnih dela vezanih za kršenje autorskih prava putem računarske mreže.

Države potpisnice se obavezuju da kao krivično delo inkriminišu u domaćim za-konodavstvima sledeće aktivnosti: proizvodnju dečje pornografije u cilju njenog distribuiranja kroz računarski sistem; nuđenje ili činjenje dostupnim dečje pornografije kroz računarski sistem; distribuciju ili slanje dečje pornografije kroz računarski sis-tem; nabavljanje dečje pornografije za sebe ili drugoga putem računarskog sistema; posedovanje dečje pornografije na računarskom sistemu ili na medijumu za prenos računarskih podataka.

Evropska konvencija o visokotehnološkom kriminalu, uvidevši ozbiljnost i rasprostranjenost ovog problema, pokušava da autoritativno navede države da harmonizuju svoja zakonodavstva i na taj način doprinesu njegovom suzbijanju. Ne samo što su sve države u obavezi da inkriminišu različite oblike proizvodnje, posedovanja i distribucije dečje pornografije već Konvencija sadrži i neke odredbe koje su daleko obuhvatnije od svih uporednih rešenja u nacionalnim zakonodavstvima. Tako je najpre starosna granica osoba koje se smatraju decom postavljena na 18 godina, uz mogućnost da države individualno odluče da je smanje na 16 godina. Potom su inkriminisani sadržaji u kojima se pojavljuju osobe za koje se može osnovano pretpostaviti da su mlađe od 18 godina, ili se predstavljaju kao takve, kao i drugi grafički sadržaji (crteži, crtani filmovi i sl.) u kojima se predstavljaju osobe mlađe od propisane granice u pornografskom kontekstu. Ipak, verovatno uvidevši da većina nacionalnih zakonodavstava ne predviđa ovakve inkriminacije, Konvencija ostavlja

[21] Član 9 Konvencije.

mogućnost stavljanja rezervi na takva rešenja, čime se svakako ne doprinosi unifikaciji zakonodavstava u ovoj oblasti, a ni efikasnijem suzbijanju dečje pornografije i eksploatacije dece na internetu.

Četvrti segment ovog poglavlja posvećen je delima kršenja autorskih i srodnih prava i takođe je sadržan u jednom članu Konvencije.[22] U tri stava, kršenje autorskih prava se ne inkriminiše samostalno, nego putem definicija sadržanih u već postojećim međunarodnim ugovorima.

Konačno, poslednji članovi drugog poglavlja koji govore o materijalnom pravu grupisani su u peti podnaslov i bave se inkriminacijom pokušaja izvršenja, pomaganja i podstrekavanja za navedena dela, odgovornosti pravnih lica i propisivanju sankcija za počinjena dela iz Konvencije.[23]

---

[22] Član 10 Konvencije.

[23] Članovi 11-13 Konvencije. Članom 12 predviđena je krivična, građanska i administrativna odgovornost pravnog lica, kao i posebna krivična odgovornost samih počinilaca dela. Da bi se pravno lice moglo smatrati odgovornim za krivično delo iz Konvencije, ono mora biti počinjeno u njegovu korist, a izvršilac (saizvršilac, pomagač, podstrekač) tog dela mora biti jedan od funkcionera pravnog lica. Sam pojam „lice koje ima rukovodeću ulogu u pravnom licu“ (prema originalnom tekstu Konvencije – *person who has a leading position*) određuje se prema tri karakteristike, odnosno tri vrste ovlašćenja koja mora posedovati: ovlašćenja da predstavlja pravno lice, ovlašćenja da donosi obavezujuće odluke u ime pravnog lica i ovlašćenja da vrši nadzor (odnosno obavlja poslove kontrole) unutar pravnog lica. Ovo je od izuzetnog značaja u praksi za eventualno ustanovljavanje odgovornosti pravnog lica kod ove vrste krivičnih dela, čije se radnje izvršenja mogu veoma specifično manifestovati – naime, pravno lice neće biti oglašeno krivim kada krivično delo počini neko ko koristi njegove računarske kapacitete, bez obzira na koji način je došao do njih – legalnim putem (npr. iznajmljivanjem) ili ilegalnim putem (neovlašćenim preuzimanjem kontrole nad računarom ili ubacivanjem u računarsku mrežu). Opširnije: *Convention on Cybercrime – Explanatory Report*, *loc. cit.*, str. 23-24.

Drugi deo drugog poglavlja pod nazivom „Procesno pravo“ bavi se procesnim ovlašćenjima državnih organa prilikom istraživanja krivičnih dela vezanih za nove tehnologije.[24] Konvencija uvodi stare instrumente procesuiranja krivičnih dela u novoj sredini, poštujući specifičnu prirodu sajber prostora.

Osim opštih odredaba koje nalažu državama da u svoje krivično pravo uvedu pomenuta krivična dela, kao i druga dela koja se ne nalaze u tekstu Konvencije a koja mogu da se podvedu pod ovu grupu, velika pažnja se posvećuje načinu prikupljanja podataka koji se nalaze na računarima ili prenosnim uređajima, kao i zaštiti osnovnih prava pojedinca garantovanih Evropskom konvencijom o ljudskim pravima i paktovima o ljudskim pravima UN.[25]

Prema Konvenciji, nadležni državni organi imaju ovlašćenja da pregledaju i zaplene svaki računar ili nosač podataka na kome se nalaze, ili sumnjaju da se mogu nalaziti inkriminišući materijali, kao i da od provajdera elektronskih komunikacija prikupljaju podatke koji se odnose pre svega na upotrebu interneta i kreditnih kartica, preko kojih se može doći do imena ili IP adrese potencijalnog počinioca krivičnog dela.[26]

Prema Konvenciji, nadležni državni organi imaju ovlašćenja da pregledaju i zaplene svaki računar ili nosač podataka na kome se nalaze, ili sumnjaju da se mogu nalaziti inkriminišući materijali, kao i da od provajdera elektronskih komunikacija prikupljaju podatke koji se odnose pre svega na upotrebu interneta i kreditnih kartica, preko kojih se može doći do imena ili IP adrese potencijalnog počinioca krivičnog dela.

Jedna od verovatno najdalekosežnijih odredaba tiče se tzv. „presretanja podataka“, odnosno neke vrste prisluškivanja elektronskih komunikacija, pre svega onih vezanih za internet (član 21 Konvencije). Do ove mere će doći kada je za dokazivanje o postojanju krivičnog dela potrebno imati dokaze sakupljene u, kako se kaže u Konvenciji, „realnom vremenu“, odnosno u trenutku kada se komunikacija odigrava.[27] Ova oblast intervencije državnih organa je i najosetljivija, jer se praktično povređuje pravo na privatnost i pravo na prepisku, a sama Konvencija ne sadrži odgo-

[24] Članovi 14-22 Konvencije.
[25] Član 15 Konvencije.
[26] Članovi 19 i 20 Konvencije.
[27] Nasuprot tome je mera zaplene postojećih dokaza koji su ranije snimljeni na računaru ili drugom medijumu za čuvanje i prenos podataka, koju Konvencija takođe predviđa.

varajuća ograničenja i garantije da takva prava neće biti zloupotrebljena (osim generalnog ograničenja da se pri izvršenju svih mera moraju poštovati međunarodni standardi ljudskih prava postignuti kroz pomenute međunarodne dokumente). Član 21, koji reguliše presretanje podataka, navodi da će se ova mera preduzeti za „ozbiljna dela“, ali se iz same Konvencije ne može uvideti na koja se dela tačno mislilo i koje bi karakteristike mogle neko delo odrediti kao „ozbiljno“. Ovako formulisan, član 21 zapravo ostavlja državama potpisnicama da same odrede kada će se primenjivati ovakve mere, što i pored garantija u međunarodnim dokumentima o ljudskim pravima i slobodama, može da dovede do zloupotrebe ovlašćenja državnih organa. Štaviše, stav 3 pomenutog člana određuje da države moraju propisati uslove pod kojima će provajderi, koji nužno moraju da učestvuju u sakupljanju ovakvih informacija, činjenicu da se određeni korisnik špijunira, kao i sadržinu podataka prikupljenih na taj način, morati da čuvaju kao tajnu. Kada se posmatraju istrage koje mogu da dovedu do jednog ili više izvršilaca krivičnih dela kao što su prevara, terorizam, zlostavljanje dece, ovakva procedura je opravdana i jedina moguća. Problem je što Konvencija ne poseduje mehanizme zaštite, kako se ona ne bi sprovodila za elektronske komunikacije preko računara i računarskih mreža osoba koje nisu počinioci, niti su pod istragom za vršenje dela visokotehnološkog kriminala, već se mogu naći na udaru vlasti jedne zemlje iz sasvim drugih pobuda, koje veoma često nisu ni pravno utemeljene.

Ipak, ne treba previše kritikovati ovo rešenje, s obzirom na to da je reč o međunarodnom instrumentu, koji treba da zaživi kroz legislativu i praksu svake pojedinačne zemlje.[28] U tom smislu je zanimljivo i tumačenje nastanka ove odredbe, kao i njenog domašaja. Naime, prema tvorcima teksta Konvencije, ova odredba, kao i sve ostale odredbe Konvencije koje se tiču procesnog prava, isključivo su usmerene na

[28] Što se u komentaru ovog rešenja izričito i navodi. *Convention on Cybercrime – Explanatory Report*, *loc. cit.*, str. 44.

prikupljanje podataka (u smislu dokaza) u krivičnim istragama ili krivičnom postupku. Međutim, Konvencija ne predviđa automatsko prikupljanje i snimanje podataka od strane provajdera, koje bi oni mogli po potrebi da ustupe policiji ili drugim nadležnim organima, već samo ciljano sakupljanje nakon što za to dobiju nalog od organa koji sprovodi istražni ili krivični postupak. Zašto se odustalo od prvobitnog rešenja? Prema rečima tvoraca Konvencije, nije postojao konsenzus da bi se ovo pitanje uredilo na takav način[29] – može na to da se doda, iz očiglednih razloga da bi se zahtevanjem od provajdera da sakupljaju sve podatke koji su u vezi sa aktivnostima njihovih klijenata i čuvaju ih određeni period, ozbiljno ugrozilo pravo na privatnost svakog korisnika, koje on mora da poseduje bez obzira na to kakvo sredstvo komunikacije upotrebljavao – pismo, telefon ili elektronsku poštu.

Član 22 Konvencije bavi se nadležnošću države potpisnice kada dođe do činjenja nekog od krivičnih dela iz Konvencije. Država će imati nadležnost za procesuiranje ukoliko je krivično delo počinjeno na njenoj teritoriji, na brodu ili avionu koji nosi njenu zastavu, kao i ako je krivično delo počinio državljanin te države, pod uslovom da je ono u drugoj državi koja poznaje istu takvu inkriminaciju, ili van državnih teritorija (npr. na slobodnom moru).[30] Može se reći da kombinacija teritorijalno-personalne jurisdikcije nije najsrećnije rešenje, iako je reč o klasičnom instrumentu kada su u pitanju međunarodni ugovori. Ipak, visokotehnološki kriminal izmiče klasičnim obrascima krivičnih dela, pa i krivične nadležnosti, tako da ovakva formulacija ostavlja niz otvorenih pitanja, o čemu će više reči biti kasnije. Situaciju dalje komplikuje stav 2 istog člana, koji omogućava državama da ne primenjuju pravila o nadležnosti u određenim slučajevima ili pod određenim okolnostima. Kao da su i tvorci Konvencije bili svesni slabašnog dometa ovog rešenja, stavovi 3 i 4 pokušavaju da stvari postave na malo čvršćim osnovama – ako država ne izvrši ekstradici-

Država će imati nadležnost za procesuiranje ukoliko je krivično delo počinjeno na njenoj teritoriji, na brodu ili avionu koji nosi njenu zastavu, kao i ako je krivično delo počinio državljanin te države, pod uslovom da je ono u drugoj državi koja poznaje istu takvu inkriminaciju, ili van državnih teritorija (npr. na slobodnom moru).

[29] *Convention on Cybercrime – Explanatory Report*, *loc. cit.*, str. 25.
[30] Član 22, stav 1 Konvencije.

ju svog državljanina, mora da mu sudi za počinjena dela na teritoriji druge države potpisnice;[31] takođe, odredbe o nadležnosti države sadržane u Konvenciji neće derogirati odredbe domaćeg prava, prema kojem država može i na neki drugi način uspostaviti svoju krivičnu nadležnost.

Treći deo Konvencije bavi se međunarodnom saradnjom država na suzbijanju visokotehnološkog kriminala, i to pre svega na način koji bi trebao da prevaziđe praktične prepreke pri sprovođenju nacionalnog zakonodavstva za krivična dela koja po pravilu prelaze državne granice, a često i podrazumevaju učešće pojedinaca iz nekoliko zemalja širom sveta.[32]

Otuda su glavne odredbe ovog dela posvećene saradnji država na organizovanoj ili spontanoj razmeni podataka[33] koji se tiču eventualnog izvršenja nekog od krivičnih dela vezanih za upotrebu elektronskih komunikacija, kao i mogućnosti ekstradicije počinilaca takvih dela iz jedne države potpisnice u drugu. Svaka država potpisnica mora određenom telu da poveri posao saradnje sa drugim državama u oblasti visokotehnološkog kriminala, a u slučaju hitnosti, saradnja može da bude uspostavljena i direktno između pravosudnih organa dve države, kao i preko Interpola i drugih relevantnih kanala saradnje, dakle bez dugih procedura koje bi išle preko centralnih vlasti država a koje su predviđene kao pravilo pri saradnji u ovoj oblasti.[34] Prema članu 31 Konvencije, svaka država potpisnica može da traži od druge da sprovede određene istražne radnje na svojoj teritoriji, ako je to neophodno za vršenje istrage u vezi sa nekim od dela predviđenih Konvencijom. Ukupno gledano, Konvencija predviđa različite vidove saradnje država, prilagođene tehnologiji vršenja istraga i procesuiranja ove vrste krivičnih dela. Takođe, državama je ostavljeno

[31] Na ovaj slučaj se primenjuje i odredba sadržana u članu 24, stav 6.
[32] Članovi 23-35 Konvencije.
[33] Videti član 26 Konvencije.
[34] Član 27, stav 9 Konvencije.

dosta prostora da u praksi, ili dodatnim bilateralnim sporazumima, dalje preciziraju one vrste saradnje za koje imaju poseban interes.

Kada je o ekstradiciji reč, treba posvetiti pažnju izuzecima – kada država neće biti u obavezi da izruči neko lice. To je pre svega slučaj kada je u pitanju nedostatak dvostruke inkriminacije, ali Konvencija predviđa i dopunski uslov – delo mora da bude označeno kao ozbiljno u samom zakonu, odnosno za njegovo izvršenje mora da bude zaprećena minimalna kazna od jedne godine zatvora, ako nije drugačije predviđeno nekim drugim međunarodnim ugovorom između država u pitanju, koji se može primeniti na datu situaciju.[35] Takođe, između država koje nemaju međusobne bilateralne ili multilateralne ugovore o ekstradiciji, Konvencija će služiti kao osnov za ekstradiciju.

Zanimljiva je i odredba koja se tiče osnivanja „mreže 24/7“ u svakoj od država, koja bi služila kao podrška policijskim i drugim organima, kao kontakt za sva obaveštenja i početna tačka za sve zahteve koji se tiču procesuiranja i istraživanja krivičnih dela visokotehnološkog kriminala.[36] Ovo rešenje se nastavlja na neki način, odnosno ima isti cilj kao odredba iz člana 27, stav 2. Konvencije, koja predviđa angažovanje posebnog državnog organa za saradnju sa drugim državama potpisnicama. Opet, nema reči o specijalizaciji takvog tela – saradnja na polju visokotehnološkog kriminala može da bude samo jedan od aspekata njegovog rada. Ove mere su pokušaj da se ublaži jedan od nedostataka ove Konvencije – državama potpisnicama nije data obaveza da uvedu posebne organe koji bi se bavili isključivo ovom vrstom krivičnih dela. S obzirom na nužnost specijalizacije policijskih, istražnih, tužilačkih, sudskih i drugih organa pri istraživanju i procesuiranju, čini se da će države morati i bez konkretnih odredaba Konvencije da učine mnogo više od osnivanja „mreže 24/7“ da bi se efikasno suprotstavile sajber kriminalcima.

[35] Član 24, stav 1 Konvencije.
[36] Član 35 Konvencije.

Ova Konvencija je specifična i po jednom nimalo pozitivnom aspektu, a to je da je razvijene države veoma nerado ratifikuju. Od zemalja koje možemo nazvati visokorazvijenim kada je reč o savremenim tehnologijama, ratifikovale su je samo SAD 2006. godine, Francuska, Danska i Norveška. Otkuda ovaj otpor? Pre svega zbog pomenutih procesnih ovlašćenja državnih organa, koje Konvencija predviđa i gotovo ne ograničava. EFF[37] je zato naziva „najgorim internet pravom na svetu“, koje predviđa da čak i akti koji nisu predviđeni kao krivična dela u SAD mogu da budu gonjeni u ovoj zemlji po zahtevu neke druge države u kojoj se smatraju kažnjivim.[38] Ovaj problem postaje još dublji kada je reč o interpretaciji šta se, npr. može smatrati nedozvoljenim sadržajem na internetu koji ne pokriva sloboda izražavanja – standardi u demokratskim i nedemokratskim zemljama u tom slučaju se znatno razlikuju.[39] Činjenica je da se ovakva kategorizacija Konvencije ne može u potpunosti opravdati, ali veoma dobro ilustruje strah od „sudara“ potpuno različitih kultura, civilizacija i vrednosti na internetu. Stoga možda i nedostatak relevantnog međunarodnog do-

[37] EFF (*Electronic Frontier Foundation*) jedna je od najpoznatijih organizacija koja se bavi zaštitom privatnih podataka u odnosu na nove tehnologije. Više informacija o EFF-u na internet adresi: *http://www.eff.org*, 01.05.2009.

[38] Reč je o aktima za koje Konvencija predviđa mogućnost uvođenja u nacionalno zakonodavstvo. Teorijski je moguće da država ne izjavi rezervu na prihvatanje saradnje kada je reč o svim delima predviđenim Konvencijom, a istovremeno neka od njih ne uvede u svoje zakonodavstvo, čime stvara ovakvu donekle apsurdnu situaciju, jer je obavezana da goni počinioca koji je delo učinio na njenoj teritoriji a koga ne želi da izruči drugoj državi (član 22, stav 1, tačke a-c; član 22, stav 3 Konvencije) ili čak kada je reč o domaćem državljaninu koji ne ispunjava uslove za ekstradiciju iz člana 24, stav 1, tačka a, koji se upravo tiču dvostruke inkriminacije. Naravno, u svakom slučaju se država može pozvati samo na član 24, stav 1, tačka a, čime će ovaj teorijski problem u praksi biti prevaziđen, a u svakom slučaju se može primeniti i član 24, stav 6, koji predviđa procesuiranje prema inkriminaciji krivičnog dela slične prirode.

[39] Izvor: Nate Anderson, *World's Worst Internet Law*, *http://arstechnica.com/news.ars/post/20060804-7421.html*, 01.05.2009.

kumenta koji bi bio prihvaćen kako na globalnom nivou, tako i od strane najrazvijenijih država sveta.

Dodatni protokol uz Konvenciju o visokotehnološkom kriminalu, koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema, donet je 2003. godine a stupio na snagu 1. marta 2006. godine.[40] Od zemalja u okruženju, ratifikovale su ga Albanija, Bosna i Hercegovina, Hrvatska i Makedonija. Rumunija i Crna Gora su potpisale Protokol, ali ga još nisu ratifikovale.[41]

Kao što sam naziv ovog dokumenta kaže, osnovna svrha njegovog donošenja jeste da se inkriminišu ponašanja koja nisu obuhvaćena Konvencijom, a koja se tiču širenja mržnje, netolerancije i netrpeljivosti prema rasnim, nacionalnim, verskim i drugim grupama i zajednicama, korišćenjem računara kao sredstva komunikacije i širenja propagande. I zaista, razvoj računarskih mreža, a naročito porast dostupnosti i popularnosti interneta i imejl servisa, učinili su računar moćnim sredstvom širenja različitih ideja, koje mogu da budu korisne i edukativne, ali isto tako, npr. i poziv na veličanje nacističkih tekovina, uperene na bojkotovanje, ili otvoreni poziv na linč pojedinaca ili grupa koje se razlikuju po svojim ličnim karakteristikama od drugih grupa u svojoj sredini. Ovi akti su vrlo opasni jer se njihovo širenje ne može adekvatno kontrolisati – svako ima pravo mišljenja i izražavanja mišljenja, a kada se to pravo zloupotrebi na internetu ili nekoj drugoj mreži, korišćenjem računara, često ne može pravovremeno i adekvatno da se reaguje kako bi se zloupotreba sprečila. Otuda je Protokol pre svega usmeren na retribuciju, odnosno inkriminaciju i kažnjavanje ovakvih ispada, bez obzira na to da li se njima širi mržnja, ili se istorijske či-

[40] Tekst Protokola (na engleskom jeziku) na internet adresi: *http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm*, 01.05.2009.

[41] Srbija i Crna Gora su potpisale Protokol 7.04.2005. godine. Lista ratifikacija može se naći na internet adresi: *http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=189&CM=&DF=&CL=ENG*, 01.05.2009.

njenice predstavljaju na neistinit način, ili se nekim drugim sredstvima diskriminiše ili nipodaštava određena etnička, rasna, verska grupa ili organizacija koja ih predstavlja.

I sami autori Protokola se još u preambuli pozivaju na Evropsku konvenciju o ljudskim pravima i osnovnim slobodama, Protokol 12 uz Evropsku konvenciju, kojim se zabranjuje svaki vid diskriminacije pojedinaca ili grupa na osnovu njihovih zaštićenih ličnih svojstava, i Konvenciju o eliminaciji svih oblika rasne diskriminacije, donetu 1965. u okviru Ujedinjenih nacija.

U relativno kratkom tekstu, Protokol uvodi obavezu za države potpisnice da u nacionalnom zakonodavstvu inkriminišu sledeća ponašanja:[42]

Širenje rasističkog i ksenofobičnog materijala preko računarskih sistema podrazumeva svaku radnju kojom se ovakav materijal čini dostupnim javnosti, korišćenjem računara, odnosno računarskog sistema. Materijal se može učiniti dostupnim na različite načine, kao što je njegovo slanje na veliki broj imejl adresa ili postavljanje na internet prezentaciju. Državama je ostavljena sloboda da li će ovakav postupak povući krivičnu odgovornost ili ne, kao i da stave rezervu na one oblike ponašanja koji su prema njihovom unutrašnjem pravu dozvoljeni kao vid izražavanja slobode govora.

Pretnja motivisana rasizmom ili ksenofobijom predstavlja stavljanje u izgled pojedincu ili grupi da će prema njima biti izvršeno neko teško krivično delo, kako je definisano u domaćem zakonodavstvu država, korišćenjem računara ili računarskih sistema. Pojedinac ili grupa treba da se izdvajaju prema svojoj rasi, boji kože, poreklu, nacionalnoj, etničkoj ili verskoj pripadnosti, da bi ovo delo imalo specifičan oblik predviđen Protokolom.

Uvreda motivisana rasizmom ili ksenofobijom ima iste elemente kao prethodno delo, samo nije reč o pretnji, nego o vređanju pojedinca ili grupe, zasnovanom na

Širenje rasističkog i ksenofobičnog materijala preko računarskih sistema podrazumeva svaku radnju kojom se ovakav materijal čini dostupnim javnosti, korišćenjem računara, odnosno računarskog sistema.

Pretnja motivisana rasizmom ili ksenofobijom predstavlja stavljanje u izgled pojedincu ili grupi da će prema njima biti izvršeno neko teško krivično delo, kako je definisano u domaćem zakonodavstvu država, korišćenjem računara ili računarskih sistema.

[42] Članovi 3-6 Protokola.

rasi, boji kože, poreklu, nacionalnoj, etničkoj ili verskoj pripadnosti. Država može da stavi rezervu na ovaj član i ne primenjuje ga, ili može da ograniči inkriminaciju samo na one uvrede kojima se širi mržnja, ili se pojedinac ili grupa ponižavaju ili izvrgavaju podsmehu. Ostaje nejasno zašto je državama data sloboda da ovo delo ne označe kao kažnjivo ponašanje.

Poricanje, značajno umanjenje, odobravanje ili opravdanje genocida ili zločina protiv čovečnosti uvodi zanimljiv koncept kažnjavanja za navedene radnje učinjene putem računara ili računarskih sistema, ako je reč o slučajevima koji su bili predmet odlučivanja od strane međunarodnih sudova, počev od Međunarodnog vojnog tribunala 1945. godine i nadalje. Kao i kod prvog navedenog dela u Protokolu, ovakav sadržaj mora na neki način da se učini dostupnim javnosti, dakle većem broju ljudi koji koriste računar i internet ili drugu računarsku mrežu.

Rešenja o implementaciji, procesnim radnjama i međunarodnoj saradnji, koja sadrži Konvencija, shodno se primenjuju i na dela utvrđena Protokolom.

Konvencija o zaštiti prava pojedinca u vezi sa automatskom obradom ličnih podataka[43]

Konvencija je otvorena za potpisivanje državama članicama 28. januara 1981. godine a na pravnu snagu je stupila 1. oktobra 1985. godine. Osnovni cilj usvajanja ove konvencije jeste jačanje pravne regulative na polju zaštite podataka o ličnosti usled dramatičnog porasta upotrebe računarske tehnologije u administrativne svrhe. Osnovano se pošlo od pretpostavke da je u modernim društvima donošenje mnogobrojnih odluka koje se tiču ostvarivanja prava pojedinaca bazirano na informacijama i podacima pohranjenim u računarima i računarskim sistemima (socijalna i medicinska zaštita, podaci o zdravstvenom stanju pojedinaca, podaci neophodni

[43] „Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data“ (ETS No.108, the 28 January 1981, Entry into force: 1.10.1985).

za obračun i isplatu zarada itd.). Zbog navedenog, ukazuje se kao neophodno da se licima koja imaju pristup ovim informacijama uskrati i onemogući zloupotreba ili bilo kakva nezakonita upotreba ovih podataka. Konačno, uočeno je da nacionalna zakonodavstva država članica ne pružaju dovoljan nivo zaštite građanima u ovoj oblasti, naročito kada su u pitanju mehanizmi koji bi omogućili efikasnu kontrolu građana ličnim podacima koje o njima prikupljaju i koriste državni organi i druga pravna lica.

Dalje, došlo se i do saznanja da postoji problem u tzv. „prekograničnom protoku informacija“ pa se postavilo i pitanje zaštite prava pojedinca i u ovim slučajevima. Sa jedne strane, razvoj računarskih tehnologija i telekomunikacionih uređaja omogućava lakši i brži protok elektronskih podataka i relativizuje činioce kao što su razdaljina, vreme, jezik i cena, koji su ranije predstavljali prepreku u efikasnom protoku podataka. U pojedinim oblastima poslovanja i života, kao što su pružanje bankarskih usluga, turizam ili upotreba kreditnih i platnih kartica, efikasan prekogranični protok elektronskih podataka pokazuje se kao neophodan. Sa druge strane, kvalitet zaštite podataka o ličnosti slabijeg je kvaliteta kako se posmatrani prostor širi u geografskom smislu.

Zbog svega navedenog, a u cilju efikasne zaštite podataka o ličnosti koji se automatski obrađuju, usvojena je Konvencija koja se sastoji od tri osnovna poglavlja.

Najpre, definisan je opseg važenja Konvencije, u smislu da se ona odnosi na lične podatke prikupljene kako u javnom, tako i u privatnom sektoru.

Centralni i suštinski deo Konvencije jeste drugo poglavlje u kome su sadržane materijalne odredbe u formi osnovnih principa koji se tiču: 1) kvaliteta podataka koji se prikupljaju (zakonitost u prikupljanju podataka, prikupljanje u svrhe koje su zakonom dozvoljene, tačnost i ažurnost podataka, kao i čuvanje u formi i obliku koji omogućava identifikaciju, član 5 Konvencije), 2) posebnih kategorija podataka (podaci o rasnoj i političkoj pripadnosti, religijskim uverenjima, kao i podaci koji se tiču zdravstvenog stanja, seksualnog opredeljenja i ranije osuđivanosti ne mogu se au-

tomatski prikupljati i činiti dostupnim osim ukoliko zakon ne predviđa posebne mere zaštite u pogledu navedenih podataka, član 6 Konvencije), 3) bezbednosti prikupljenih podataka (obaveza da se primene odgovarajuće mere bezbednosti koje bi onemogućile slučajno ili neovlašćeno uništenje prikupljenih podataka kao i gubitak, neovlašćeni pristup, izmenu ili distribuciju automatski prikupljenih podataka, član 7 Konvencije), 4) dodatnih mera sigurnosti za lica o kojima se podaci automatski prikupljaju (tiču se prava na pristup, odnosno uvid u automatski prikupljene podatke, prava da se zahteva brisanje nezakonito prikupljenih podataka i prava na pravni lek ukoliko ovim zahtevima ne bude udovoljeno, član 8 Konvencije), 5) izuzetaka i ograničenja (prava propisana čl. 5, 6 i 8 ove Konvencije mogu biti ograničena samo zakonom države članice, i to u slučajevima kada je to neophodno radi zaštite bezbednosti države, javnog poretka, monetarnog sistema države, suzbijanja krivičnih dela, kao i kada je to neophodno radi zaštite lica o kome se podaci prikupljaju ili zaštite prava i sloboda drugih lica, član 9 Konvencije). Takođe, svaka država se obavezuje da će u svom nacionalnom zakonodavstvu predvideti odgovarajuće sankcije kako bi se efikasno otklonila bilo kakva povreda ili zloupotreba prava koja je predviđena odredbama Konvencije.

U trećem poglavlju nalaze se odredbe koje se tiču prekograničnog prometa automatski prikupljenih podataka o ličnosti. Suština ovih odredaba jeste da se obezbedi da protok informacija između država članica bude slobodan, odnosno da bude lišen bilo kakvih specijalnih kontrolnih mehanizama ili da bude podvrgnut kakvom režimu dozvola ili odobrenja. Ovo rešenje je logično imajući u vidu da Konvencija propisuje osnovne principe u automatskom prikupljanju informacija koje čine tzv. „zajedničko jezgro“ među državama članicama, tako da nema potrebe za dodatnom regulacijom ili pojedinačnim restrikcijama u prometu podataka o ličnosti (osim onih ograničenja koja su ustanovljena Konvencijom u članu 12, stav 3).

Konačno, u četvrtom i petom poglavlju Konvencije predviđeni su mehanizmi saradnje država ugovornica kako u pojedinim slučajevima koji se odnose na saradnju

nadležnih tela i pomoć licima koja imaju prebivalište u državi ugovornici koja nije njihova matična država, tako i u pogledu pitanja koja se odnose na primenu Konvencije kao takve (kroz konsultativni savet za primenu odredaba Konvencije).

Konvencija o zaštiti dece od seksualne eksploatacije i seksualnog zlostavljanja[44]

Konvencija je usvojena 25. oktobra 2007. godine i potpisale su je zemlje članice Saveta Evrope. U pitanju je vrlo važan međunarodni dokument koji će, nakon što ga zemlje potpisnice ratifikuju, dovesti do toga da krivični postupci u kojima se deca pojavljuju kao žrtve seksualne eksploatacije i zlostavljanja budu efikasniji. Takođe, sa aspekta borbe protiv visokotehnološkog kriminaliteta, ovaj pravni akt predstavlja legislativni iskorak ka harmonizaciji nacionalnih zakonodavstava u pogledu materijalnog krivičnog zakonodavsta u svim onim slučajevima, nažalost brojnim, u kojima se računarske tehnologije i mreže koriste u cilju distribucije, razmene i skladištenja nedozvoljenih sadržaja.

Motivacija za pravno regulisanje ovog pitanja na međunarodnom nivou proističe iz saznanja da su seksualna eksploatacija i zloupotreba dece narasle do zabrinjavajućih proporcija kako na nacionalnom, tako i na međunarodnom nivou, naročito usled rapidnog porasta upotrebe informacionih tehnologija kako od strane dece, tako i od počinilaca krivičnih dela. Navedeno ukazuje na potrebu za efikasnijom saradnjom na međunarodnom nivou, a kao rezultat te potrebe usvojena je Konvencija.

Konvencija detetom smatra svaku osobu mlađu od 18 godina, što je naročito važno imajući u vidu dosadašnja iskustva koja su ukazivala na velike probleme u međunarodnoj saradnji, koji su poticali od činjenice da su razna zakonodavstava na

Konvencija detetom smatra svaku osobu mlađu od 18 godina.

[44] „Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote, 25.10.2007. godine.

Nuđenje ili činjenje dostupnim dečje pornografije podrazumeva, između ostalog, postavljanje nedozvoljenih onlajn sadržaja kako bi se omogućio pristup drugim licima ili pravljenje pornografskih internet sajtova.

različit način definisala pojam deteta (u smislu uzrasta), što je ponekad dovodilo i do nepremostivih prepreka prilikom progona izvršilaca krivičnih dela. Naprosto, dela izvršena prema licima istog uzrasta u različitim državama jednostavno nisu mogla biti kvalifikovana kao dela seksualne eksploatacije i zloupotrebe dece, što je dovodilo do nemogućnosti da se prema počiniocima izreknu odgovarajuće mere i sankcije.

Tematski, Konvencija je podeljena na više poglavlja kao što su: preventivne mere, specijalizovana tela za koordinaciju, mere zaštite i podrške žrtvama, materijalno krivično pravo, istraga, krivični progon i procesne odredbe, objedinjena evidencija o osuđenim licima kao i međunarodna saradnja.

Na ovom mestu zadržaćemo se na članu 20 Konvencije, koji se odnosi na krivična dela dečje pornografije, imajući u vidu da se pojedine odredbe neposredno tiču (zlo)upotrebe računarskih tehnologija. Navedenom odredbom države potpisnice se obavezuju da preduzmu neophodne izmene u nacionalnim zakonodavstvima kako bi se kriminalizovale sledeće protivpravne radnje: proizvodnja dečje pornografije, nuđenje ili činjenje dostupnim dečje pornografije, distribucija ili objavljivanje dečje pornografije, pribavljanje dečje pornografije za sebe ili za drugo lice, posedovanje dečje pornografije i umišljajno ostvarivanje pristupa sadržajima dečje pornografije putem informatičkih tehnologija.

U smislu odredaba Konvencije, nuđenje ili činjenje dostupnim dečje pornografije podrazumeva, između ostalog, postavljanje nedozvoljenih onlajn sadržaja kako bi se omogućio pristup drugim licima ili pravljenje pornografskih internet sajtova. Ova odredba pokriva i slučajeve kada se čine dostupnim grupe hiperlinkova sa sadržajima dečje pornografije kako bi se omogućio pristup nedozvoljenim sadržajima.

Distribucija podrazumeva aktivno i redovno dostavljanje nedozvoljenih pornografskih sadržaja drugim osobama uz upotrebu računarskih mreža.

Distribucija podrazumeva aktivno i redovno dostavljanje nedozvoljenih pornografskih sadržaja drugim osobama uz upotrebu računarskih mreža.


NOT FOR SALE

Izraz „pribavljanje za sebe ili za drugo lice“ odnosi se na pribavljanje nedozvoljenog pornografskog materijala putem skidanja video-klipova sa interneta ili kupovine dečje pornografije u formi filmova ili fotografija.

Posedovanje dečje pornografije podrazumeva posedovanje nedozvoljenih sadržaja u bilo kakvoj formi (magazini, video-kasete, optički mediji) a, između ostalog, i skladištenje ovakvih podataka u elektronskom obliku na računaru ili prenosnim medijima. Odluka da se zabrani i posedovanje dečje pornografije proizlazi iz potrebe da se inkriminiše svako ponašanje učesnika u lancu, dakle od produkcije i proizvodnje do distribucije i posedovanja nedozvoljenih materijala.

Odredba koja se odnosi na umišljajno ostvarivanje pristupa sadržajima dečje pornografije putem računarskih tehnologija ima kao cilj da inkriminiše onlajn pristup nedozvoljenim sadržajima, ali bez skidanja sa interneta i skladištenja na optičkim medijima. Da bi se utvrdila odgovornost učinioca, potreban je i jedan subjektivni element, odnosno neophodno je da je počinilac imao saznanje da se na određenom sajtu nalazi dečja pornografija i da je želeo da tom sajtu pristupi kako bi mogao da vidi navedene materijale.

U vezi sa odredbama procesnopravne prirode, Konvencija obavezuje potpisnice da preduzmu zakonske i druge neophodne mere kako bi sudije, tužioci i ostalo osoblje koje učestvuje u krivičnim postupcima primilo odgovarajuću obuku i steklo dodatna znanja neophodna za postupanje sa tzv. „posebno osetljivim kategorijama oštećenih“, odnosno sa maloletnim žrtvama koje su bile podvrgnute seksualnoj eksploataciji i zloupotrebi. Dalje, obaveza je i da se nacionalnim procesnim zakonicima predvidi mogućnost za postupajućeg sudiju da odredi saslušanje bez prisustva javnosti (izuzetak od načela javnosti prilikom suđenja), kao i da maloletnim žrtvama bude omogućeno, uz upotrebu informatičkih tehnologija, da daju iskaz bez fizičkog prisustva u sudnici.

Konačno, strane ugovornice se obavezuju da će zakonskim putem ili preduzimanjem drugih odgovarajućih mera obezbediti, putem interneta ili telefonskog ser-

Posedovanje dečje pornografije podrazumeva posedovanje nedozvoljenih sadržaja u bilo kakvoj formi a, između ostalog, i skladištenje ovakvih podataka u elektronskom obliku na računaru ili prenosnim medijima.

visa, službu za pomoć žrtvama, koja bi služila i kao savetodavni servis i podrška prilikom prijavljivanja krivičnih dela i suočavanja sa psihološkim posledicama koje nastupaju za žrtvu.

Konvencija o sprečavanju terorizma[45]

Pitanje terorizma i njegove veze sa visokotehnološkim kriminalitetom novije je prirode i usko je vezano sa razvojem informatičkih tehnologija i njihovom upotrebom u svim sferama života i na svim nivoima, od privatnog do javnog, od nacionalnog do međudržavnog. Mogućnosti koje pružaju informacione tehnologije, kao što je opisano u uvodnom delu ovog poglavlja, dovele su i do visokog stepena zavisnosti komunalnih, javnih, bezbednosnih i drugih službi od upotrebe ovih tehnologija. Na ovaj način i fokus terorista i terorističkih organizacija delimično je uperen i ka eksploatisanju ranjivosti računarskih sistema i upotrebi informatičkih oruđa kao sredstava za izvršavanje terorističkih akata. Otuda potiče i veza između visokotehnološkog kriminala i terorizma, kao i činjenica da se Konvencija o sprečavanju terorizma delimično oslanja i poziva na Konvenciju o visokotehnološkom kriminalu. U skorije vreme, u upotrebu je ušao i izraz „cyberterrorism“ kao posebna vrsta terorističkih napada koji su usmereni ka računarskim sistemima i mrežama u nameri ostvarivanja kakvih političkih ciljeva.

U prilog navedenom rečito govori i Mišljenje Komiteta eksperata za pitanje terorizma (CODEXTER) od 10. novembra 2005. godine, koje je dato na zahtev Komiteta ministara u vezi sa sajber terorizmom i upotrebom interneta u svrhu vršenja terorističkih akata. Komitet eksperata ističe da bi pitanja u vezi sa sajber terorizmom trebalo da budu postavljena u vezi sa procenom efekata primene Konvencije o visokotehnološkom kriminalu. Naime, uočeno je da je najveći broj pitanja koja se odnose na napade na računarske sisteme i mreže pokriven odredbama Konvencije o viso-

[45] „Council of Europe Convention on the Prevention of Terrorism“ (CETS No. 196).

kotehnološkom kriminalu, ali i da je potrebno vršiti kontinuiranu evaluaciju efekata Konvencije i eventualno upotpuniti njene odredbe rešenjima koja se ukažu kao neophodna. Izvršena je i komparativna analiza konvencija o visokotehnološkom kriminalu i sprečavanju terorizma i nisu pronađene pravne praznine ili propusti, odnosno zaključeno je da su navedeni pravni akti kompatibilni. Konačno, kao najveći problem u borbi protiv računarskog kriminala i terorizma, Komitet eksperata ukazuje na činjenicu da je nedovoljan broj država potpisao i ratifikovao ove konvencije. U skladu sa navedenim, zaključeno je da bi fokus trebalo da bude na omogućavanju efikasne i dosledne primene odredaba konvencija o sprečavanju terorizma i visokotehnološkom kriminalu, kao i podsticanju država da konvencijama pristupe, ratifikuju ih i sprovedu u delo, odnosno integrišu u nacionalna zakonodavstva.

U vezi sa borbom protiv terorizma, Savet Evrope je još 1977. godine usvojio *Konvenciju o suzbijanju terorizma* koja je 2005. godine dopunjena *Konvencijom o sprečavanju terorizma* koja je stupila na pravnu snagu 1. juna 2007. godine. Konvencija definiše akte terorizma kao akte navedene u 10 tematskih konvencija koje su navedene u prilogu.[46]

Pre nego što analiziramo odredbe Konvencije koje su u vezi sa zloupotrebom računarskih tehnologija za vršenje terorističkih akata, ukazaćemo na koje se načine internet i računarske tehnologije generalno mogu koristiti u navedene svrhe. Najpre, reč je o napadima putem interneta koji mogu da budu usmereni u dva pravca, ka infrastrukturi i objektima, sa jedne strane, i ljudskom životu, sa druge strane. Dalje, pored napada na navedene ciljeve, računarska tehnologija može da se koristi i radi distribucije raznih sadržaja i pribavljanja sredstava koja omogućavaju dalju terorističku aktivnost. Ovde se pre svega misli na objavljivanje vesti i informacija preko portala terorističkih organizacija, zatim na širenje propagande i upućivanje pretnji, na regrutaciju i obuku za vršenje terorističkih napada, kao i na prikupljanje finansijskih sred-

[46] „Council of Europe Convention on the Prevention of Terrorism“ (CETS No. 196), Appendix.

stava i finansiranje terorizma. Konačno, internet kao globalna mreža služi i kao sredstvo za komunikaciju između članova grupe i kao instrument za planiranje i podršku.

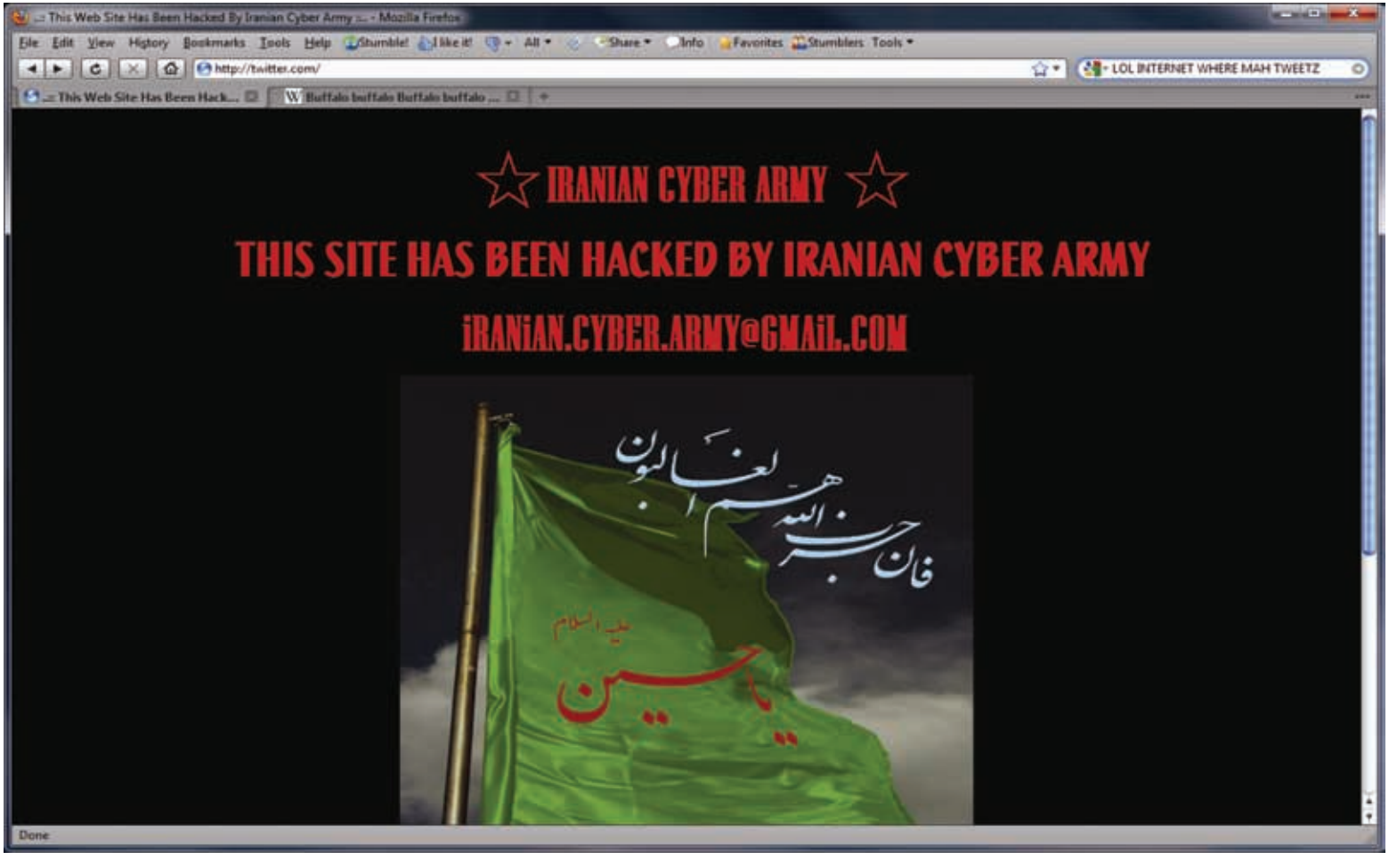
Iz ugla informatičkih tehnologija, značajni su čl. 5-7 Konvencije, koji se odnose na određene pripremne radnje takvog kvaliteta i značaja da imaju potencijal da izazovu ili pomognu akte terorizma. Konkretno, reč je o javnom pozivanju na vršenje terorističkih akata, regrutovanju za vršenje terorističkih akata i treningu, odnosno obuci budućih terorista.

Javno pozivanje da se čine akti terorizma predstavlja, u stvari, nezakonitu i namernu javnu provokaciju, odnosno širenje ili dostavljanje na drugi način javnosti određene poruke u cilju podsticanja na vršenje terorističkog dela, kada takvo ponašanje, bez obzira na to da li je u njemu prisutno ili nije direktno pozivanje na krivična dela terorizma, izaziva opasnost da bi jedno ili više takvih dela moglo da bude počinjeno. Jasno je da se ovako definisana javna provokacija može odaslati zloupotrebom računarskih tehnologija, a naročito interneta kao globalne mreže za komunikaciju i razmenu informacija. Naročito je uočljiva veza sa Dodatnim protokolom uz Konvenciju o visokotehnološkom kriminalu, koja se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih uz upotrebu računarskih sistema, koja u članu 2 definiše rasistički i ksenofobični materijal kao „svaki pisani materijal, svaku sliku i svako predstavljanje ideja ili teorija koje zagovaraju, promovišu ili podstrekavaju mržnju, diskriminaciju ili nasilje, protiv bilo kojeg pojedinca ili grupe pojedinaca, zasnovano na rasi, boji kože, naslednom, nacionalnom ili etničkom poreklu, kao i veri, ako se koriste kao izgovor za bilo koji od tih faktora“.

Regrutovanje za terorizam označava podstrekivanje drugog lica da počini krivično delo terorizma ili da učestvuje u izvršenju takvog dela, ili da stupi u udruženje ili grupu, kako bi doprinelo da to udruženje ili grupa počini jedno ili više terorističkih dela. Jasno je da se postupak regrutacije, na način kako je definisan, može uspešno vršiti pomoću interneta kao globalne mreže. U skladu sa odredbama Konvencije, neophodno je i da je regrutacija izvršena prtivpravno i u određenoj nameri.

Javno pozivanje da se čine akti terorizma predstavlja, u stvari, nezakonitu i namernu javnu provokaciju, odnosno širenje ili dostavljanje na drugi način javnosti određene poruke u cilju podsticanja na vršenje terorističkog dela, kada takvo ponašanje, bez obzira na to da li je u njemu prisutno ili nije direktno pozivanje na krivična dela terorizma, izaziva opasnost da bi jedno ili više takvih dela moglo da bude počinjeno.

Regrutovanje za terorizam označava podstrekivanje drugog lica da počini krivično delo terorizma ili da učestvuje u izvršenju takvog dela, ili da stupi u udruženje ili grupu, kako bi doprinelo da to udruženje ili grupa počini jedno ili više terorističkih dela.


This Web Site Has Been Hacked By Iranian Cyber Army ... - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://twitter.com/
LOL INTERNET WHERE MAH TWEETZ
IRANIAN CYBER ARMY
THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY
iRANiAN.CYBER.ARMY@GMAiL.COM
فان حزب الله هم الغالبون
یا حسین
Done

Konačno, računarske tehnologije i internet (kao i elektronska pošta, diskusioni forumi, *chat* ili *news* grupe itd.) mogu da se upotrebe i radi vršenja obuke za terorizam, koja je definisana kao „davanje uputstava za proizvodnju ili korišćenje eksploziva, vatrenog oružja ili drugog oružja ili štetnih ili opasnih materija, ili za druge specifične metode ili tehnike, u cilju izvršenja ili doprinošenja izvršenju krivičnih dela terorizma, uz svest o tome da će veštine kojima se lice podučava biti korišćene u tu svrhu“.

Računarske tehnologije i internet mogu da se upotrebe i radi vršenja obuke za terorizam, koja je definisana kao „davanje uputstava za proizvodnju ili korišćenje eksploziva, vatrenog oružja ili drugog oružja ili štetnih ili opasnih materija, ili za druge specifične metode ili tehnike, u cilju izvršenja ili doprinošenja izvršenju krivičnih dela terorizma, uz svest o tome da će veštine kojima se lice podučava biti korišćene u tu svrhu“.

Evropska unija

Od pravnih instrumenata koji su nastali u okvirima Evropske unije, za potrebe ove monografije, kao i radi potpunijeg pregleda najvažnijih međunarodnih dokumenata u oblasti borbe protiv visokotehnološkog kriminala, izdvajamo Direktivu o pravnoj zaštiti kompjuterskih programa i Direktivu o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža.

Direktiva Saveta Evropske zajednice o pravnoj zaštiti kompjuterskih programa

Potrebu za uniformnim rešenjima u oblasti pravne zaštite kompjuterskih programa nametnule su razlike u nacionalnim zakonodavstvima država članica koje su imale nepovoljan uticaj na funkcionisanje zajedničkog tržišta, kao i opasnost da bi se ovi problemi mogli usložiti ukoliko bi se nastavilo sa praksom pojedinačnog i neusklađenog regulisanja ove materije. Takođe, uzeto je u obzir i da ekskluzivno pravo autora da spreči neovlašćeno umnožavanje svog dela treba da podleže i izvesnim ograničenjima kada su u pitanju kompjuterski programi. Naime, kako bi se omogućilo umnožavanje koje je tehnički neophodno legalnom sticaocu kopije programa, propisano je da se operacije učitavanja i puštanja u rad ovakve kopije ne mogu zabraniti ugovorom i da se u odsustvu specifičnih odredaba u ugovoru, a naročito u slučaju prodaje jedne kopije programa, i svaka druga operacija neophodna za korišćenje programa može izvršavati od strane lica koje je legalno steklo kopiju.

U skladu sa odredbama Direktive, države članice zaštićuju autorskim pravom kompjuterske programe kao književna dela, i to u smislu odredaba Bernske konvencije za zaštitu književnih i umetničkih dela, a pojam „kompjuterski program“ obuhvata i pripremni materijal za koncipiranje programa.

Autorom kompjuterskog programa smatra se kako fizičko lice ili grupa fizičkih lica koja su stvorila program, tako i pravno lice ukoliko zakonodavstvo države članice predviđa da ova lica mogu da budu titulari autorskog prava. Takođe, kada je kompjuterski program stvarao jedan službenik u obavljanju svoje službe ili prema nalozima poslodavca, jedino je poslodavac ovlašćen da vrši imovinska prava koja se odnose na ovako stvoren kompjuterski program, osim ako odredbama ugovora nije predviđeno suprotno.

Autorom kompjuterskog programa smatra se kako fizičko lice ili grupa fizičkih lica koja su stvorila program, tako i pravno lice ukoliko zakonodavstvo države članice predviđa da ova lica mogu da budu titulari autorskog prava.

Pravna zaštita pruža se svakom fizičkom i pravnom licu koje potpada pod odredbe nacionalnih zakonodavstava u oblasti autorskog prava primenjivog na književna dela.

Direktiva predviđa i obavezu da se kao nedozvoljena, pravno sankcionišu tačno navedena ponašanja, i to:

- stavljanje u promet kopije kompjuterskog programa, znajući da je kopija nedozvoljena ili imajući razloge za osnovanu sumnju u njenu nedozvoljenost;
- držanje iz komercijalnih razloga kopije kompjuterskog programa, znajući da je kopija nedozvoljena ili imajući razloge za osnovanu sumnju u njenu nedozvoljenost;
- stavljanje u promet ili držanje u komercijalne svrhe svakog sredstva čija je jedina svrha da olakša nedozvoljeno uklanjanje ili neutralizaciju svakog tehničkog mehanizma eventualno napravljenog u cilju zaštite kompjuterskog programa.

Propisana je i obaveza da se zapleni svaka nedozvoljena kopija kompjuterskog programa u skladu sa pocedurom koja je propisana procesnim pravilima nacionalnih zakonodavstava.

Što se tiče trajanja, zaštita je obezbeđena tokom života autora i pedeset godina nakon njegove smrti ili smrti poslednjeg živog autora ukoliko je u pitanju grupa autora. Ukoliko je reč o kompjuterskom programu koji je anonimno delo ili delo objavljeno pod pseudonimom ili se nacionalnim zakonima autorom smatra pravno lice,

U pitanju je Direktiva o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža.

trajanje zaštite je pedeset godina počevši od dana kada je kompjuterski program zakonito učinjen javno dostupnim po prvi put.

Direktiva 2006/24/EU Evropskog parlamenta i Saveta

U pitanju je Direktiva o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža.[47] Sa stanovišta efikasnog otkrivanja i krivičnog gonjenja svih krivičnih dela čije izvršenje ostavlja „elektronske tragove“ koji u propisno sprovedenoj proceduri mogu dobiti snagu neoborivog dokaza pred sudom, Direktiva o čuvanju podataka i procedure koje ona propisuje ukazuju se kao neizostavan, možemo reći i suštinski korak ka suzbijanju delatnosti koje ugrožavaju bezbednost računarskih podataka.

Pre nego što analiziramo sadržaj odredaba ovog pravnog akta, neophodno je učiniti nekoliko važnih napomena imajući u vidu da se ova direktiva oslanja na neke druge međunarodne dokumente i dopunjuje ih.

Najpre, Direktiva o čuvanju podataka ujedno predstavlja i izmenu i dopunu Direktive 2002/58/EU o obradi ličnih podataka i zaštiti privatnosti u sektoru elektronskih komunikacija. Članovima 5, 6 i 9 navedene Direktive utvrđena su pravila koja primenjuju davaoci mreža i usluga u pogledu obrade podataka o predmetu i lokaciji nastalih usled korišćenja usluga elektronske komunikacije. Takvi podaci se moraju izbrisati ili moraju postati anonimni kada više nisu potrebni u svrhu prenosa komunikacije. Članom 15, stav 1 Direktive 2002/58/UE, međutim, predviđeni su i uslovi

[47] „Directive 2006/24/EC of the European Parliament and of the Council: on the retention of data generated or processed in connection with provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC“ Official Journal of the European Union, 13.04.2006.

pod kojima države članice mogu da ograniče navedeni obim prava i obaveza, s tim da svako takvo ograničenje mora da bude nužno, prikladno i srazmerno svrsi očuvanja javnog reda, zaštite nacionalne sigurnosti, odbrane, javne bezbednosti ili sprečavanja, otkrivanja, istrage i progona krivičnih dela i neovlašćene upotrebe sistema elektronske komunikacije.

U vezi sa navedenom odredbom je i zaključak Saveta za pravosuđe i unutrašnje poslove EU od 19. decembra 2002. godine, kojim se ukazuje da su, zbog značajnog porasta mogućnosti koje pružaju elektronske komunikacije, podaci koji se tiču upotrebe elektronskih komunikacija posebno važni i predstavljaju vredno sredstvo u sprečavanju, istrazi, otkrivanju i gonjenju krivičnih dela, prvenstveno organizovanog kriminala.

Deklaracija o borbi protiv terorizma koju je Evropski savet usvojio 25. marta 2004. godine takođe upućuje na potrebu da se detaljno ispitaju mere za utvrđivanje pravila o čuvanju podataka o komunikacijskom prometu od strane davalaca usluga.

Dalje, članom 8 *Evropske konvencije o zaštiti ljudskih prava i osnovnih sloboda*[48] propisano je da svako ima pravo na poštovanje svog privatnog života i korespondencije i da se državni organi i druga javna tela mogu umešati u uživanje ovoga prava samo u skladu sa zakonom i samo kada je to neophodno radi očuvanja interesa nacionalne ili javne bezbednosti, radi sprečavanja nereda ili zločina ili radi zaštite prava i sloboda drugih lica. Kako se pitanje čuvanja podataka o elektronskim komunikacijama pokazalo kao neophodno sredstvo za organe otkrivanja i gonjenja (naročito u vezi sa suzbijanjem organizovanog kriminala i terorizma), nužno je obezbediti da čuvani podaci budu na raspolaganju organima koji primenjuju zakon tokom određenog perioda. Na ovaj način kroz Direktivu o čuvanju podataka doprinosi

[48] „Convention for the Protection of Human Rights and Fundamental Freedoms“, CETS No.: 005, Council of Europe, Rome, 4.11.1950.

se efikasnijoj borbi protiv kriminala uz poštovanje Konvencije o osnovnim ljudskim pravima i slobodama. Koliki je značaj održavanja ravnoteže između zaštite osnovnih ljudskih prava, sa jedne, i potrebe za efikasnom borbom protiv kriminala, sa druge strane, govori nam i tumačenje (član 8 Evropske konvencije o zaštiti ljudskih prava i osnovnih sloboda) Evropskog suda za ljudska prava prema kome zadiranje javnih tela u pravo na privatnost mora da ispunjava zahteve nužnosti i srazmernosti i mora da služi tačno određenim, jasnim i legitimnim svrhama te da bude izvedeno na način koji je primeren, relevantan i ne preteran u odnosu na svrhu zadiranja.

Konačno, i *Konvencija Saveta Evrope o visokotehnološkom kriminalu* iz 2001. godine te *Konvencija Saveta Evrope o zaštiti prava pojedinaca u vezi sa automatskom obradom ličnih podataka* iz 1981. godine takođe obuhvataju i podatke koji se čuvaju u smislu Direktive 2006/24/EU Evropskog parlamenta i Saveta.

Osnovni cilj Direktive o čuvanju podataka jeste da se usklade odredbe država članica koje se tiču obaveze davaoca javno dostupnih usluga elektronske komunikacije i javnih komunikacionih mreža da čuvaju određene podatke koje dobijaju ili obrađuju kako bi se osiguralo da ti podaci budu dostupni u svrhu istrage, otkrivanja i progona teških krivičnih dela (član 1 Direktive). Da bi se ispravno razumelo područje primene ove Direktive, nužno je objasniti da se ona primenjuje *samo na podatke o prometu i lokaciji* pravnih i fizičkih lica i na uz to vezane podatke nužne za identifikaciju pretplatnika ili registrovanog korisnika. Dakle, ona se *ne primenjuje na podatke na sadržaj* elektronske komunikacije, kao ni na informacije do kojih se dolazi korišćenjem mreža elektronske komunikacije.

Za potrebe Direktive primenjuju se odgovarajuće definicije najznačajnijih pojmova. Tako se pod izrazom „podatak“ smatraju podaci o prometu i lokaciji i uz njih vezani podaci nužni za identifikaciju pretplatnika ili korisnika. Sam izraz „korisnik“ označava sva pravna ili fizička lica koja koriste javno dostupne elektronske komunikacije za poslovne ili privatne potrebe, a koja nisu nužno i pretplaćena na tu uslugu. Izraz „telefonska usluga“ odnosi se na pozive (glasovne, glasovnu poštu i konferen-

Tako se pod izrazom „podatak“ smatraju podaci o prometu i lokaciji i uz njih vezani podaci nužni za identifikaciju pretplatnika ili korisnika.

cijske pozive), dopunske usluge (preusmeravanje i prenos poziva) i usluge slanja poruka i multimedijalne poruke (SMS, EMS i MMS). Kada Direktiva koristi izraz „korisničko ime“, on se odnosi na jedinstvenu identifikaciju koja se dodeljuje osobi koja stupa u pretplatnički odnos ili se registruje za pristup internetu ili uslugu komunikacije putem interneta. Izraz „identitet ćelije“ odnosi se na identitet ćelije u mobilnoj telefoniji iz koje poziv otpočinje ili u kojoj se taj poziv završava. Konačno, kada se koristi izraz „neuspešan poziv“, on se odnosi na komunikaciju u kojoj je telefonski poziv uspešno spojen, ali na njega nije odgovoreno ili je došlo do intervencije uprave operatera telefonije. Ovo, u stvari, znači da Direktiva ne zahteva da se čuvaju podaci koji se odnose na nespojene pozive.

Pravo na pristup podacima države članice daju samo nadležnim nacionalnim telima u postupku predviđenom nacionalnim pravom.

Pravo na pristup podacima države članice daju samo nadležnim nacionalnim telima u postupku predviđenom nacionalnim pravom, poštujući pri tome propise Evropske unije ili međunarodnog javnog prava, a naročito Evropsku povelju o osnovnim ljudskim pravima i slobodama (član 4).

Centralni deo Direktive zauzima kategorizacija podataka koji se čuvaju, a koji su taksativno nabrojani i razvrstani u kategorije i potkategorije.

Najpre, tu su podaci potrebni *za pronalaženje i identifikaciju izvora komunikacije*. U slučaju fiksne i mobilne telefonije to su sledeći podaci:

- telefonski broj priključka sa kojeg poziv dolazi;
- ime i adresa registrovanog korisnika ili pretplatnika.

U slučaju pristupa internetu, elektronskoj pošti i internet telefoniji čuvaju se:

- podaci o dodeljenom korisničkom imenu/imenima;
- korisničko ime i telefonski broj dodeljen svakoj komunikaciji s kojom se stupa u javnu telefonsku mrežu;
- ime i adresa pretplatnika ili registrovanog korisnika kojem je u trenutku komunikacije dodeljena adresa internet protokola (IP), korisničko ime i telefonski broj.

Druga kategorija podataka koji se čuvaju jesu podaci potrebni *za otkrivanje odredišta komunikacije.* U slučaju fiksne i mobilne telefonije to su sledeći podaci:

- birani broj/brojevi i, u slučaju koji uključuje korišćenje dodatnih usluga poput preusmeravanja ili prenosa poziva, broj/brojevi na koje je poziv preusmeren;
- ime/imena i adresa/adrese pretplatnika ili registrovanog korisnika.

U slučaju elektronske pošte i internet telefonije čuvaju se:

- korisničko ime ili telefonski broj primaoca kome je namenjen poziv preko internet telefonije;
- ime i adresa pretplatnika ili registrovanog korisnika i korisničko ime primaoca prema kome je komunikacija usmerena.

Treća kategorija podataka odnosi se na one namenjene *utvrđivanju datuma, vremena i trajanja komunikacije*. U slučaju fiksne i mobilne telefonije to su datum i vreme početka i završetka komunikacije.

U slučaju pristupa internetu, elektronskoj pošti i internet telefoniji čuvaju se:

- datum i vreme prijave i odjave pristupa internetu prema određenoj vremenskoj zoni, zajedno sa IP adresom, bilo da je statička ili dinamička, koju je komunikaciji dodelio davalac usluga pristupa internetu, kao i korisničko ime pretplatnika ili registrovanog korisnika;
- datum i vreme prijave i odjave od usluge elektronske pošte ili usluge internet telefonije prema određenoj vremenskoj zoni.

Četvrtu kategoriju čine podaci neophodni *za otkrivanje vrste komunikacije.* U slučaju fiksne i mobilne telefonije to je korišćena telefonska usluga, a u slučaju elektronske pošte i internet telefonije u pitanju je korišćena internet usluga.

Peta kategorija podataka koji se čuvaju jesu podaci neophodni *za identifikaciju komunikacijske opreme korisnika ili njihove navodne opreme*. U slučaju fiksne telefonije to su telefonski brojevi sa kojih se poziva i brojevi koji se pozivaju. Prilikom komunikacije putem mreže mobilne telefonije čuvaju se: telefonski brojevi sa kojih

se poziva i brojevi koji se pozivaju, međunarodni identitet mobilnog pretplatnika (IMSI) stranke koja poziva i koja prima poziv, međunarodni identitet mobilnog uređaja (IMEI) stranke koja poziva i koja prima poziv, u slučaju unapred plaćenih (*prepaid*) anonimnih usluga, datum i vreme početka upotrebe usluge i lokacijska oznaka (identitet ćelije) s koje je usluga aktivirana.

U slučaju pristupa internetu, elektronskoj pošti i internet telefoniji čuvaju se podaci o telefonskom broju s kojeg se poziva u svrhu telefonskog (*dial-up*) pristupa ili digitalna pretplatnička linija (DSL) ili druga krajnja tačka lica koje započinje komunikaciju.

Konačno, šesta grupa podataka koji se moraju čuvati jesu podaci potrebni *za otkrivanje lokacije opreme za mobilne komunikacije*. To su lokacijska oznaka (identitet ćelije) na početku komunikacije i podaci kojima se identifikuje geografska lokacija ćelija navođenjem lokacijskih oznaka (identiteta ćelije) tokom razdoblja za koje su čuvani podaci o komunikaciji.

Prema odredbama Direktive, države članice preuzimaju obavezu da sve navedene kategorije podataka čuvaju u razdoblju koje nije kraće od šest meseci niti duže od dve godine od datuma komunikacije (član 6 Direktive). Međutim, države članice mogu da preduzmu potrebne mere koje u posebnim okolnostima opravdavaju produženje najdužeg vremena čuvanja koje propisuje Direktiva, uz obavezu da o navedenom produženju roka obaveste Komisiju i druge države članice o preduzetim merama i razlozima zbog kojih su ove mere primenjene. Posle dobijanja obaveštenja o primenjenim merama, Komisija ima rok od šest meseci u kome odobrava ili odbija nacionalne mere nakon ispitivanja da li su one preduzete kao sredstvo proizvoljne diskriminacije ili predstavljaju prikriveno ograničenje trgovine među državama članicama i stvaraju prepreku funkcionisanju unutrašnjeg tržišta.

Po pitanju pravne zaštite lica o kojima se podaci prikupljaju i čuvaju za određeni period, popisana je obaveza preduzimanja potrebnih mera kako bi za svaki protivpravan pristup podacima koji se čuvaju bile predviđene zakonske posledice i odgovornost koja se utvrđuje bilo u upravnom, bilo u krivičnom postupku. Navodi se da sankcije po svojoj prirodi i težini moraju da budu srazmerne i takve da odvraćaju od daljeg kršenja zakona.

Specifičnosti procesuiranja dela visokotehnološkog kriminala

- *Transnacionalni karakter koji po pravilu prati dela visokotehnološkog kriminala*. –Ovaj problem može se svesti na jednostavno pitanje: Kako goniti delo koje je „izvršeno“ u nekoliko država istovremeno? Veliki broj krivičnih dela iz ove oblasti vezan je svojom prirodom za veći broj država, a kombinacije koje pri tome mogu nastati gotovo su beskonačne: npr. državljanin Srbije izvrši prevaru preko internet prezentacije koja se nalazi na serveru u Austriji, dok su oštećeni iz Kanade i Australije. Verovatno najpoznatiji primer umešanosti više međunarodnih elemenata u izvršenje jednog krivičnog dela posredstvom računara i računarskih mreža dogodio se u Austriji, prilikom akcije protiv vlasnika internet prezentacije sa dečjom pornografijom. Austrijski državljanin je postavio prezentaciju na kojoj su članovi, nakon što plate određenu sumu novca za pristup, mogli da preuzimaju različite materijale vezane za dečju pornografiju. Server na kome se prezentacija nalazila zakupljen je u Rusiji, a sam provajder je poslao dojavu austrijskoj policiji kada je uvideo da se prezentacija koristi za nelegalne radnje i na taj način inicirao istragu i potonja hapšenja. Korisnici prezentacije, koji su takođe počinili krivično delo jer je posedovanje dečje pornografije u njihovim državama krivično delo, uglavnom su iz Velike Britanije i Danske. I pored komplikovanog zapleta priče, ovde je situacija (gotovo) jasna, budući da su nadležni organi različitih država sarađivali u celom poduhvatu – vlasniku prezentacije će se suditi u Austriji, ostalim okrivljenim u zemljama čiji su državljani. Situacija ne mora, međutim, uvek da bude takva, a čak i ovaj slučaj povlači za sobom još jedno važno pitanje, odnosno problem: kako goniti počinioce dela koja u državama čiji su državljani ili na čijoj su teritoriji izvršena nisu kažnjiva?

• *Relativnost načela ignorantia iuris non excusat*. – Bez ikakve namere da se opovrgne ovo fundamentalno pravilo, mora se ukazati da „počinioci“ pojedinih dela uopšte ne moraju biti svesni toga šta čine, ili imati nameru da bilo kome naude ili steknu određenu protivpravnu imovinsku (ili drugu) korist. Dešavalo se da prijatelji na internetu šalju jedan drugome različite forme računarskih virusa da bi testirali svoju zaštitu, bez znanja da će se taj virus širiti preko sistema elektronske pošte na sve druge imejl adrese koje poseduju. Dešavalo se takođe da putem elektronske pošte ljudi dođu u posed nelegalnog materijala koji dalje distribuiraju, npr. njihove omiljene pesme (koja, pri tom, nije legalno kupljena). Problem koji ovakvi incidenti nose, naravno ukoliko se javljaju kao usamljena aktivnost pojedinca, a ne njegova svakodnevna praksa, jeste: kakva je društvena opasnost u tom aktu?

• Međutim, da bi se u samom postupku pravilno odvagale okolnosti slučaja, *sudija mora da ima zavidno predznanje o stvarima o kojima je reč*. Isto se odnosi i na tužioca, kao i na ostale državne institucije koje učestvuju u postupku.

• *Kako biti siguran ko je počinilac dela?* Iako ovo pitanje može da deluje trivijalno, neko može i „preuzeti“ računar bez znanja vlasnika, čak i u trenutku kada vlasnik radi na tom računaru. Kako rešiti ovaj problem ako okrivljeni tvrdi da nije učinio delo za koje se tereti, posebno kada sve okolnosti, a naročito njegovo znanje rada na računaru, ne indikuju da je on učinilac? Ovde se dolazi do novog problema, a to je temeljnost istražnih radnji, koja opet iziskuje specifično obrazovanje tužioca i policijskih organa koji sprovode istragu. Većina računarskih prevara je dovedena do takvog oblika savršene manipulacije tuđim računarima, pa se mora veoma pažljivo postupati sa eventualnim osumnjičenima dok se ne dođe do nedvosmislenog saznanja da su oni na bilo koji način mogli da budu umešani u izvršenje krivičnog dela.

• U vezi sa prethodnim pitanjem otvara se još jedno, kao posledica razvoja novih mogućnosti za omogućavanje internet komunikacije: *kako otkriti počinioca koji je delo izvršio koristeći javne mreže i laptop računar?* Kao što je već objašnjeno, sasvim je moguće da neko koristi otvorenu WiFi mrežu drugog korisnika, ali i javne mreže koje se danas mogu naći na aerodromima, drugim javnim mestima, internet kafeima, restoranima širom sveta? U takvom slučaju, počinilac je gotovo nevidljiv, odnosno kada delo bude otkriveno i preko korišćene IP adrese lokacije sa koje je izvršeno, kriminalac će po pravilu odavno biti na nekoj drugoj, sigurnoj lokaciji.

• *Kako dokazivati delo visokotehnološkog kriminala?* – Ponekad su podaci koje dostavi internet (ili drugi) provajder dovoljni da se neko lice poveže sa određenim krivičnim delom. Kada oni nisu dovoljni, koliko je validno prihvatiti sadržaj hard diska, fleš memorije ili drugih medijuma pred sudom? Posebno u slučaju kada sudija

ne zna šta je to hard disk i ne može valjano proceniti da li se može prihvatiti kao dokaz, kao i težinu takvog dokaza?[49]

- Takođe u vezi sa dokazivanjem dela, pitanje koje je poslednjih godina veoma aktuelno jeste: *kako „slušati" komunikacije a ne ugroziti pravo na privatnost pojedinca?* Za razliku od istrage povodom drugih krivičnih dela gde, npr. prisluškivanje telefona dolazi kao mera kojoj prethode neke druge istražne radnje koje bi identifikovale da je neko lice umešano u protivpravno delovanje, kod visokotehnološkog kriminala ponekad se ne može utvrditi jasna granica kada postoji sumnja, odnosno kada je traženje pojedinih privatnih podataka o ličnosti dozvoljeno, i uopšte relevantno za istragu. Ovaj problem ne dolazi od tendencije policijskih i drugih organa da svoja ovlašćenja tumače široko. Naprotiv, sama priroda visokotehnološkog kriminala je takva da je on „skriven" i da je potrebno veliko znanje i iskustvo da bi se uopšte percipirao.[50]

- *Kako uspostaviti efikasnu međunarodnu saradnju između različitih pravnih sistema širom sveta?* – Globalni instrumenti međunarodnog prava koji bi regulisali saradnju u ovoj oblasti ne postoje. To je ostavljeno na volju državama koje se mogu različitim bilateralnim sporazumima i regionalnim konvencijama, poput one Saveta Ev-

[49] U tom smislu vredi proučiti iskustva SAD, koje su verovatno najdalje stigle kada je reč o praksi prikupljanja elektronskih dokaza i njihovog (ne)uvažavanja u sudskom postupku. Videti, npr. *One Year Later: The Most Significant Electronic Discovery Cases Under The New Federal Rules Of Civil Procedure*, na internet adresi *http://technology.findlaw.com/articles/01036/011041.html*, 01.03.2009; *Electronic Crime Scene Investigation: A Guide for First Responders*, *http://www.ojp.usdoj.gov/nij*, 01.05.2009.

[50] Videti, npr. tekst sa zanimljivim linkovima o sakupljanju dokaza i „računarima kao očevicima": K. A. Taipale, *Investigating Cybercrime; Digital Evidence*, http://www.information-retrieval.info/cybercrime/index08.html, 01.03.2009; takođe: Jeffrey Carr, *Anti-Forensic Methods Used by Jihadist Web Sites*, *http://www.esecurityplanet.com/trends/article.php/3694711/Anti-Forensic-Methods-Used-by-Jihadist-Web-Sites.htm*, 01.05.2009.

rope, boriti za stvaranje jednoobraznog sistema. A stanje koje postoji nije obećavajuće: pojedine države uopšte ne poznaju dela visokotehnološkog kriminala; one koje ga poznaju veoma često ta dela inkriminišu na poseban način; veliki je broj zemalja u kojima zakonodavstvo postoji, ali se ne primenjuje, ili ne postoji konzistentna praksa. Kada je reč o ekstradiciji počinilaca ili obezbeđivanju dokaza o izvršenom delu, tradicionalne prepreke i izgovori se kombinuju sa novim, među kojima nedostatak regulative, političke volje ili tehničkih mogućnosti prednjače. Kada su i ostvarljivi kontakti i saradnja između relevantnih tela dveju ili više država, procedure su spore (a visokotehnološki kriminal zahteva brzinu reagovanja) a rezultati neizvesni.

- *Kako postupati sa maloletnim učiniocima?* – Naravno, sva zakonodavstva imaju posebnu regulativu u slučaju da su počinioci delimično ili potpuno neodgovorni sa stanovišta krivičnog prava, ali su pitanja koja se postavljaju kako moralne, tako i praktične prirode – kako objasniti mladim (ponekada i vrlo mladim) počiniocima da je, npr. slanje kompjuterskog virusa u određenu računarsku mrežu kažnjivo i da može izazvati ogromnu materijalnu štetu? Kako ih kazniti (ili – da li ih kazniti?), ali i kako sprečiti ponavljanje izvršenja ovakvih krivičnih dela? Instituti klasičnog krivičnog prava koji su na raspolaganju državnim organima i institucijama koje brinu o maloletnim osobama, najčešće nisu od pomoći u ovakvim slučajevima.

- Prethodno pitanje otvara novi problem u odnosu na sve počinioce (i potencijalne počinioce): *kako raditi na prevenciji izvršenja krivičnih dela iz ove oblasti?* Treba naglasiti i drugu stranu ovog problema: *kako onemogućiti počinioca da ponovi svoje delo?* Kazne koje su se u pojedinim državama koristile na početku razvoja zakonodavstava o visokotehnološkom kriminalu – kao što je kućni pritvor, jednostavno ne mogu da budu efikasne. Zabrana „kontakta“ osobe sa računarom takođe je besmislena, posebno kada se ima u vidu i hiperrazvoj ovih tehnologija i mogućnost da se mnoga od ovih dela izvrše i pomoću neke druge savremene naprave.

- Procesnopravne probleme ne možemo da razmatramo mimo razmatranja zakona iz kojih proističu. Dobri procesni zakoni i razrađene procedure, preduslov su primene materijalnih zakona, bez kojih bi ovi bili samo „mrtvo slovo na papiru“. Procesni i materijalni zakoni moraju da se razvijaju uporedo ukoliko želimo da izbegnemo probleme u njihovoj primeni.

- Materijalni zakoni moraju da odražavaju vreme u kojem traju, međutim, nepostojanje instrumenata koji bi omogućili njihovu primenu čini ih neupotrebljivim ma koliko oni savremeni bili. U približno takvoj situaciji, upravo se nalazi i krivično zakonodavstvo Republike Srbije.

Ono što je u ovom trenutku izvesno jeste činjenica da postojeći procesni zakonik anahronim rešenjima otežava primenu KZ-a, koji se, uvođenjem novih pojmova i čitavih poglavlja krivičnih dela, već odavno pridružio tendencijama savremenog krivičnog zakonodavstva. Usled ovakve neusklađenosti KZ-a i ZKP-a, u svakodnevnoj sudijskoj i tužilačkoj praksi, neretko se pribegava analogiji i ekstenzivnom tumačenju procesnih normi, na način koji je suprotan intencijama zakonodavca koji ih je doneo.

Na terenu procesnih odredaba koje su u direktnoj vezi sa otkrivanjem krivičnih dela visokotehnološkog kriminala možemo konstatovati da važeći Zakonik o krivičnom postupku *ne predviđa posebne dokazne radnje niti posebna ovlašćenja vezana za otkrivanje ovih krivičnih dela*.[51]

[51] Treba imati u vidu da je ovaj zakonik stupio na pravnu snagu pre reformi materijalnog krivičnog zakonodavstva, u vreme kada su pitanja koja se odnose na kompjuterski kriminalitet bila van žiže interesovanja pravne nauke.

Upravo iz napred navedenih razloga, u postupku otkrivanja i procesuiranja krivičnih dela visokotehnološkog kriminala, od strane nadležnih državnih organa koriste se iste odredbe Zakonika o krivičnom postupku koje se primenjuju i na sva druga krivična dela.

Tako, na primer, odredbe koje propisuju uslove pod kojima je moguće narediti nadzor i snimanje telefonskih i drugih razgovora, ili komunikacija drugim tehničkim sredstvima (*računarske mreže*), nije moguće primeniti s obzirom na to da taksativno navedenim krivičnim delima na koja se ova mera odnosi nisu obuhvaćene i inkriminacije iz oblasti VT kriminala.

I ostale specijalne istražne metode, kao što su pružanje simulovanih pravnih usluga, angažovanje prikrivenih islednika, snimanje telefonskih i drugih razgovora i optička snimanja lica – ostala su van domašaja primene od strane organa za borbu protiv visokotehnološkog kriminala, imajući u vidu da su prema zakonskim odredbama primenjiva samo za krivična dela organizovanog kriminala, odnosno tajni video i audio- nadzor, i za krivična dela protiv ustavnog uređenja i bezbednosti, kao i za krivična dela protiv čovečnosti i međunarodnog prava.

U ovakvoj situaciji, susretanje sa procesnopravnim problemima deo je svakodnevne prakse.

Državni organi koji primenjuju ZKP, da bi uopšte obavljali posao koji im je u nadležnosti, usled nedostatka odgovarajućih procesnih instrumenata često pribegavaju analogiji i ekstenzivnom tumačenju njegovih pravnih normi.

Tako, prilikom preduzimanja radnji obezbeđivanja i zaplene digitalnih[52] i drugih materijalnih dokaza, primenjuju se odredbe ZKP-a koje se odnose na pretresanje stana i lica (čl. 77-81) i privremeno oduzimanje predmeta (čl. 82-85), za pregled računarske opreme na licu mesta, odredbe ZKP-a koje se odnose na uviđaj (čl. 110-112), a u pogledu veštačenja tako oduzete opreme i njenog digitalnog sadržaja, opšte odredbe o veštačenju iz čl. 113-123. ZKP-a.

Paradoks je da su specijalna istražna radnja „snimanje telefonskih i drugih razgovora“ (*fiksna i mobilna telefonija, Skype i Voip, npr*.) i „obična“ istražna radnja iz člana 232 ZKP-a, koja predviđa nadzor i snimanje komunikacija tehničkim sredstvima (*prikupljanje i presretanje računarskih podataka i komunikacije u realnom vremenu*), rezervisane isključivo za otkrivanje i prikupljanje dokaza u vezi sa izvršenjem nekih drugih krivičnih dela, ali ne i krivičnih dela iz oblasti VT kriminala kod kojih je *modus operandi* upravo korišćenje telekomunikacionih mreža i uređaja!

Kada je u pitanju efikasna borba protiv visokotehnološkog kriminala, od neprocenjivog je značaja postojanje kvalitetne pravne regulative u oblasti pružanja međunarodne pravne pomoći.

Kada je u pitanju efikasna borba protiv visokotehnološkog kriminala, od neprocenjivog je značaja postojanje kvalitetne pravne regulative u oblasti pružanja međunarodne pravne pomoći.

[52] Postojeći ZKP ne daje ni elementarnu definiciju dokaza, a kamoli elektronskog, koji se pojavljuju u vezi sa izvršenjem krivičnih dela visokotehnološkog kriminala. Elektronski dokaz je informacija ili podatak od značaja za istragu, koji su smešteni ili preneti putem računara. Imaju istu vrednost kao i svi drugi materijalni dokazi i za njih važe potpuno ista procesna pravila kao i za sve ostale dokaze. Međutim, pri ovome treba imati u vidu specifičnost elektronskih dokaza koja proizlazi iz njihove prirode, a to je da su veoma osetljivi, da se vrlo lako mogu izmeniti, obrisati ili na bilo koji drugi način uništiti, što zahteva posebnu pažnju i pristup u postupku pribavljanja i obezbeđivanja ovakvih dokaza.

S obzirom na maršrutu kriminalnog akta iz oblasti visokotehnološkog kriminala, koja se u kiber prostoru neretko pruža i preko teritorije nekoliko kontinenata, pitanje pravilnog postavljanja mesne nadležnosti može da bude od prvorazrednog značaja. Ovakve slučajeve višestruke nadležnosti sudova različitih država, isključivo specifične za *cyber*[53] *crime*, svojim odredbama nisu regulisali ni KZ ni ZKP.[54]

Nadnacionalni i transnacionalni karakter visokotehnološkog kriminala u praksi ne implicira isključivo probleme u pogledu pravilnog određivanja mesne nadležnosti. Prikupljanje dokaza u cilju rasvetljavanja kriminalnog akta koji je svoje tragove „ostavio“ na globalnoj računarskoj mreži i računarskim sistemima više kontinenata ili država jedino je moguće u postupku pružanja međunarodne pravne pomoći.

Zbog neprimereno dugog trajanja ovog postupka, u praksi se često odustajalo od primene odgovarajućih odredaba ZKP-a iz poglavlja XXXII, čak i u situacijama kada je pružanje takve pomoći bilo od neprocenjive važnosti za ishod samog postupka.

Čekanje odgovora po upućenim zamolnicama u trajanju od po dve i više godina obesmišljavalo je ne samo korišćenje ovog pravnog instituta već i same krivične postupke u kojima je trebalo da bude primenjen.

---

[53] Engleska reč izvedena od grčke Κυβερνήτης / kybernetes – upravljač, pilot, kormilar. U duhu srpskog jezika pravilno je izgovarati „kiber“.

[54] Takva situacija, gde bi više od jedne države moglo da zahteva nadležnost, može biti posebno česta u slučajevima napada na informacione sisteme, kao što su, na primer, napadi virusa i drugih malicioznih programa koji istovremeno mogu da nanesu štetu velikom broj informacionih sistema na globalnom nivou.

Zakon o pružanju međunarodne pravne pomoći u krivičnim stvarima,[55] čijim su donošenjem stavljene van snage odredbe ZKP-a koje se tiču postupka za pružanje međunarodne pravne pomoći i izvršenje međunarodnih ugovora u krivičnopravnim stvarima, propustio je da reguliše specifične aspekte pružanja međunarodne pravne pomoći u krivičnim stvarima iz oblasti visokotehnološkog kriminala u kojoj je, više nego u bilo kojoj drugoj, brzina[56] u postupanju od presudnog značaja za uspešno vođenje krivičnog postupka.

Osim što je previdео postojanje „mreže 24/7",[57] zakon je propustio da predvidi i upotrebu modernih načina komuniciranja,[58] uključujući imejl i faks, za upućivanje zahteva (*za kojima bi usledila zvanična pisana molba*) u hitnim postupcima pružanja međunarodne pravne pomoći kao što su uzajamna pomoć u pogledu prikupljanja podataka o saobraćaju u realnom vremenu, zaplena i dostava sačuvanih računarskih podataka za potrebe druge države itd.

U tom smislu praksa je pokazala da je zaobilaženje ovako „tromih" zakona i sporih procedura jedino moguće uspostavljanjem neformalnih kontakata i saradnje, što, nažalost, implicira pitanje pravne validnosti na ovaj način prikupljenih dokaza.

[55] „Službeni glasnik RS", br. 20/2009.

[56] Kao što je već rečeno, priroda podataka relevantnih u visokotehnološkom kriminalu izuzetno je nestabilna i čuva se veoma ograničen period (ponekad samo nekoliko minuta). Stoga je brzo reagovanje od ključnog značaja u izvršenju uzajamne pomoći.

[57] Autori Konvencije o VT kriminalu uvideli su da postojeći modaliteti policijske saradnje i uzajamne pomoći iziskuju dodatne kanale radi efikasne borbe u računarskoj eri. Takvo mesto za kontakt bi trebalo da bude u stanju da obezbedi momentalnu pomoć u istragama i sudskim postupcima.

[58] Do stepena koji garantuje odgovarajuće nivoe bezbednosti i autentičnosti (uz korišćenje enkripcije, elektronskog potpisa i sertifikata).

Jedan od potencijalnih procesnopravnih problema svakako bi mogao da bude i problem nekažnjavanja i nepostojanja odgovornosti zbog izvršenih krivičnih dela iz oblasti VT kriminala lica mlađih od 14 godina.[59] Pri postojanju argumentacije koja se tiče sve ubrzanijeg polnog i mentalnog sazrevanja ljudskih jedinki, te pri postojanju činjenice da su deca uzrasta 13-14 godina, neretko, vrsni poznavaoci korišćenja IT-a, mišljenja smo da bi starosnu granicu krivične odgovornosti trebalo „spustiti“ na odgovarajući kalendarski uzrast, u prilog čemu govori i statistika u pogledu kalendarskog uzrasta učinioca krivičnih dela uopšte. U sklopu navedenog, moralo bi da se preispita i pitanje stvarne nadležnosti sudova za suđenje maloletnim licima[60] zbog izvršenih krivičnih dela iz oblasti VT kriminala, s obzirom na to da u ovom trenutku pozitivnopravnim propisima ona nije data Posebnom odeljenju Okružnog suda u Beogradu za borbu protiv VT kriminala, pred kojim Posebno tužilaštvo za VTK postupa.

Najzad, ne sporeći argumentaciju pravnog stava Vrhovnog suda Republike Srbije, u pravnom stavu iznetom u presudi Kzz. br.10/06 od 16. marta 2006. godine, da radnja izvršenja krivičnog dela Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199 KZ-a opisana u presudi[61] mora da bude bliže određena objektom dela, odnosno nazivom autorskog dela i subjektom autorskog prava – moramo konstatovati da je isti i pored pozitivne intencije, ipak, implicirao znatne probleme u praksi, koji se možda ne bi mogli okarakterisati kao procesnopravni, ali ozbiljni, u svakom slučaju, jesu.

Naime, dosledno sprovodeći ovakav stav suda, svi državni organi koji se bave otkrivanjem, gonjenjem i suđenjem zbog krivičnog dela iz člana 199 Krivičnog zakonika,

[59] Deca koja nisu krivično odgovorna.
[60] Kategorija lica od 14 do 18 godina.
[61] Dakle, i u optužnim aktima tužilaštva.

dužni su da u svojim pismenim aktima navedu sve naslove autorskih dela, pri čemu tužilaštvo i sud i podatke koji se odnose na ošt. subjekte autorskih prava, u vidu nabrajanja njihovih imena, ili naziva distributera na koje su ova prava preneli. U „ozbiljnijim" slučajevima ulične, ili internet „piraterije", koji podrazumevaju količine zaplenjenih optičkih diskova od 1.000 do 15.000 komada, dispozitivi optužnih akata i presuda znaju da broje po 50 i više strana. Mišljenja smo da je u takvoj situaciji nužno iznaći neko razumno rešenje, s obzirom na neprimereno trošenje vremena i materijalnih resursa.

S obzirom na to da se navedeni stav Vrhovnog suda RS ne može osporiti, rešenje se može iznaći u inkorporiranju u procesni zakon odredaba člana 22 „novog" ZKP-a[62] kojim se definiše značenje izraza *„spis, pismeno, pošiljka i drugi dokumenti"*,[63] na koji način bi prepisi optužnih akata tužilaštva i odluka suda, osim eventualno izvornika, mogli da budu u celosti, ili samo delom – i u elektronskoj formi. U tom smislu ova odredba morala bi pretrpeti određene izmene, utoliko što bi se u samom tekstu na kraju rečenice, iza reči *„sadržane u spisima"*, unele reči *„kao i na prepise optužnih akata i odluka suda, ili njihovih delova, osim izvornika koji moraju da budu i u pismenoj formi"*. Ovakvo rešenje uvelo bi „na velika vrata" primenu elektronskog potpisa i elektronskog sertifikata, što podrazumeva ozbiljnu pripremu za njihovu primenu.

U sklopu drugih problema s kojima se u svakodnevnom radu susreću državni organi na poslu suzbijanja visokotehnološkog kriminala, svakako treba istaći i one materijalne, koji se prvenstveno očituju u nepostojanju odgovarajućih uslova rada i adekvatne tehničke opreme. Kao takvi, oni su rezultat još nedovoljnog postojanja svesti o opasnostima koje VT kriminal nosi i srazmerama štete koju prouzrokuje).

[62] Sa odloženom primenom do 2010, koja neće ni uslediti.

[63] Spis, pismeno, pošiljka i drugi dokumenti mogu da budu i u elektronskom obliku i sadržani u odgovarajućim nosiocima podataka, kao što su CD, drugi diskovi, magnetne trake i bilo koji drugi nosioci podataka, što se odnosi i na dokaze i isprave sadržane u spisima.

Dosadašnja iskustva Srbije u borbi protiv VTK

1. Specijalna policijska jedinica za visokotehnološki kriminal

Proces osnivanja posebnih organa po Zakonu o osnivanju i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala trajao je dve i po godine. Poslednja karika u tom lancu koja je osnovana jeste Posebna služba u okviru MUP RS, koja je počela sa radom u aprilu 2008. godine. Početak njihovog rada obeležen je prvo rešavanjem problema broja ljudi i prostornog smeštaja, kao i snabdevanjem kompjuterskom opremom. Bez obzira na sve ove probleme, uspeli su da u kratkom periodu ostvare određene rezultate.

Prema posebnom zakonu, oni su pod direktnom ingerencijom posebnog tužioca za visokotehnološki kriminal, pa su rezultati rada, kao i vrsta krivičnih dela za koja su podnošene krivične prijave, uslovljeni nedostatkom stvarne nadležnosti, o kojoj je već bilo reči u prethodnim poglavljima.

Naime, u toku 2008. godine podnete su krivične prijave protiv trideset pet lica, oduzeta su 53 računara, kao i 49.000 optičkih diskova. Karakteristika rada u ovom periodu ogleda se u činjenici da se 90 odsto predmeta odnosi na izvršenje krivičnog dela iz člana 199 KZ.

Međutim, već za prvih pet meseci 2009. godine, situacija se menja i u statistici se pojavljuju i krivične prijave iz glave Krivičnog zakonika, koje se odnose na bezbednost računarskih podataka.

Tako, podnete su krivične prijave za krivično delo Ugrožavanje sigurnosti iz člana 138 KZ, Izazivanje rasne, nacionalne i verske mržnje iz člana 317 KZ. Podnete su po dve krivične prijave zbog krivičnih dela Računarska sabotaža iz člana 299 KZ, Neovlašćen pristup zaštićenom računaru iz člana 302 KZ, kao i Računarska prevara iz člana 301 KZ.

Ono što već sad možemo da zaključimo jeste da je povećan broj izvršenja krivičnih dela Računarske prevare i zloupotrebe platnih kartica iz člana 225 Krivičnog zakonika.

2. Specijalno tužilaštvo za visokotehnološki kriminal

Posebno tužilaštvo za borbu protiv visokotehnološkog kriminala ovlašćeno je za krivično gonjenje učinilaca krivičnih dela visokotehnološkog kriminala koji, u smislu ovog zakona, predstavlja vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku,[64] dok se pod proizvodima u elektronskom obliku posebno podrazumevaju računarski programi i autorska dela koja mogu da se upotrebe u elektronskom obliku. Posebno tužilaštvo za borbu protiv visokotehnološkog kriminala je organizaciono formirano kao posebno odeljenje Okružnog javnog tužilaštva u Beogradu. Radom Posebnog tužilaštva rukovodi posebni tužilac za visokotehnološki kriminal, koga postavlja republički javni tužilac iz reda javnih tužilaca i njihovih zamenika koji ispunjavaju uslove za izbor za zamenika okružnog javnog tužioca uz pismenu saglasnost lica koje se postavlja. Posebni tužilac se postavlja na četiri godine i može da bude ponovo postavljen, a po prestanku funkcije vraća se na funkciju koju je vršio pre postavljenja. Posebni tužilac podnosi pred-

Posebno tužilaštvo za borbu protiv visokotehnološkog kriminala ovlašćeno je za krivično gonjenje učinilaca krivičnih dela visokotehnološkog kriminala koji, u smislu ovog zakona, predstavlja vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, dok se pod proizvodima u elektronskom obliku posebno podrazumevaju računarski programi i autorska dela koja mogu da se upotrebe u elektronskom obliku.

[64] Član 2 Zakona o organizaciji i nadležnosti državnih organa u borbi protiv visokotehnološkog kriminala.

log o unutrašnjoj organizaciji i sistematizaciji radnih mesta u okviru Posebnog tužilaštva, o čemu odluku donosi okružni javni tužilac uz prethodnu saglasnost ministra nadležnog za poslove pravosuđa. Takođe, na predlog posebnog tužioca republički javni tužilac donosi odluku o upućivanju javnog tužioca ili zamenika javnog tužioca na rad u Posebno tužilaštvo, uz pismenu saglasnost tog lica, na period ne duži od dve godine; upućivanje uz ispunjenje iste procedure može da bude produženo.

Specifičnost rada Posebnog tužilaštva za visokotehnološki kriminal ogleda se u stvarnoj i mesnoj nadležnosti koja je koncipirana drugačije u odnosu na tužilaštva opšte nadležnosti. Naime, mesna nadležnost Posebnog tužilaštva prostire se na celoj teritoriji Republike Srbije, dok je stvarna nadležnost takođe specifična i ustanovljena samo za određena krivična dela. Stvarna nadležnost je definisana članom 3 Zakona o organizaciji i nadležnosti državnih organa u borbi protiv visokotehnološkog kriminala i odnosi se na krivična dela protiv bezbednosti računarskih podataka određenih krivičnim zakonom (glava XXVII Krivičnog zakonika), kao i na krivična dela protiv intelektualne svojine (glava XX Krivičnog zakonika), imovine (glava XXI Krivičnog zakonika) i pravnog saobraćaja (glava XXXII Krivičnog zakonika), kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj primeraka autorskih dela prelazi 500 ili nastala materijalna šteta prelazi iznos od 850.000 dinara. Kada dođe do saznanja da je u jednom krivičnom predmetu reč o nekom od pobrojanih krivičnih dela, posebni tužilac se u pismenoj formi obraća republičkom javnom tužiocu zahtevajući od njega da mu poveri ili prenese nadležnost za postupanje u tom krivičnom predmetu.

Za obavljanje poslova kojima se ostvaruje osnovna funkcija u okviru Posebnog tužilaštva obrazovane su organizacione jedinice: Krivično odeljenje i Sekretarijat u okviru koga postoje unutrašnje organizacione jedinice – pisarnica, daktilo biro, sektor informatike i analitike i sektor za odnose sa javnošću. U Krivičnom odeljenju se postupa po svim predmetima iz krivičnopravne materije, koji spadaju u stvarnu nad-

ležnost Posebnog tužilaštva od početka pretkrivičnog postupka do završetka glavnog pretresa, kao i u postupcima po pravnim lekovima. Pored posebnog tužioca za visokotehnološki kriminal, u Krivičnom odeljenju sada postupaju tri zamenika posebnog tužioca iako je po sistematizaciji predviđeno da postupa sedam zamenika. Razlog tome je u nedostatku službenih prostorija sa kojima se suočava Posebno tužilaštvo. Naime, prostorije Posebnog tužilaštva trenutno se nalaze u okviru službenih prostorija Okružnog javnog tužilaštva u Beogradu. Ovakva situacija ne odgovara prostornim potrebama Posebnog tužilaštva zbog čega nije moguće u potpunosti popuniti sistematizaciju radnih mesta odobrenu od strane ministra pravde i predviđenu kadrovskim planom. Navedena situacija se negativno odražava na popunjenost zamenika tužilaca i tužilačkih saradnika, ali i na administrativno osoblje. Usled toga, normativne i analitičke poslove preuzima posebni tužilac uz pomoć sekretara, a sekretar obavlja i poslove administrativno-tehničkog sekretara imajući u vidu da ovo radno mesto još nije popunjeno. Takođe, posebni tužilac obavlja i sve poslove koji se odnose na kontakte sa javnošću, a u njegovom odsustvu ove poslove obavlja prvi zamenik posebnog tužioca. Navedeni poslovi se inače nalaze u okviru Sektora za odnose sa javnošću, koji će biti formiran nakon rešavanja pomenutih problema. Konačno, Posebno tužilaštvo ne raspolaže ni odgovarajućim prostorom za prijem i skladištenje predmeta koji su oduzeti od izvršilaca krivičnih dela visokotehnološkog kriminala i koji služe kao dokaz u krivičnom postupku. Primera radi, policijski službenici koji rade na otkrivanju učinilaca krivičnih dela visokotehnološkog kriminala su u toku 2008. godine od izvršilaca oduzeli ukupno 53 računara, 48.400 optičkih nosača slike i zvuka na kojima se nalazi ukupno 171.160 autorskih dela, što takođe pruža dobru sliku sa kakvim problemom se suočava Posebno tužilaštvo zbog nedostatka adekvatnog prostora. Radi rešavanja predmetnog problema od strane nadležnih institucija, Posebno tužilaštvo je primilo na korišćenje službene prostorije za koje očekujemo da će po odobrenju potrebnih finansijskih sredstava i renoviranja u toku 2009. godine biti i useljene.

Što se tiče broja i strukture krivičnih predmeta koji se nalaze u radu u Posebnom tužilaštvu, ukupan broj predmeta zaveden u upisnicima za 2008. godinu jeste 184, dok su krivične prijave podnete protiv 166 lica, što predstavlja znatan porast u odnosu na 2007. i broj od 122 lica. Zahtevi za sprovođenje istrage podneti su protiv 147 lica, što je porast u odnosu na 2007. godinu i broj od 62 lica, dok je optužnica podignuta protiv 74 lica, što je takođe porast u odnosu na 21 lice protiv kojih je u toku 2007. godine podignuta optužnica. Struktura krivičnih dela za koja Posebno tužilaštvo preduzima krivično gonjenje pokazuje da se protiv 137 lica vodi postupak zbog krivičnih dela protiv intelektualne svojine, protiv 10 lica zbog krivičnih dela protiv imovine, a protiv 17 lica zbog krivičnih dela protiv bezbednosti računarskih podataka. Vidljivo je da se pretežan broj krivičnih predmeta u kojima postupa Posebno tužilaštvo odnosi na krivična dela čiji je objekat zaštite autorsko delo. Najveći broj ovih krivičnih predmeta odnosi se na neovlašćeno umnožavanje i stavljanje u promet zakonom zaštićenih autorskih dela.[65] Razlog tome je u činjenici da izvršilac ovih krivičnih dela može da bude svako lice, da nisu potrebna specijalizovana znanja iz oblasti informacionih ili komunikacionih tehnologija, te da su sredstva za izvršenje ovih krivičnih dela jeftina i lako dostupna svima. Navedeni statistički podaci, međutim, ne pružaju pravu sliku o aktivnostima Posebnog tužilaštva na rasvetljavanju izvršenih krivičnih dela visokotehnološkog kriminala na teritoriji Republike Srbije s obzirom na manjkavost posebnog zakona kojim je određena stvarna nadležnost posebnog tužilaštva. Naime, u stvarnu nadležnost nisu ušla krivična dela falsifikovanja i zloupotrebe platnih kartica[66] i internet pedofilije, odnosno krivično delo prikazivanje pornografskog materijala i iskorišćavanje dece za pornografiju,[67] koja po svojoj prirodi i načinu izvršenja svakako spadaju u stvarnu nadležnost Posebnog

[65] Član 199 Krivičnog zakonika Republike Srbije.
[66] Član 225 Krivičnog zakonika Republike Srbije.
[67] Član 185 Krivičnog zakonika Republike Srbije.

tužilaštva. Stoga, od strane tužilaštva podneta je inicijativa Ministarstvu pravde radi izmene Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala u pravcu proširenja stvarne nadležnosti. Pored toga, u pogledu krivičnih dela protiv intelektualne svojine nadležnost Posebnog tužilaštva prepliće se sa nadležnošću tužilaštava opšte nadležnosti imajući u vidu da ukoliko je reč o količini ispod 500 komada autorskih dela, postupaju tužilaštva opšte nadležnosti, a ukoliko je u pitanju količina od preko 500 komada ili pričinjena šteta u iznosu od preko 850.000 dinara, postupa Posebno tužilaštvo. Radi ilustracije obima posla Posebnog tužilaštva u pretkrivičnom postupku i sagledavanja učestalosti izvršenja krivičnih dela visokotehnološkog kriminala, prema podacima Ministarstva unutrašnjih poslova, u toku 2008. godine izvršeno je ukupno 1.313 krivičnih dela visokotehnološkog kriminala, a ukupno 639 lica je prijavljeno da su izvršila neko od krivičnih dela ove vrste kriminala.

3. Dosadašnja sudska praksa

Ono što se može primetiti u dosadašnjoj sudskoj praksi posebnog sudskog Veća za borbu protiv visokotehnološkog kriminala jeste da se najveći broj krivičnih predmeta odnosi na krivična dela protiv intelektualne svojine, u kojima je objekat zaštite autorsko delo, i to na krivično delo neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199 Krivičnog zakonika Republike Srbije.

Sudska praksa Veća za borbu protiv visokotehnološkog kriminala Okružnog suda u Beogradu pre svega je određena zakonom postavljenim okvirom, odnosno odredbama kojima je regulisana stvarna nadležnost ovog suda za suđenje krivičnih dela visokotehnološkog kriminala.

Ono što se može primetiti u dosadašnjoj sudskoj praksi posebnog sudskog Veća za borbu protiv visokotehnološkog kriminala jeste da se najveći broj krivičnih predmeta odnosi na krivična dela protiv intelektualne svojine, u kojima je objekat zaštite autorsko delo, i to na krivično delo neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199 Krivičnog zakonika Republike Srbije.[68] U pogledu ostalih krivičnih dela iz oblasti visokotehnološkog kriminala koja su predmet

[68] „Službeni glasnik RS“, br. 85/05, 88/05, 107/05.

sudskog postupka, najzastupljeniji su prevara iz člana 208 KZ,[69] u kojoj se kao sredstvo izvršenja krivičnog dela pojavljuje računar, računarska prevara iz člana 301 KZ, računarska sabotaža iz člana 299 KZ i neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka iz člana 302 KZ.

U pogledu krivičnog dela neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava može se reći da je najzastupljeniji oblik izvršenja ovog krivičnog dela koji je bio predmet presuđenja suda neovlašćeno umnožavanje, držanje radi stavljanja u promet i stavljanje u promet neovlašćeno umnoženih primeraka autorskih dela snimljenih na optičke nosače slike i zvuka u vidu CD-ova i DVD-ova u cilju pribavljanja protivpravne imovinske koristi za sebe ili drugoga. Najčešći oblici stavljanja u promet su u vidu ulične prodaje i prodaje oglašavanjem preko interneta. U slučajevima prodaje putem interneta, učinilac ovog krivičnog dela oglašava se na internet sajtovima ostavljajući kao kontakt adresu elektronske pošte ili broj mobilnog telefona, koji služe za naručivanje autorskih dela, pa po prijemu narudžbe vrši neovlašćeno umnožavanje naslova autorskih dela na prazne optičke nosače slike i zvuka, najčešće na svom personalnom računaru na adresi prebivališta ili boravišta. Nabavljanje autorskih dela koja su predmet stavljanja u promet vrši se takođe putem interneta preko bit *torrenta* ili *rapdishare* mreže, ili kupovinom legalnih kopija u za to ovlašćenim prodavnicama. Ovako neovlašćeno umnoženi primerci autorskih dela naručiocima se dostavljaju korišćenjem usluga JP PTT Srbije – plaćanje pouzećem, odnosno podizanje novca nakon prijema obaveštenja o završenoj isporuci u poslovnicama JP PTT-a. Predmet presuđenja ovih sudskih postupaka su samo lica koja stavljaju u promet primerke autorskih dela ili učestvuju u radnji izvršenja kroz neki od oblika saizvršilaštva, dok lica koja su naručioci nisu obuhvaćena ovakvim krivičnim postupkom, s obzirom na to da samo posedovanje ovako neovlašćeno

[69] Krivični zakonik.

Za krivično delo prevare, u kome se kao sredstvo izvršenja koristi računar, karakteristično je da učinilac najčešće putem interneta lažno prikazuje određene činjenice koje oštećenog dovode u zabludu i na taj način ga navodi da izvrši određenu radnju na štetu svoje ili tuđe imovine, a sve u nameri pribavljanja protivpravne imovinske koristi.

umnoženih primeraka autorskih dela nije inkriminisano krivičnim zakonodavstvom. Što se tiče broja autorskih dela koja su predmet izvršenja ovog krivičnog dela, u slučaju ulične prodaje obično je reč o nekoliko stotina komada, dok je u slučaju stavljanja u promet putem interneta broj daleko veći i kreće se od nekoliko hiljada do nekoliko desetina hiljada komada. Najveći do sada pronađeni broj neovlašćeno umnoženih primeraka autorskih dela stavljenih u promet, koji je bio predmet sudskog postupka, jeste 28.800 komada.

Za krivično delo prevare, u kome se kao sredstvo izvršenja koristi računar, karakteristično je da učinilac najčešće putem interneta lažno prikazuje određene činjenice koje oštećenog dovode u zabludu i na taj način ga navodi da izvrši određenu radnju na štetu svoje ili tuđe imovine, a sve u nameri pribavljanja protivpravne imovinske koristi. Za krivična dela računarske prevare i računarske sabotaže karakterističan način izvršenja, koji je bio predmet sudskih postupaka, jeste da se unošenjem netačnog podatka, ili brisanjem ili izmenom podataka, utiče na elektronsku obradu podataka, u nameri da se u slučaju računarske prevare pribavi protivpravna imovinska korist, a u slučaju računarske sabotaže onemogući ili znatno omete postupak elektronske obrade ili prenosa podataka značajnih za državne organe, javne službe, preduzeća ili druge subjekte.

Sadržaj

УДРУЖЕЊЕ ЈАВНИХ ТУЖИЛАЦА И
ЗАМЕНИКА ЈАВНИХ ТУЖИЛАЦА СРБИЈЕ

www.aecid.es