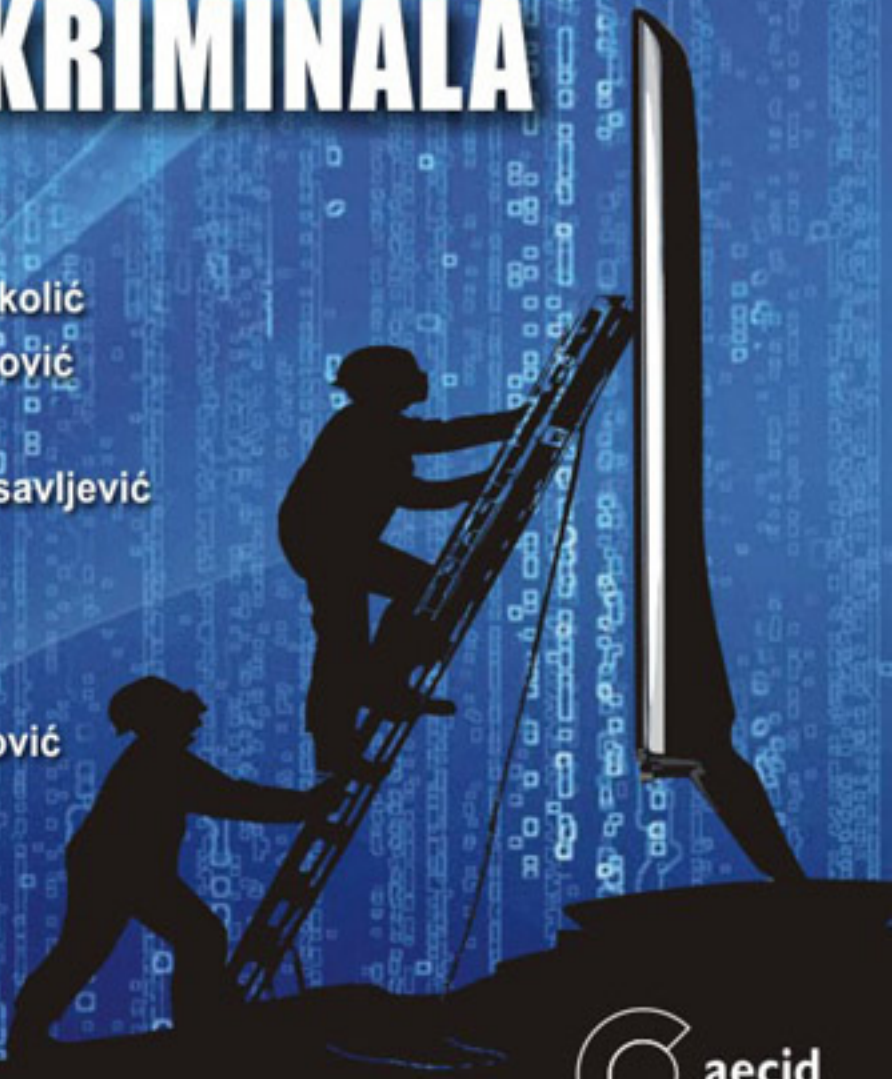
УДРУЖЕЊЕ ЈАВНИХ ТУЖИЛАЦА И ЗАМЕНИКА ЈАВНИХ ТУЖИЛАЦА СРБИЈЕ

SUZBIJANJE VISOKOTEHNOLOŠKOG KRIMINALA

Lidija Komlen Nikolić
Radoje Gvozdenović
Saša Radulović
Aleksandar Milosavljević
Ranko Jerković
Vladan Živković
Saša Živanović
mr Mario Reljanović
Ivan Aleksić



aecid

Kao Ambasadoru Španije u Srbiji, zadovoljstvo mi je da srpskoj javnosti predstavim ovo delo posvećeno prevenciji informatičkog kriminala, koje je praktični i opipljivi rezultat projekta saradnje izmedju Španske agencije za međunarodnu razvojnu saradnju (AECID) i Udruženja javnih tužilaca i zamenika javnih tužilaca Srbije tokom 2009. godine.

Ovo delo ne pretenduje da bude samo puka teorijska studija, već praktični dokument sa preporukama i predlozima koji će omogućiti napredak u borbi protiv ove vrste kriminala, koji u današnje vreme predstavlja opasan i hitan zadatak za naša društva.

Iskreno se nadam da će ovo delo, koje je dokaz uspešne saradnje sa profesionalnim organizacijama Srbije, doprineti borbi protiv kriminala a time i podržati jačanje pravne države i reforme pravosuđa, koji su među glavnim ciljevima španske saradnje u Srbiji.

Injigo de Palasio Espanja
Ambasador Španije u Srbiji

Izdavač:
Udruženje javnih tužilaca i
zamenika javnih tužilaca Srbije

Autori:
Lidija Komlen Nikolić
Radoje Gvozdenović
Saša Radulović
Aleksandar Milosavljević
Ranko Jerković
Vladan Živković
Saša Živanović
Mr Mario Reljanović
Ivan Aleksić

Tehničko uređenje:
Siniša Lekić

Tiraž:
500

Štampa:
ATC Beograd

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

343.533::004

SUZBIJANJE visokotehnološkog kriminala / Lidija Komlen Nikolić ... [et al.]. - Beograd : Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, 2010 (Beograd : ATC). - 284 str. : ilustr. ; 24 cm

Tiraž 500. - Napomene i bibliografske reference uz tekst.

ISBN 978-86-87259-10-2

COBISS. SR-ID 172571660

Lidija Komlen Nikolić ◆ Radoje Gvozdenović ◆ Saša Radulović ◆
Aleksandar Milosavljević ◆ Ranko Jerković ◆ Vladan Živković ◆
Saša Živanović ◆ mr Mario Reljanović ◆ Ivan Aleksić

SUZBIJANJE VISOKOTEHNOLOŠKOG KRIMINALA

УДРУЖЕЊЕ ЈАВНИХ ТУЖИЛАЦА
И ЗАМЕНИКА ЈАВНИХ ТУЖИЛАЦА СРБИЈЕ

PREDGOVOR

Sadašnjost se ogleda u činjenici da je internet povezao oko dve stotine zemalja, kao i činjenici da je napredak tehnologije u poslednjih dvadesetak godina dostigao granice potpune kompjuterske kontrole najvažnijih društvenih procesa. Logično je da iz ovako velikog procesa proisteknu i zloupotrebe.

Pojedini autori će ga nazvati kompjuterskim kriminalom, neki će ga zvati računarskim kriminalom, a u Srbiji zvaničan naziv je visokotehnološki kriminal.

Prema najnovijim podacima, u tzv. sajber (*cyber)* prostoru nalazi se više od milijardu i po ljudi. To je uslovilo nova pravila ponašanja, nove običaje, nove opasnosti.

Visokotehnološki kriminal je globalni problem koji zahteva puno učešće i saradnju društvenog i privatnog sektora u svim zemljama.

Kad bi samo jedan odsto od milijardu i po ljudi imao nameru da korišćenjem informacionih tehnologija čini krivična dela, to bi dovelo u situaciju da na svetskom nivou imamo 15 miliona potencijalnih prestupnika.

Međutim, mora da postoji svest o postojanju ozbiljnosti problema.

Monografija o visokotehnološkom kriminalu jeste pokušaj da različite aspekte visokotehnološkog kriminala približimo, pre svega stručnoj javnosti, potom i kolegama unutar javnotužilačke organizacije.

Na projektu monografije, pored saradnika iz Instituta za uporedno pravo i pripadnika MUP RS, učestvovali su i svi zaposleni u tužilaštvu za visokotehnološki kriminal sa punom verom u opravdanost postojanja ozbiljnih institucija za borbu protiv visokotehnološkog kriminala.

KOLEKTIV TUŽILAŠTVA
ZA VISOKOTEHNOLOŠKI KRIMINAL

I

OSNOVNI POJMOVI I RAZVOJ VISOKOTEHNOLOŠKOG KRIMINALA

1. UVODNA RAZMATRANJA

Sada već davne 1936. godine, Konrad Zuse je sastavio prvi binarni računar.[1] Godine 1953. kompanija *International Bussiness Machines*, kasnije mnogo poznatija po skraćenici svoga naziva IBM, napravila je moderan računar, a već sledeće godine i prvi računarski jezik za programiranje. Godine 1964. nastao je prvi prototip operativnog sistema *Windows*, a 1970. američka kompanija *Intel* napravila je prvi računar koristeći revolucionarnu tehnologiju mikročipa. Godinu dana pre toga nastao je *Arpanet*, preteča interneta kakav svi danas poznajemo i koristimo. Od tih dana stvari su počele da se razvijaju geometrijskom progresijom: 1973 – pojavljuje se *Ethernet*; 1974–1976 – prvi personalni računari *IBM, Apple* i *Commodore*; 1981 – prvi kućni računar sa *MS DOS* sistemom; konačno, 1985. godine nastaje *Windows* sistem koji opstaje u različitim verzijama do današnjih dana, naravno uz pojavu mnogih drugih operativnih sistema i neprestano usavršavanje računara.[2]

Pojava modernih računara i korisničkih programa za najširu upotrebu definitivno je promenila živote ljudi širom sveta. Računari su danas svakodnevica i ne može se zamisliti osoba koja se bavi čak i najobičnijim poslovima a da ne poseduje osnovno obrazovanje o radu na njima. Računari danas služe za ubrzavanje osnovnih kancelarijskih poslova, ali i za složena projektovanja, baze podataka, komunikaciju, informisanje, edukaciju i zabavu. Uporedo sa ovakvim razvojem računara razvile su se i računarske mreže (ili računarski sistemi), od kojih je zasigurno najpoznatija tzv. svetska mreža – internet. Ekspanzija i „invazija“ računara u gotovo svaki dom na planeti neminovno su donele i nove oblike njihovog korišćenja radi ostvarivanja različitih poslova, koji često nisu u skladu sa zakonom.

Prvi računari bili su autonomni, izolovani od ostalih računara. Međutim, računarske mreže su osmišljene u veoma kratkom periodu nakon početka masovnije proizvodnje računara, pre svega da bi se podaci koji se nalaze na različitim računarima mogli deliti (engl. *share*) i distribuirati pojedinim ili svim korisnicima određene mreže. Danas se primeri ovakvih mreža mogu naći u svakoj kompaniji čiji službenici koriste računare u svom poslu, povezane u jedinstveni sistem radi lakše i brže međusobne komunikacije, eventualno uz

[1] Interesantna priča o nastanku ovog računara može se pročitati na internet adresi: *http://www.epemag.com/zuse/part3a.htm*, 1. 5. 2009.

[2] Isečak iz istorije razvoja računara preuzet iz članka *The History of Computers,* sa internet adrese: *http://inventors.about.com/library/blcoindex.htm*, 1. 5. 2009.

različite nivoe pristupa informacijama. Istovremeno, način na koji računari i računarske mreže funkcionišu postali su zahvaljujući korisničkim programima jednostavniji i pristupačniji najvećem broju ljudi koji se mogu bez problema za nekoliko dana obučiti za osnove rada na računaru. Na taj način se polako naziru osnovne komponente za pojavu i delovanje visokotehnološkog kriminala: lako dostupno oruđe za vršenje nezakonitih radnji, ranjivost sistema i veliki broj novih korisnika koji, osim uobičajenih ljudskih slabosti, imaju još neke izuzetno bitne za uspeh kriminalaca: neiskustvo i neznanje.

Računari i računarske mreže nisu, međutim, jedina oruđa koja se mogu koristiti za činjenje ove vrste nezakonitih radnji. Gotovo svake godine se pojave nove generacije različitih uređaja koji su originalno osmišljeni za prenos informacija, komunikaciju i zabavu. Ove inovacije su pozitivne jer čine nove tehnologije jeftinijim, pristupačnijim, jednostavnijim, ali imaju i svoju lošu stranu – prosečan korisnik nema dovoljno volje, vremena i mogućnosti da se upozna sa opasnostima koje sa sobom nosi korišćenje ovih uređaja, na taj način postajući potencijalna žrtva iskusnih i daleko bolje edukovanih pojedinaca sa nečasnim namerama. Visokotehnološki kriminal je tako postao svakodnevica, a fantastičan razvoj tehnologija je uslovio i neverovatnu diferencijaciju vrsta nedozvoljenih dela koja se mogu izvršiti njihovim korišćenjem, od onih naivnih i bezopasnih koja se uglavnom vezuju za reklamiranje različitih proizvoda, do veoma opasnih ponašanja koja spadaju među teška (ponekad čak i najteža) krivična dela u mnogim nacionalnim zakonodavstvima.

Računarske mreže razvile su se kao posledica potrebe vojske i različitih vladinih institucija u SAD. Ove mreže su bile samo za internu upotrebu, sa jakom zaštitom od nedozvoljenog upada i korišćenja, i bez ikakve namere da se komercijalizuju. Međutim, na takvim modelima je nastalo nekoliko civilnih mreža, najčešće na različitim univerzitetima koji su eksperimentisali sa računarskim mrežama kao novim vidom komunikacije između korisnika. Ove mreže su tokom poslednjih 15 godina potisnute razvojem globalne računarske mreže – interneta. Internet je od luksuza i apstraktnog eksperimenta, nepoznatog većini ljudi, postao neminovnost i sredstvo informisanja i komunikacije, zabave i edukacije koje svakodnevno koristi milijardu i po ljudi širom planete (videti Tabelu 1). I taj broj se svake godine uvećava novim korisnicima, pre svega iz mnogoljudnih azijskih zemalja kao što su Kina i Indija (videti tabele 2 i 3).

Region	Br. stanovnika	Korisnici 2000.	Korisnici 2008.	% popul.	% rast 2000-08.
Afrika	975. 330. 899	4. 514. 400	54. 171. 500	5. 6	1100. 0
Azija	3. 780. 819. 792	114. 304. 000	650. 361. 843	17. 2	469. 0
Evropa	803. 903. 540	105. 096. 093	390. 141. 073	48. 5	271. 2
Bliski istok	196. 767. 614	3. 284. 800	45. 861. 346	23. 3	1296. 2
Severna Amerika	337. 572. 949	108. 096. 800	246. 822. 936	73. 1	128. 3
Lat. Amerika & Karibi	581. 249. 892	18. 068. 919	166. 360. 735	28. 6	820. 7
Australija i Okeanija	34. 384. 384	7. 620. 480	20. 593. 751	59. 9	170. 2
Svet ukupno	6. 710. 029. 070	360. 985. 492	1. 574. 313. 184	23. 5	336. 1

Tabela 1: Broj korisnika interneta prema regijama[3]

	Država	Broj korisnika	% u uk. broju	% rast 2000-2008.
1	Kina	253. 000. 000	17. 3	1024. 4
2	SAD	220. 141. 969	15. 0	130. 9
3	Japan	94. 000. 000	6. 4	99. 7
4	Indija	60. 000. 000	4. 1	1100. 0
5	Nemačka	52. 533. 914	3. 6	118. 9
6	Brazil	50. 000. 000	3. 4	900. 0
7	Ujedinjeno Kraljevstvo	41. 817. 847	2. 9	171. 5
8	Francuska	36. 153. 327	2. 5	325. 3
9	Južna Koreja	34. 820. 000	2. 4	82. 9
10	Italija	34. 708. 144	2. 4	162. 9
	Prvih 20 država uk.	1. 115. 713. 572	76. 2	284. 5
	Ostatak sveta	347. 918. 789	23. 8	391. 2
	Ukupno – svet	1. 463. 632. 361	100	305. 5

Tabela 2: Države koje imaju najviše korisnika na internetu sa trendom rasta[4]

[3] Stanje na dan 31. 12. 2008. godine. Izvor: *http://www.internetworldstats.com/stats.htm*, 1. 5. 2009.

Najviši procenat korisnika				Najniži procenat korisnika			
	Država	**Broj korisnika**	**% uk. popul.**		**Država**	**Broj korisnika**	**% uk. popul.**
1	Holandija	15. 000. 000	90. 1	**1**	Bangladeš	500. 000	0. 3
2	Norveška	4. 074. 100	87. 8	**2**	Kamerun	370. 000	0. 7
3	Kanada	28. 000. 000	84. 3	**3**	Tanzanija	400. 000	0. 8
4	Novi Zeland	3. 360. 000	80. 5	**4**	Zambija	500. 000	1
5	Australija	16. 355. 427	79. 4	**5**	Gana	650. 000	1. 3
6	Švedska	7. 000. 000	77. 4	**6**	Avganistan	580. 000	1. 8
7	Japan	94. 124. 000	73. 8	**7**	Sudan	1. 500. 000	3. 7
8	Portugal	7. 782. 760	72. 9	**8**	Šri Lanka	771. 700	3. 7
9	SAD	215. 088. 000	71. 4	**9**	Gvatemala	1. 327. 000	4. 7
10	Južna Koreja	34. 820. 000	70. 7	**10**	Indija	61. 431. 000	5. 4
11	Hongkong	4. 878. 713	69. 5	**11**	Uzbekistan	1. 745. 000	6. 2
12	Ujedinjeno Kaljevstvo	41. 817. 847	68. 9	**12**	Bolivija	580. 000	6. 3

Tabela 3: Države sa najvišim i najnižim procentima korisnika interneta u odnosu na ukupnu populaciju[5]

Internet se razvio osvajajući ne samo nove teritorije zemljine kugle i postajući dostupan u gotovo svakoj državi na svetu. On je takođe uznapredovao korišćenjem novih tehnologija transfera podataka, koji danas omogućavaju prenos neslućene količine informacija za samo nekoliko sekundi. Ova činjenica je veoma važna kada je reč o delima visokotehnološkog kriminala vezanim za kršenje autorskih prava.

Internet se može koristiti i za druge oblike aktivnosti kojima se čini šteta drugima, bez obzira na to da li je u pitanju samo zla namera pojedinca ili grupe, ili plan za ostvarivanje neke finansijske ili druge dobiti. Godine 1998.

[4] Stanje na dan 31. 12. 2008. godine. Izvor: *http://www.internetworldstats.com/top20.htm*, 1. 5. 2009.

[5] U pitanju je 100 država širom sveta u kojima su dostupni podaci o korišćenju interneta. Stanje na dan 31. 12. 2008. godine. Izvor:
http://en.wikipedia.org/wiki/List_of_countries_by_number_of_internet_users, 1. 5. 2009.

desio se prvi masovni napad na internetu, kada je u mrežu ubačen samoreplicirajući program koji uništava podatke na računarima i širi se samostalno po mreži (tzv. „crv“, engl. *worm*), koji je napravio veliku štetu i praktično uništio gotovo trećinu internet sadržaja u SAD. U narednim godinama gotovo da nije bilo internet prezentacije važnije vladine institucije u SAD, multinacionalne korporacije, međunarodne organizacije i sl., koja nije „hakovana“ (engl. *hacked*) – čiji sadržaj nije izbrisan, zamenjen drugim sadržajem ili sklonjen na izvesno vreme sa interneta, tako što bi neka osoba (osobe) neovlašćeno pristupila računaru-serveru na kome se čuvaju podaci tih sajtova. Godine 2003. pušten je do sada najdestruktivniji crv, tzv. „safirni crv“, koji je u roku od deset minuta zarazio 90 odsto računarskih sistema na planeti koji nisu imali (adekvatnu) zaštitu. Prema rečima Dejvida Perija (David Perry), direktora sektora za obrazovanje kompanije *Trend Micro* koja se bavi bezbednošću računara, napadi na računarske mreže postaju sve sofisticiraniji i teži za uočavanje i odbranu, ali i sve više okrenuti lukrativnoj dimenziji ove aktivnosti.[6] Uporedo sa tim, ponekad čak i simpatičnim i naivnim pokušajima da se skrene pažnja na određeni problem ili da se izrazi protest zbog postupanja neke države ili organizacije, nastale su i prve ozbiljnije finansijske prevare, naročito nakon pojave elektronskog bankarstva sredinom devedesetih godina prošlog veka i početkom korišćenja platnih kartica putem interneta. Na taj način su stvorene pretpostavke za rađanje modernog visokotehnološkog kriminala.[7]

Život je daleko ispred mogućnosti zakonodavca da inkriminiše sve potencijalno opasne društvene pojave koje su vezane za savremene tehnologije. Broj dela koja se mogu podvesti čak i pod najrestriktivnije i najuže definicije sajber kriminala (*cybercrime*) gotovo se svakodnevno uvećava. Klasifikacija takvih ponašanja je teška zato što se ne mogu utvrditi kriterijumi koji će određena dela svrstati isključivo u jednu kategoriju, dok, sa druge strane, pojave novih načina zloupotrebe nužno iziskuju i proširenje pomenute liste kriterijuma. Sa druge strane, više je nego potrebno identifikovati i na sistematičan način razdvojiti poželjna i dozvoljena ponašanja od onih

[6] Izvor: Michael Coren, *Cyber-crime bigger threat then cyber-terror*, CNN International, 24. 1. 2005. (*http://www.cnn.com/2005/TECH/internet/01/18/cyber.security*, 1. 5. 2009).

[7] Koliko je visokotehnološki kriminal opasan, može se videti iz napada koji se desio u februaru 2007. godine, kada su „hakeri“ simultano napali – u cilju potpunog onesposobljavanja – šest od trinaest tzv. *root* servera na internetu. Da su uspeli u svojoj nameri, internet bi kao takav u potpunosti prestao da funkcioniše. Na sreću, samo su dva servera pretrpela značajnije posledice (izvor: *http://www.crime-research.org/articles/threat-ti-internet*, 1. 3. 2009). Zanimljivu priču o „tradicionalnom“ visokotehnološkom kriminalu videti na internet adresi: *http://cybercrime.planetindia net/intro.htm*, 1. 5. 2009.

koja zloupotrebom tehnologije nanose ogromnu štetu pojedincima, organizacijama i preduzećima širom sveta svake godine.[8] Pavan Dugal, predsednik međunarodne organizacije koja se bavi izučavanjem visokotehnološkog kriminala *Cyberlaws*, izneo je jednostavnu podelu koja zadovoljava osnovne pretpostavke analize, ali ne pomaže mnogo detaljnijoj klasifikaciji. Dugal deli sva krivična dela iz ove grupe na: dela protiv ličnosti, dela protiv imovine i dela protiv države.[9]

Nije svrsishodno po svaku cenu praviti veštačke podele, iako je važno razdvojiti visokotehnološki od ostalih oblika kriminala, kako bi se on mogao efikasno suzbijati. Međutim, koliko god kategorija tom podelom obuhvatili, uvek će neko delo izmaći upotrebljenoj logici i ostati po strani. Adam Graycar, direktor Kriminološkog instituta Australije, pokušao je da prevaziđe ovaj problem navođenjem devet kategorija sajber kriminala: dela protiv telekomunikacionih službi, komunikacija u cilju zločinačkog udruživanja, telekomunikaciona piraterija, rasturanje materijala „neprikladnog" sadržaja, pranje novca i evazija poreza, elektronski vandalizam, terorizam i iznuda, prevare u vezi sa prodajom i investicijama, nezakonito presretanje telekomunikacija, prevare vezane za elektronsko poslovanje. Širokim definicijama navedenih grupa on je zaista gotovo uspeo da pokrije sve oblike neželjenog i nezakonitog ponašanja. Ipak, koliko je ovaj posao samo relativno koristan i koliko su ovakve podele ponekad neupotrebljive pokazuje, recimo, analiza „rasturanja materijala neprikladnog sadržaja" – u ovu grupu bi spadale kako reklamne poruke (čije slanje u principu nije kažnjivo), tako i slanje, npr. rasističkih poruka, pornografskog materijala (uključujući i dečju pornografiju) i uputstava za pravljenje eksplozivnih naprava (dakle, postupci koji se smatraju teškim krivičnim delima u tradicionalnom krivičnom pravu).[10]

Kada je reč o suzbijanju visokotehnološkog kriminala u Srbiji, može se reći da se ovom problemu poslednjih godina pristupilo ozbiljno i da postoje prva pozitivna iskustva u radu novih, specijalizovanih organa kao što su: posebne jedinice policije, Specijalnog tužilaštva i Specijalnog odeljenja Okružnog suda u Beogradu. Međutim, proces suzbijanja je nerazdvojivo povezan sa

[8] Procena je da šteta od različitih delovanja visokotehnološkog kriminala – ne uzimajući u obzir njegove potencijalne veze sa organizovanim kriminalom – na godišnjem nivou iznosi oko 200 milijardi dolara. Dragan Prlja, *Sajberkriminal*, predavanje održano na Pravnom fakultetu Univerziteta u Beogradu, 28. 12. 2008. godine. Tekst predavanja može se naći na internet adresi: *http://www. prlja.info/sk2008.pdf*, 1. 5. 2009.

[9] Izvor: *http://www. crime-research.org/analytics/702*, 1. 5. 2009.

[10] Izvor: *http://www.aic.gov.au/conferences/other/graycar_adam/2000-02-cybercrime.html*, 1. 5. 2009.

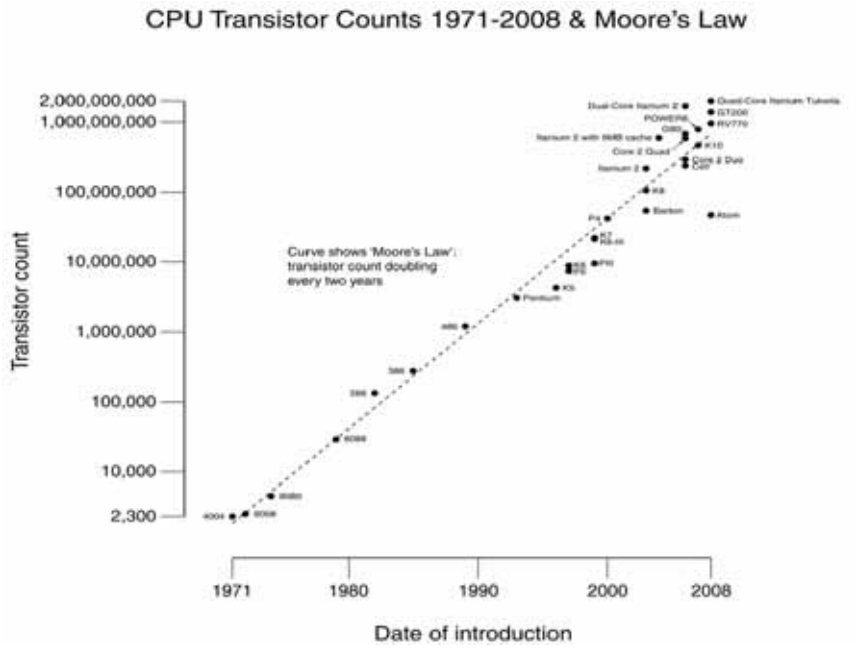
prevencijom i edukacijom u ovoj oblasti, a na tim poljima se do sada nije mnogo uradilo. Prema nekim procenama, u Srbiji oko dva miliona ljudi koristi internet.[11] Zabeleženi su prvi slučajevi prevara, kao i zloupotreba kreditnih kartica, dečje pornografije i sl. Otuda će i ovo istraživanje imati za cilj da približi sajber kriminal kako stručnoj javnosti, tako i običnim korisnicima računara koji budu zainteresovani za proučavanje opasnosti i izazova sa kojima se mogu susresti.

[11] Dragan Prlja, *loc. cit.*

2. OSNOVNI POJMOVI

„Neznanje je moć“
Džordž Orvel, 1984.

Računar ili *kompjuter* svoje korene nalazi u drevnoj Kini, pre više od 500 godina, i to u računaljci koja se zvala *Abacus*. Računari, veliki kao soba, spočetka četrdesetih godina XX veka, bivaju s vremenom zamenjeni personalnim računarima (*PC – Personal Computer*); ovoj, tzv. digitalnoj revoluciji najviše je doprinelo izum tranzistora i njegova komercijalna upotreba u šezdesetim godinama, što je omogućilo da se računarske komponente izrađuju u mikroveličini, a samim tim zauzmu fizički mali prostor uz štednju energije neophodne za rad. Prvi PC je izašao iz laboratorije IBM-a, i to 1981. godine. Sledeći Murov zakon (slika 1) da će se broj tranzistora koji su smešteni na integrisanom kolu udvostručavati na dve godine, dolazimo i do današnjih računara, sa nezamislivim performansama.



Slika 1: Grafički prikaz Murovog zakona [12]

[12] Izvor: *http://en.wikipedia.org/wiki/Moore%27s_la*, 1. 5. 2009.

Osnovna karakteristika računara da su to mašine koje koristeći određene instrukcije manipulišu podacima (niz logički povezanih naredbi čini računarski program), omogućila je ljudima da im nađu svrhu u skoro svakom segmentu života i privređivanja.

Pojam računar, odnosno njegova zloupotreba, igra glavnu ulogu kada je u pitanju visokotehnološki kriminal i zakonodavac ga spominje u svim krivičnim delima iz glave XVII – Krivična dela protiv bezbednosti računarskih podataka, Krivičnog zakonika Srbije.[13] Koristeći se računarom i uređajima iz oblasti IT (*Information Technology*), moderni kriminalac dolazi do protivimovinske koristi, nanosi štetu privredi, podriva bezbednosni sistem jedne države, i sve to bez potrebe da izađe iz svoje sobe.

Računar čine *HARDWARE* [npr. *CPU – Central processing unit, Motherboard* (matična ploča), *Hard Disk Drive,* grafička kartica, *RAM – Random Access memory, NIC (Network Interface Card)* – mrežna kartica… i *SOFTWARE* (npr. OS – *Operating system, Word, Excel, Photoshop, Internet Explorer…*)]. Hardverske komponente računara poznaju samo dva stanja: – i +, ili u binarnom obliku, jedinicu i nulu. Teško je zamisliti da sve što se iscrtava na ekranu prilikom upotrebe računara predstavlja u stvari skupove jedinica i nula. Da bi čovek mogao da upravlja računarom koji je sposoban da izvodi razne računske operacije potrebno je da postoji program, aplikacija (*SOFTWARE*) koja će komande razumljive ljudima prevoditi na jezik koji će mašina rastumačiti i upotrebiti, kako bi manipulisala odgovarajućim podacima. Treba istaći *operativni sistem* (OS u daljem tekstu), kao najbitniju softversku komponentu računara, koji služi kao „most" između korisnika *(user)* i računara, odnosno njegovih hardverskih komponenata. Ostale aplikacije, programi rade pod, odnosno kompatibilne su sa određenim OS-om, koristeći njegove resurse da bi komunicirali sa hardverom. Kao primere OS-a možemo navesti najpoznatiji Microsoft Windows (u različitim izdanjima, kao Windows 98, Windows NT, Windows 2000, Windows XP, Windows Vista i najavljeni Windows 7), UNIX, MacOS, Linux... Najveći deo tržišnog udela drži Microsoft sa svojom Windows platformom, koji je, između ostalog, i zbog toga najčešće izložen napadima i bezbednosnim rizicima. Pored spomenutih operativnih sistema koji su predviđeni za tzv. *Desktop* ili *Laptop* (prenosne) računare, te se još zovu i klijentski operativni sistemi, moramo razlikovati i serverske operativne sisteme, koji su specifični utoliko što se instaliraju na računarima, tzv. *serverima,* koji imaju daleko jače performanse od klijentskih. U tu grupu spadaju Microsoft Windows Server 2000, 2003, 2008, kao i razne edicije OS-ova, baziranih na Unix platformi, Sun Solaris…

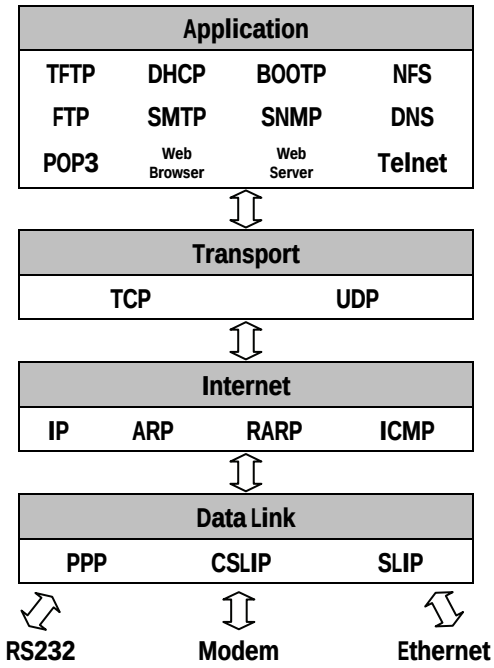
[13] „Službeni glasnik RS", br. 85/2005, 88/2005 – ispr. i 107/2005 – ispr.

Polazeći od ove podele računara na serverske i klijentske, dolazimo do pojma *računarskih mreža*. Serverski računari, koji zahvaljujući bogatijim hardverskim performansama „opslužuju“ (reč server potiče od engleskog glagola – *to serve*, služiti) i dele svoje resurse sa klijentskim računarima, svoju ulogu ostvaruju upravo u okruženju umreženih računara. Ne treba mnogo ulaziti u potrebe za umrežavanjem; prednost deljenih resursa (deljeni štampač, server na kome se nalaze deljeni podaci, aplikacija koja objedinjuje celo poslovanje firme i ima centralizovanu server/klijent strukturu) jeste *conditio sine qua non* za današnje poslovanje. Najkraće rečeno, kompjuterska mreža je grupa međusobno povezanih računara. U prvo vreme računarskih mreža različiti proizvođači komunikacione i računarske mrežne opreme dozvoljavali su komunikaciju samo između uređaja koji potiču od istog proizvođača. Kako bi se izbegla ova prepreka, ISO (*International Standard Organization*) uspostavila je set protokola na osnovu kojih bi trebalo unificirati komunikaciju između računara, a samim tim i proizvođače „naterati“ da se pridržavaju ovog standarda prilikom proizvodnje opreme. Model, skup protokola o kome je ovde bilo reči, nazvan je OSI (*Open System Interconnect*) model. U principu, u pitanju je teoretski model koji ima sedam nivoa preko kojih se odvija protok i razmena podataka između povezanih uređaja. Nešto slično postoji i u diplomatskim odnosima, gde se poštuju određeni protokoli prilikom komunikacije između država i državnih predstavnika.

7	**Application**	Web Application
6	**Presentation**	HTTP
5	**Session**	80
4	**Transport**	Transmission Control Protocol (TCP)
3	**Network**	Internet Protocol (IP)
2	**Data Link**	Ethernet
1	**Physical**	CAT 5

Slika 2: OSI model[14]

[14] Izvor: *http://www.learnthat.com/certification/files/432/img/OSI%20Model.jpg*, 1. 5. 2009.



Slika 3: TCP/IP model[15]

Tok komunikacije između računara sledi sledeći obrazac: podaci putuju od računara koji ih šalje tako što se od sedmog aplikativnog nivoa dodaju izvesne informacije, pri tome se podaci enkapsuliraju sve do poslednjeg, prvog fizičkog nivoa, pa do odredišnog računara koji prima podatke i gde se obrnutim redosledom (dakle, od prvog do sedmog nivoa) poslati podaci „otpakuju". Ovaj proces se dešava fantastičnom brzinom i nije transparentan za običnog korisnika. Treba naglasiti da je, iako je umnogome olakšao i ubrzao komunikaciju između računara, OSI model ostao teoretski model komunikacije, dok se mnogo poznatiji tzv. TCP/IP model, koji sledi korake OSI modela, definitivno ustoličio kao najiskorišćeniji, naravno i stoga što najveća kompjuterska mreža na svetu, *Internet*, funkcioniše na bazi ovog modela. Postoje različiti tipovi mreža, a nama su najvažniji LAN (*Local Area Network*, u najčešćem slučaju to je kompjuterska mreža koja pokriva mali fizički prostor, npr. kancelariju, zgradu, školu, aerodrom) i WAN (*Wide Area Network,* mreža koja doseže velike prostore i podrazumeva složenu konfiguraciju komunikacionih uređaja i kombinaciju više tehnologija, a najpoznatiji primer ovog tipa mreže svakako je *Internet*). Treba napomenuti da se u komunikaciji između računara nalazi izves-

[15] Izvor: *http://www.computer-solutions.co.uk/chipdev/images/tcp-ip.jpg,* 1. 5. 2009.

tan broj komunikacionih uređaja (*Bridges*, *Swiches*, *Routers*), koji *de facto* čine tu komunikaciju mogućom. U njima se, takođe, nalaze procesori, koji vrše određena izračunavanja, i njima upravljaju programi, tako da u širem smislu i ovi uređaji predstavljaju računarsku opremu. Iz imena TCP/IP modela izdvojio bih, pre svega, IP (*Internet Protocol*). Ovaj protokol je zadužen za adresiranje računara i njihovo raspoznavanje na mreži po ovom kriterijumu. IP adresiranje računara možemo shvatiti kao i adresiranje koje je nama mnogo jasnije, a to je grad, broj kuće, broj stana. Tako i računari u jednoj mreži moraju imati svoju jedinstvenu IP adresu da bi između njih bila uspostavljena komunikacija. IP adrese su, u stvari, iako predstavljene računaru u binarnom obliku, niz brojeva koje ljudi lako raspoznaju i kojima mogu da manipulišu, npr. 192. 168. 1. 3, 10. 0. 0. 2, 172. 16. 0. 5, 74. 125. 43. 99. Osnovna podela IP adresa je na privatne i javne IP adrese, gde se privatne koriste u LAN mrežama, dok se javne koriste na internetu i u drugim WAN mrežama. Bitno je napomenuti da na internetu, bez obzira na to koliko računara je u tom trenutku povezano na ovu mrežu (neka istraživanja kažu da je u 2007. godini taj broj bio oko 500 miliona), ne sme biti preklapanja adresa. Budući da se internet razvija fantastičnom brzinom, postojeća verzija IP adresiranja IP v4, preći će u IP v6, koja nudi mnogo veći opseg adresa. Drugi pojam je TCP (*Transmission Control Protocol*), koji je u modelu zadužen za otvaranje i održavanje pouzdanih sesija u komunikaciji, preko određenih „vrata“ *(ports)* koje programi koriste. Prva 1024 porta spadaju u grupu tzv. w*ell-known ports* (za spisak ovih portova bila je zadužena IANA (*Internet Assinged Number Authority*) i poznata je lista protokola koji ih koriste. Tako je port broj 80 zadužen za HTTP (*Hyper Text Transfer Protocol*), zatim broj 25 za SMTP (*Simple Mail Transfer Protocol*); korišćenje ova dva porta omogućava uvid u internet stranice i razmenu elektronske pošte. Neophodno je upoznati se sa ovim protokolima TCP/IP modela komunikacije upravo iz razloga bezbednosti na mreži, pre svega zato što se hakeri najčešće koriste poznavanjem i eksploatacijom ovih protokola.

Osnovni, možda i najvažniji pojam kad je u pitanju visokotehnološki kriminal svakako je internet. Njegovi počeci se vezuju za šezdesete godine i doba Hladnog rata, kada je u SAD formirana agencija ARPA (*Advanced Research Projects Agency*), sa namerom da od SSSR preuzme tehnološki primat (SSSR je tih godina uspešno lansirao satelit Sputnik). Jedan od projekata na kome su radili imao je za cilj da umreži računare, kako ne bi izgubili komunikaciju, čak iako između njih ne postoji fizička veza, i to u slučaju nuklearnog rata ili totalnog prekida komunikacije. ARPANET je, kako se to kaže, ugledao svetlost dana 29. oktobra 1969. godine, i to uspešnim povezivanjem UCLA (*University of California, Los Angeles*) i SRI (*Stanford Research Institute*). Od 1983. godine TCP/IP model postaje nezamenjivi deo ove mreže,

a u komercijalne vode internet ulazi od 1988. godine. Kasniji razvoj WWW (*World Wide Web*) servisa, DNS (*Domain Name System*), zaduženog da „prevodi" imena internet stranice u IP adrese, i HTML (*Hyper Text Markup Language)* programskog jezika, u početku korišćenog za razvoj internet stranica, koji su omogućili da na najjednostavniji način, upisom ljudski razumljivog teksta, posetite različite internet lokacije, doveli su do toga da *Internet* postane sastavni deo ljudskog života u XXI veku.

Apsolutna zavisnost od računara, mreža i interneta, upozorava na veliki broj potencijalnih opasnosti do kojih može doći zloupotrebom i malicioznim korišćenjem ovih tehnologija. Vanredno dobro poznavanje funkcionisanja računara, računarskih programa i računarskih mreža dovodi nas do pojma haker. Iako je s vremenom ovaj pojam dobio razne konotacije, pa se išlo dotle da postoji grupa hakera *White Hat*, koja koristi hakerske alate da bi upozorila na bezbednosne propuste, i *Black Hat*, ili još i *cracker*s, čija se namera karakteriše kao zlоćudna, termin haker se zadržao u upotrebi kao generički naziv za osobe koje, na volšebno uspešan način, koriste računare, i to svoje preimućstvo u poznavanju tehnologije rada računara i programiranja koriste za sopstvene ciljeve. U to ime treba spomenuti više, u praksi prepoznatih, motiva koji služe kao pokretači hakerima, pa se tako pojam *hacktavist* odnosi na osobu koja svoj „zanat" upotrebljava zarad viših ciljeva u koje veruje (na primer, pobornik čiste životne okoline napada i obara internet sajt neke organizacije koja se bavi „prljavom industrijom"), zatim osobe koje to rade iz političkih ubeđenja (skorašnji su primeri „rata" između albanskih i srpskih hakera, i takmičenja koja će grupa da obori više internet sajtova vladinih institucija), a tu je i uloga terorističkih organizacija u mogućem napadu na, recimo, sistem koji održava nuklearnu centralu, ili nama bliže, sistem kojim se upravlja i prati stanje na hidroelektrani Đerdap. Napominjem, ovde je reč samo o upadima u sisteme, a ne o drugim aktivnostima terorista koji mogu iskoristiti sve prednosti koje im savremene tehnologije pružaju. Danas je aktuelan i pojam *script kiddie* – mladi hakeri koji ne poseduju nivo tehničkog znanja, ali zbog dostupnosti hakerskih alata preko interneta preuzimaju ulogu hakera, a da pri tome ne znaju koje tehnologije se koriste u pozadini napada.

Lista napada na vaš sistem i spisak potencijalnih opasnosti prevazilazi okvire ove teme. U ovom tekstu će biti obrađene neke najčešće pojave, između ostalih i one koje čine biće krivičnih dela iz glave XXVII – Krivičnog zakona Republike Srbije.

Tipični napadi su DOS – *Denial of Service, IP Spoofing, Back Door, Man in The Middle, Network Sniffing, „Rupe" u pragramima,* zatim opasnosti koje nosi *Malware* (virusi, trojanski konji – *Trojan Horses* – i „crvići" – *Worms*)*, imejl prevare,* te opasnosti od pojave socijalnog inženjeringa, a na kraju i od „kompjuterske piraterije".

DOS – *Denial of Service – The United States Computer Emergency Readiness Team* (deo američkog *Homeland Security)* kaže da ovaj napad karakterišu sledeće pojave:[16]

- neobično spore performanse mreže,
- nedostupnost određenog internet sajta,
- nemogućnost otvaranja nekog internet sajta,
- velika pojava neželjene pošte.

Ovaj napad na računar je karakterističan po tome što je cilj da računar ne „obavi" svoj posao, odnosno da odbije da izvrši neki servis (ref. Računarska sabotaža, član 299 Krivičnog zakonika). Najčešće mete ovog napada su veb serveri na internetu. Bilo da napadač koristi dijagnostički protokol (ICMP) iz TCI/IP modela i njegovom izmenom „bombarduje" računar ili komunikacioni uređaj primoravajući ga da iskoristi sve svoje resurse odgovarajući na ovaj niz zahteva (*ping – of – death attack*), ili da koristi određene registre računarske memorije koji se zovu *buffer*-i i da njih popunjava nepotrebnim nizom podataka (*buffer over-flow attack*), krajnji rezultat je isti – računar nije u mogućnosti da izvrši računarske operacije kako treba i postaje potpuno beskorisitan. Podvarijanta DOS napada je i DDOS (*Distributed Denial of Service*) za koji je karakteristična upotreba više računara u organizovanom, frontalnom napadu na određeni računarski sistem.

IP Address Spoofing. – Lažiranje IP adrese predstavlja pokušaj napadača da svoj računar ili neke podatke sa „spoljne" mreže predstavi kao da dolaze sa računara čija je IP adresa deo adresnog opsega unutrašnje mreže (većina ovih računara ne mora „svesno" da učestvuje u napadu, već ih metodom daljinskog pristupa koristi napadač).

Back Door. – Na „zadnja vrata" nailazimo u umreženom okruženju, odnosno kada se na nekom sistemu instalira program koji će omogućiti neovlašćenom licu pristup informacijama i resursima na toj mreži (ref. Neovlašćeno korišćenje računara ili računarske mreže, član 304 Krivičnog zakonika).

Man in the Middle. – U bukvalnom prevodu, „čovek u sredini", leži i objašnjenje ove pretnje. Naime, napadač se namešta između dva sistema koji komuniciraju i presreće njihovu komunikaciju, preuzimajući ulogu jednog od njih. Ovaj napad je znatno aktuelizovan pojavom i sve većom upotrebom WLAN tehnologija (*Wireless Local Area Network* – podvrsta LAN-a, o kojima je bilo reči, samo što se ovde koristi bežična komunikacija, odnosno komunikacija kroz etar, u cilju izbegavanja kablova kao medijuma za prenos podataka), gde se jednostavnom vožnjom kroz grad (na Zapadu se to zove *War Driving*) lociraju ove mreže i napadom, odnosno eksploatacijom bezbe-

[16] Izvor: *http://en.wikipedia.org/wiki/Denial-of-service_attack*, 1. 5. 2009.

dnosne zaštite (WEP – *Wired Equiavalent Privacy* šifrovanje, koje je karakteristično za bežične mreže) pristupa nezaštićenim računarima.

Network Sniffing (osluškivanje mreže). – Napadač može koristiti aplikacije koje „osluškuju" sav saobraćaj koji dolazi do mrežne kartice (NIC) i koristeći te informacije dolazi do vrednih podataka (korisničkih imena, šifri, čitavih poruka...). Popularni su sledeći programi: *Kismet* (koristi se za osluškivanje bežičnog saobraćaja), *Wireshark*...

Keystroke logging je metoda snimanja svega što korisnik otkuca. Princip je da se na računaru instalira neidentifikovani program, koji će beležiti sve što korisnik kuca na tastaturi, i kasnije dati na uvid trećem, nepozvanom licu (ref. Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka, član 302 Krivičnog zakonika). Zamislite onlajn kupovinu ili proveru bankarskog računa putem elektronskog bankarstva, gde se korisnik predstavlja serveru tako što pruži podatke, obično to budu korisničko ime i šifra ili PIN, a *key logger* pokupi te informacije. *Symantec* internet sajt pruža zanimljivu priču iz života o žrtvi ovakvog napada.[17]

„Rupe" u programima mogu poticati od strane programera koji je namerno ostavio neko parče koda, kao ulaz, da bi mogao „naživo" (bez zastoja u radu programa) da izvrši kontrolu i otkloni eventualne greške u aplikaciji, a mogu biti i posledica nenamerne greške programera (neke aplikacije su izuzetno složene i imaju više miliona kodnih linija), gde u tzv. Nultom danu [0-*day* – vreme u kome je hakerska zajednica pronašla „rupu", pa sve do zvanične „zakrpe" *(patch)* od strane programera] hakeri distribuiraju tzv. „exploit", program koji će zloupotrebiti tu „rupu".

Kompjuterski virusi su programi koji su sposobni da zaraze i da se iskopiraju na kompjuter bez znanja korisnika (ref. Pravljenje i unošenje računarskih virusa, član 300 Krivičnog zakonika). Da bi se virus izvršio mora biti pokrenut, a da bi se „zarazili" drugi računari mora se preneti preko nekog medijuma (*DVD, USB Memory Stick, shared*, deljeni mrežni diskovi). Za razliku od virusa, „crvići" (*Worms*) koriste neku slabost, „rupu" u sistemu da bi se replicirali, bez ikakve intervencije od strane korisnika. Najčešće otvaraju komunikaciju na nekom od TCP portova da bi preuzeli kontrolu nad računarom (*Back door*, vrsta napada). Najpoznatiji „crvići" su *MyDoom* i *Sobig*.[18] Trojanski konji (*Trojan Horses*) su programi koji su na prvi pogled potpuno bezazleni, a u stvari kriju potpuno drugu agendu. Najčešće se koriste da omoguće napadaču kontrolu nad „zaraženim" računarom. Poznati su *waterfalls*.

[17] Izvor: *http://www.symantec.com/norton/cybercrime/stories.jsp*, 1. 5. 2009.

[18] Izvor: *http://www.thefreelibrary.com/Mydoom+Surpasses+Sobig.F+to+Become+Fastest+Spreading+Virus+Ever,+with...-a0112589554*, 1. 5. 2009.

scr,[19] *Koobface* koji napada poznate sajtove *My Space* i *Facebook*, zatim *Back Door,*[20] Sub7[21] itd.

Imejl prevare – (*e-mail spoofing*, *Phishing,* komjuterski virus *Hoax*...). Elektronska pošta je danas sastavni deo komunikacije miliona ljudi. Jednostavno govoreći, imejlovi se razmenjuju tako što, u formi podataka [prateći TCP/IP model komunikacije i koristeći SMTP protokol (*Simple Mail Transfer Protocol)* u kombinaciji sa odgovarajućim TCP portom] sa odredišnog računara putuju do servera, koji dalje prosleđuju poruku do drugih servera, i na kraju do željenog računara, odnosno aplikacije za uvid u elektronsku poštu. *E-mail spoofing* je nešto slično formi „lažnog predstavljanja", gde osoba koja šalje poruku lažira imejl, kao da ga šalje neka druga osoba. *Phishing* je metoda predstavljanja u imejl poruci, koja u svakom pogledu izgleda kao da potiče iz nekog pouzdanog izvora (npr. imejl „vaše" banke, koja vas obaveštava da morate da se prijavite ponovo na sistem banke radi provere stanja na vašem računu, gde je lokacija za prijavljivanje lažna, kao i sam imejl), i to u cilju nelegalnog dolaska do korisnikovih ličnih podataka i njihove kasnije eksploatacije. Kompjuterski virus *Hoax* je nešto slično tzv. lančanom pismu, koje u principu ne izaziva veću štetu ali je iritirajuće za „žrtve". Ako je u sadržaju elektronske pošte nalog da se neki podatak sa računara izbriše „iz razloga bezbednosti" ili nekog sličnog legitimnog razloga, onda ova prevara može imati i drastične posledice (ref. Oštećenje računarskih podataka i programa, član 298 Krivičnog zakonika), što je i bio slučaj sa *jdbgmgr.exe* zbog virusa *Hoax*.[22]

Na kraju, treba objasniti i pojam *social engineering*, „u smislu bezbednosti računarskih sistema socijalni inženjering je izraz koji opisuje netehnički napad koji zavisi od ljudskih odnosa, i prevaru, kao i dovođenje ljudi u zabludu, kada je u pitanju odavanje nekih bezbednosno relevantnih informacija ili procedura".[23] Napadač koristi svoj izraženi smisao za komunikaciju, kao i sugestivnost, u nameri da od lakovernog sagovornika dobije informaciju do koje bi inače morao da dođe klasičnim, navedenim hakerskim metodama.

Što se tiče krivičnog dela Računarska prevara iz člana 301 Krivičnog zakonika, treba napomenuti prvi slučaj kompjuterskog kriminala na našim prostorima, koji se dogodio u Puli, gde su trojica službenika „Istarske banke" svojim aktivnim delovanjem na izmeni podataka u poslovnom sistemu banke, a u

[19] Izvor: *http://en.wikipedia.org/wiki/Trojan_Horse_ (Computing)*, 1. 5. 2009.
[20] Izvor: *http://www.cyberwalker.com/article/182*, 1. 5. 2009.
[21] Izvor: *http://128.175.24.251/trojan.htm*, 1. 5. 2009.
[22] Izvor: *http://antivirus.about.com/cs/hoaxes/a/jdbgmgr.htm*, 1. 5. 2009.
[23] Izvor: *http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html*, 1. 5. 2009.

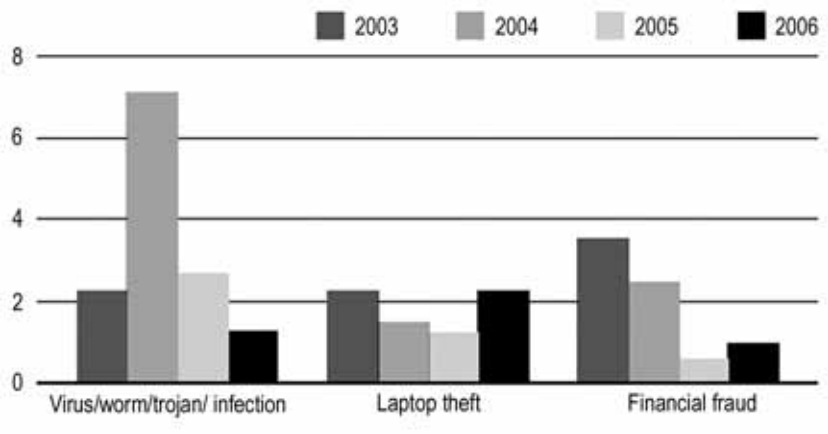
vezi sa izdavanjem štednih knjižica i lažiranjem kamatnih stopa sebi pribavili veću imovinskopravnu korist.[24]

Član 3 Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Službeni glasnik RS“, br. 61/2005) određuje koja će se grupa krivičnih dela naći u nadležnosti državnih organa u borbi protiv visokotehnološkog kriminala pa se, pored krivičnih dela protiv bezbednosti računarskih podataka određenih glavom XXVII Krivičnog zakonika, u stavu 2 spominju i krivična dela protiv intelektualne svojine, imovine i pravnog saobraćaja 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. Internet, uz sve blagodeti koje podrazumeva (baza ljudskog znanja), nudi i široku lepezu dejstvovanja potencijalnim izvršiocima krivičnih dela, pogotovo iz oblasti kršenja autorskih prava. Gotovo da nema čoveka koji nije upoznat sa terminom, „skinuću tu pesmu, knjigu, muzički album sa interneta“. Najčešće, *modus operandi* je preko P2P (*peer to peer*) programa, kao što su razne *torrent* aplikacije *Bittorrent*, *uTorrent*...), zatim S*oulseek*, *Kazaa*, *eMule* i dr. Ova vrsta razmene podataka preko računarskih mreža ili interneta u svojoj biti je zamišljena kao razmena studentskih skripti, sopstevenih dokumenata, slobodnog, *open-source* softvera... znači ne za neautorizovanu razmenu autorskih dela (muzike, knjiga, programa...), u šta se danas najčešće koristi. Princip funkcionisanja je vrlo jednostavan: vaš računar koji preuzima neki podatak istovremeno ga deli sa drugim korisnicima koji preuzimaju taj isti podatak – stručnim rečnikom, vaš računar preuzima (*download*) podatak (*file*), a deo preuzetog podatka (koji je na vašem računaru) stavlja se na mogućnost preuzimanja drugim korisnicima. U suštini, ništa od ovog materijala se ne nalazi na nekom internet serveru, već na računarima koji učestvuju u ovoj vrsti deljenja podataka. Danas postoji dosta mogućnosti da na internet pohranite svoje podatke preko onlajn servera, a tu vam uslugu pružaju *Rapidshare, Megaupload, Letitbit, Megashare* i slične firme... Ovi servisi se često koriste u lancu protivzakonite razmene autorskih dela, iako se sa ovih servera reaguje svaki put brisanjem nelegalnog sadržaja čim do adiministratora servera stigne prijava.

Iz ovog istraživanja, sprovedenog u Australiji, možemo steći uvid u novčanu štetu koju prouzrokuje ova vrsta kriminala.[25]

[24] Slobodan R. Petrović, *Kompjuterski kriminal*, Vojnoizdavački zavod, Beograd, 2004, str. 51–54.

[25] Izvor: *http://www.aic.gov.au/stats/crime/cybercrime.html*, 1. 5. 2009.



Slika 4: Major sources of financial loss due to computer crime and security breaches, 2003-06 ($ million)

Dok, prema istraživanju *Internet Crime Complaint Center* (IC3), kako objavljuje internet sajt Security Warch,[26] gubici izraženi u dolarima u 2007. godini dostižu cifru od 239 miliona samo u prevarama građana u SAD, gde je kompjuter bio sredstvo ili objekat napada, u 2008. godini gubitak u SAD povećan je na 264 miliona dolara samo na prevarama.

[26] Izvor: *http://www.securitywatch.co.uk/2008/04/04/the-latest-cybercrime-statistics/*, 1. 5. 2009.

II

MEĐUNARODNI DOKUMENTI OD ZNAČAJA ZA SUZBIJANJE VISOKOTEHNOLOŠKOG KRIMINALA

1. INFORMATIČKA REVOLUCIJA

Ubrzan razvoj ili, bolje reći, eksplozija informatičkih i komunikacionih tehnologija u drugoj polovini XX i početkom XXI veka daje nam za pravo da savremena društva okarakterišemo kao informatička društva. Iako nisu na istom stepenu razvoja, prvenstveno usled ekonomskih, ali i drugih brojnih faktora, ova društva pokazuju manji ili veći stepen zavisnosti od informatičkih tehnologija. Ova zavisnost obuhvata sve segmente života pa se tako ove tehnologije pokazuju kao neophodne prilikom pružanja usluga koje su od javnog i opšteg interesa, a naročito su zastupljene u poslovanju privrednih društava koja teže automatizaciji procesa rada i za koja su principi efikasnosti i pouzdanosti presudni.

Razvoj interneta kao globalne mreže koja omogućava slobodan pristup neograničenom broju raznovrsnih informacija doprineo je da informatičke tehnologije postanu i neizostavni deo života skoro svakog pojedinca. Elektronsko bankarstvo i elektronska trgovina omogućavaju da se uštedi vreme na obavljanju svakodnevnih operacija koje su ranije iziskivale čekanje u redovima, popunjavanje raznih obrazaca i obavljanje drugih formalnosti. Elektronske baze podataka sada su dostupne putem računara tako da potraga za određenim informacijama koje su nam u datom trenutku potrebne ne zahteva više od nekoliko minuta. Vesti iz zemlje i sveta su nadohvat ruke, elektronskom poštom stupamo u kontakt sa bilo kim nezavisno od lokacije, u vremenskom intervalu koji se meri sekundama. Uz neznatnu novčanu investiciju, krug ljudi i opseg informacija koje su nam dostupne praktično je neograničen.

Nažalost, svet informacionih tehnologija, pored prednosti koje su evidentne, poseduje i negativnu stranu. On je otvorio vrata za mnogobrojne neprihvatljive i kriminalne radnje koje se sada mogu obavljati na način koji je u prošlosti bio nezamisliv. Računarski sistemi i mreže pružaju mogućnost za izvršenje nekih tradicionalnih krivičnih dela na sasvim nov i sofisticiran način. Pored materijalne štete za pojedince i pravna lica, koja može nastati zloupotrebom informatičkih tehnologija i koja svakako nije zanemarljiva, opasnosti ovakvih zloupotreba mogu biti i mnogo teže a posledice dalekosežnije. Kao što je rečeno, kompjuterizacija i automatizacija procesa rada obuhvata skoro sve aspekte života u jednom društvu i bilo kakav neovlašćeni prodor ili sabotaža ovih sistema mogu prouzrokovati posledice koje se ne bi ogledale samo u finansijskim gubicima, već bi mogle ugroziti bezbednost života ljudi. Tako i dolazimo do zaključka da visoka tehnologija, koja je opredmećena u

bezličnim mikročipovima i koja govori nerazumljivim jezikom binarnih kodova, i te kako ima ljudsku dimenziju.

Kada se bude pisala istorija druge polovine XX veka, nema sumnje da će ovaj period biti zabeležen kao period informatičke revolucije. Motor ovog tehnološkog napretka svakako je računar i tehnologija njegove upotrebe koja se razvija takvom brzinom da omogućava njegovu primenu u obavljanju sve komplikovanijih i osetljivijih operacija od kojih zavise i sami oslonci jednog društva i međunarodnog poretka uopšte.

1.1. Potreba za globalnom reakcijom

Visokotehnološki kriminal je novi oblik kriminaliteta koji u sebi ima ugrađen transnacionalni karakter.[27] Međutim, zakonodavna regulativa, politika i metodi kriminalnog progona, kao i međunarodna saradnja, nisu pratili korak sa razvojem informacionih tehnologija. Samo nekoliko zemalja poseduje zakonodavne instrumente koji omogućavaju efikasan obračun sa visokotehnološkim kriminalom. Ubrzan razvoj kompjuterskih tehnologija zahteva budnost zakonodavaca i neprestano praćenje promena koje se dešavaju, te fino podešavanje pozitivnog zakonodavstva koje bi moglo da odgovori novim izazovima. Inertnost zakonotvoraca koja ne predstavlja ozbiljnu prepreku u drugim oblastima prava ovde može imati teške posledice. Nespremnost da se ozbiljno uhvati u koštac sa problemom visokotehnološkog kriminala obično je posledica nedovoljnog poznavanja ove materije i neshvatanja ozbiljnosti posledica koje mogu proisteći zloupotrebom informacionih tehnologija.

Sa stanovišta nacionalnih zakonodavstava, reakcija na opasnost od širenja kompjuterskog kriminaliteta trebalo bi da ide u tri pravca, i to sledećim redom:

- preduzimanje mera prevencije kako bi se sprečile ili ublažile posledice vršenja kompjuterskog kriminala i kako bi potencijalne žrtve (korisnici informacionih tehnologija) imale svest o opasnostima koje im prete;
- blagovremeno usvajanje odgovarajuće zakonodavne regulative u oblasti materijalnog i procesnog prava kako bi se stvorili pravni instrumenti za obračun sa visokotehnološkim kriminalom;
- kadrovska i materijalna osposobljenost nadležnih policijskih i pravosudnih organa za efikasno sprovođenje zakonskih ovlašćenja koja su im poverena.

[27] Izrazi „visokotehnološki kriminal“ i „sajber kriminal“ imaju isto značenje, u pitanju je terminološka razlika s obzirom na to da Konvencija Saveta Evrope koristi izraz „sajber kriminal“, dok domaće zakonodavstvo koristi izraz „visokotehnološki kriminal“.

Kada se pitanje pravne regulative posmatra sa stanovišta međunarodne saradnje, postojeći problemi postaju još ozbiljniji. Transnacionalni karakter ove vrste kriminaliteta zahteva saradnju između država, koja mora biti na visokom nivou i zasnovana na principima koji su obostrano prihvaćeni. Neusklađenost nacionalnih zakonodavstava i nepostojanje opšteprihvaćenih pravnih standarda i ovlašćenja nadležnih organa u borbi protiv visokotehnološkog kriminala može usporiti, čak i onemogućiti efikasno otkrivanje počinilaca krivičnih dela. Brzina reakcije nakon saznanja da je krivično delo izvršeno od presudnog je značaja za otkrivanje počinilaca i za obezbeđenje dokaza imajući u vidu da se tragovi izvršenog dela lako mogu uništiti, sakriti ili na drugi način učiniti nedostupnim ili neupotrebljivim.

Osnovne probleme koji predstavljaju prepreku efikasnoj međunarodnoj saradnji i globalnim naporima da se suzbije visokotehnološki kriminal možemo definisati na sledeći način:

- različito pravno definisanje radnji izvršenja i opsega ovih radnji koje predstavljaju krivično delo visokotehnološkog kriminala;
- nedovoljna obučenost policijskih službenika, tužilaca i sudija koji postupaju u predmetima visokotehnološkog kriminala;
- neusklađenost procesnih pravila u nacionalnim zakonodavstvima u pogledu istrage krivičnih dela visokotehnološkog kriminala;
- neusklađenost ili odsustvo mehanizama međunarodne pravne pomoći i sporazuma o ekstradiciji.

Globalni napori da se uspostavi efikasna međunarodna saradnja u borbi protiv visokotehnološkog kriminala zasad su najviše odmakli u zemljama zapadne Evrope i zemljana članicama OEBS-a. Iako rezultati nisu zanemarljivi, neophodno je da se frontovi borbe protiv ove vrste kriminaliteta otvore u svim delovima sveta. Potrebno je da učešće uzmu i zemlje koje su u tranziciji i razvoju jer upravo ovim državama predstoji opsežna implementacija informacionih tehnologija sa svim prednostima ali i opasnostima koje ona donosi.

2. KRATAK PRIKAZ RAZVOJA PRAVNE REGULATIVE O VISOKOTEHNOLOŠKOM KRIMINALITETU NA MEĐUNARODNOM NIVOU

Pre nego što analizi podvrgnemo najznačajnije međunarodne pravne dokumente u vezi sa borbom protiv visokotehnološkog kriminala neophodno je dati i kraći istorijski prikaz zakonodavnih i drugih napora, uspelih i neuspelih, da se problem računarskog kriminaliteta sagleda u celosti i na sistematski način. Ovo je neophodno ne radi faktografije ili suvoparnog nabrajanja, već kako bi se ukazalo na same početke borbe protiv visokotehnološkog kriminala koji sežu malo dalje u prošlost i koji su, vremenski posmatrano, decenijama udaljeni od aktuelnih napora da se obuzdaju i umanje aktuelne pretnje koje dolaze iz sajber prostora kao rezultat dramatičnog i agresivnog prodora računarskih tehnologija u život svakog pojedinca i u same osnove svakog uređenog društva i organizacije. Takođe, videćemo da je potencijalna opasnost od napada iz sajber prostora percipirana znatno pre pojave interneta i složenih računarskih sistema, odnosno da je vizija predstojećeg razvitka i eksplozije računarskih tehnologija u sebi nosila i razumevanje i bojazan od mogućnosti zloupotrebe i potrebu da se pravnim instrumentima pojedinac i društvo zaštite od, tada potencijalnih, a sada veoma realnih i opipljivih pretnji i opasnosti.

Prvi značajan pisani dokument, koji doduše nije bio u formi pravnog akta niti je usvojen od kakve međunarodne organizacije suverenih država, pojavio se 1979. godine u Sjedinjenim Američkim Državama u formi priručnika „Computer Crime – Criminal Justice Resuorce Manual“.[28] Autor priručnika bio je Donn B. Parker, viši stručni konsultant pri istraživačkom institutu Stenford (Stanford Research Institute), a priručnik je bio izrađen za potrebe nacionalne pravosudne službe za statistiku. Kao što je rečeno, iako je u pitanju stručni rad, a ne pravni akt koji bi posedovao svojstvo obaveznosti i čije bi regule bile obezbeđene pravnim sankcijama, u praksi je priručnik veoma brzo postao nezaobilazno stručno štivo svih profesionalnih istražitelja koji su se susretali sa prvim slučajevima računarskog kriminaliteta, koliko god oni bili retki u datom trenutku, odnosno krajem sedamdesetih i početkom osamdesetih godina prošlog veka.

[28] Kompletno drugo izdanje priručnika iz 1989. godine može se pronaći na internet adresi *http://www.eric.ed.gov/ERICDocs/data/ericdocs2sql/content_storage_01/0000019b/80/22/f5/3e.pdf*

I van SAD, naravno, bilo je pojedinaca koji su svojim pionirskim radom ukazali na potencijal računarske tehnologije kao oruđa za izvršenje krivičnih dela. Norvežanin Stein Schjolberg je krajem sedamdesetih godina, kao policijski istražitelj a nakon toga i kao tužilac, pružao pomoć i učestvovao u akcijama Interpola, doprinoseći tako postavljanju osnova koji su omogućili sagledavanje nove vrste kriminaliteta. U Holandiji, akademski radnik H. W. K Kaspersen je još osamdesetih godina XX veka učestvovao u raspravama vezanim za visokotehnološki kriminalitet da bi docnije kroz svoju inicijativu 1997. godine postao poznat kao svojevrsni „otac" *Konvencije o kompjuterskom kriminalu* Saveta Evrope, a poznato je danas da je u pitanju najsveobuhvatniji pravni akt na međunarodnom nivou koji se bavi pitanjima suzbijanja visokotehnološkog kriminala i postavlja osnove za međunarodnu saradnju koja je uslov bez koga se ne može zamisliti uspešna borba protiv ove vrste kriminaliteta.

Na planu međudržavnih organizacija i međunarodnog prava izdvajamo nekoliko značajnih događaja koji prvenstveno ukazuju na postojanje svesti i uočavanje potrebe da se pravno regulišu i urede pitanja koja su u vezi sa zloupotrebama računarskih tehnologija. Interpol je verovatno prva međunarodna organizacija koja ukazuje na potencijal računarske tehnologije kao sredstva za izvršenje krivičnih dela. Na redovnoj konferenciji ove organizacije koja je održana u Parizu 1979. godine naročito je istaknuto da je sama priroda računarskog kriminaliteta internacionalna, odnosno globalna imajući u vidu nagli razvoj telekomunikacionih mreža i satelita i da bi međunarodne organizacije poput Interpola ovom pitanju trebalo da posvete naročitu pažnju. Naravno, Interpol ovim pitanjima i jeste posvetio naročitu pažnju, i to ne samo 1979. godine nego i docnije, imajući u vidu da je reč o organizaciji koja povezuje organe gonjenja raznih suverenih država. Prve organizovane obuke policijskih istražitelja počele su još 1981. godine,[29] a danas Interpol ima organizovane timove koji se bave borbom protiv visokotehnološkog kriminala i poseduje operativne priručnike sa najnovijim podacima i uputstvima za istražitelje.

Što se tiče Saveta Evrope, prva međunarodna inicijativa potiče iz 1976. godine sa Evropske konferencije o kriminološkim aspektima privrednog kriminala, koja je održana u Strazburu. Na ovom stručnom skupu prvi put je ukazano na nekoliko različitih vrsta računarskog kriminaliteta.[30] Savet Evrope

[29] Program obuke organizovao je Interpol u saradnji sa Steinom Schjolbergom. Učestvovalo je 66 polaznika iz ukupno 26 zemalja, a među predavačima bio je i pomenuti Donn B. Parker kao jedan od začetnika borbe protiv sajber kriminala.

[30] Zvaničan dokument sa 12. konferencije rukovodilaca Instituta za kriminološka istraživanja, „Criminological Aspect of Economic Crime", Strasbourg, 15–18. novembar 1976, str. 225–229.

se detaljnije bavio pitanjima računarskog kriminaliteta 1989. godine, kada je i usvojena Preporuka o kriminalnim aktivnostima povezanim sa upotrebom računara.[31] Ova preporuka sadrži obavezujuću listu minimalnih zahteva koji se odnose na taksativno određena krivična dela protiv bezbednosti računarskih podataka, koji su neophodni da se na uniforman, odnosno jednoobrazan način propišu u zakonodavstvima država članica. U pitanju su dela kompjuterske prevare, falsifikati sačinjeni uz pomoć računara, oštećenje računarskih podataka i programa, računarska sabotaža, neovlašćen pristup računaru. Konačno, pored obavezujuće, Preporuka sadrži i takozvanu opcionu listu, odnosno listu delikata čije je propisivanje prepušteno dispoziciji zemalja članica. Na ovoj listi su računarska špijunaža, neovlašćena upotreba računara i neovlašćena izmena računarskih podataka ili programa.

Kako su Preporukom Saveta Evrope br. 89 od 1989. godine bila obuhvaćena pitanja materijalnog krivičnog prava, sledeća relevantna preporuka Saveta Evrope, doneta 1995. godine, za predmet regulisanja uzela je pitanja koja se tiču proceduralnih, odnosno procesnih pravila u vezi sa informatičkim tehnologijama.[32] Ova preporuka utvrđuje ukupno 18 principa koji su svrstani u sedam glavnih poglavlja, i to: pretraga i zaplena, odnosno oduzimanje predmeta, tehnički nadzor, obaveza saradnje istražnih organa, elektronski dokazi, upotreba enkripcije, istraživanje, dokumentovanje podataka i trening, kao i međunarodna saradnja.

I Evropska organizacija za bezbednost i saradnju (OEBS) određenu pažnju posvetila je problemu računarskog kriminaliteta osamdesetih godina prošlog veka. Još 1982. godine osnovana je ekspertska grupa u cilju da sagleda stanje legislative u oblasti visokotehnološkog kriminaliteta i da sačini odgovarajuće preporuke za izmenu zakonskih propisa u cilju usklađivanja pravnih normi sa realnim potrebama. Kao rezultat rada ove grupe, 1986. godine OEBS je, kroz analizu zakonodavstava zemalja članica, usvojio Preporuku za usklađivanje krivičnih zakonika. Pored toga što ukazuje na potrebu za saradnjom na međunarodnom nivou, slično preporukama Saveta Evrope, i OEBS sačinjava listu nedozvoljenih ponašanja u sajber prostoru, koja obuhvata računarske prevare i falsifikate, oštećenje računarskih podataka i programa i neovlašćeni prodor u zaštićeni računarski program ili zaštićeni računarski sistem.

Grupa ekonomski najrazvijenijih država, poznatija kao grupa G-8,[33] takođe se aktivno uključila u problematiku suzbijanja računarskog kriminaliteta.

[31] Savet Evrope: Preporuka No. R. (89) 9.

[32] Savet Evrope: Preporuka No. R. (95) 13.

[33] Grupa se sastoji od sledećih država: Kanada, Francuska, Italija, Japan, Rusija, Velika Britanija, Nemačka i Sjedinjene Američke Države.

Formirana je podgrupa za visokotehnološki kriminal koja je 1998. godine ustanovila mrežu 24/7, odnosno grupu operativaca koji su u svakoj državi dostupni u svakom trenutku radi pružanja operativne podrške u aktuelnim istragama računarskog kriminaliteta. Kao cilj formiranja ove mreže za „hitne intervencije" navedena je potreba da se spreči formiranje takozvanog „kriminalnog raja" bilo gde u svetu i da se pruži pomoć nadležnim istražnim organima u otkrivanju počinilaca i prikupljanju i obezbeđenju elektronskih dokaza. Pored toga, usvojeni su i osnovni principi koji bi trebalo da nađu svoje mesto u pravnim sistemima država članica, a ovi principi tiču se prekograničnog pristupa računarskim podacima, pristupa računarskim podacima pohranjenim u stranoj državi i očuvanja računarskih podataka koji se nalaze u računaru ili računarskom sistemu.

Kada razmatramo pitanje aktuelne pravne regulative u vezi sa borbom protiv visokotehnološkog kriminaliteta, nepodeljeno je mišljenje da jedan pravni akt zaslužuje mesto na vrhu piramide međunarodnih pravnih akata. Reč je o Konvenciji Saveta Evrope o visokotehnološkom kriminalu[34] koja je usvojena na Konferenciji u Budimpešti 23. novembra 2001. godine a stupila na pravnu snagu 1. jula 2004. godine. U pitanju je najznačajniji poduhvat harmonizacije nacionalnih zakonodavstava u borbi protiv visokotehnološkog kriminaliteta, a koliki je značaj ove konvencije i koliko su univerzalni i prihvatljivi ustanovljeni principi i rešenja možda najbolje govori činjenica da su Konvenciji pristupile i države koje nisu članice Saveta Evrope. Ukazujemo i na činjenicu da se pravni akti, rezolucije, preporuke i odluke ostalih međudržavnih organizacija gotovo redovno pozivaju na odredbe Konvencije Saveta Evrope pa stoga i zaključak da je u pitanju krovni pravni akt i najznačajniji legislativni iskorak na međunarodnom planu u okviru suzbijanja visokotehnološkog kriminaliteta.

Uzimajući u obzir da su odredbe Konvencije o visokotehnološkom kriminalu detaljno obrađene i objašnjene u prethodnom poglavlju ove monografije, na ovom mestu daćemo samo kratak pregled najznačajnijih pojmova i pravnih instituta kako bi poglavlje o međunarodnim propisima predstavljalo sistematičan i celovit pregled legislative koji nije zamisliv niti moguć bez najznačajnijeg pravnog akta.

Dakle, predstavljanje osnovnih pravnih akata i međunarodne regulative počinjemo propisima koje je doneo Savet Evrope. Pored pomenute konvencije kao najznačajnijeg akta, analiziraćemo i nekoliko drugih propisa čija je sadržina usko povezana sa računarskim tehnologijama i mogućnostima njihove zloupotrebe. Dalji pregled upotpunićemo propisima koje su donele Uje-

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

dinjene nacije, Evropska unija i druge relevantne regionalne ili specijalizovane međunarodne organizacije.

2.1. Ujedinjene nacije

Ogranizacija Ujedinjenih nacija kao međunarodna organizacija okuplja 192 suverene države i orijentisana je na očuvanje i unapređenje mira i sigurnosti, razvitak prijateljskih odnosa država članica i unapređenje životnog standarda i kvaliteta ljudskih prava u svetu. Zbog svog jedinstvenog karaktera i značaja Organizacija UN uzima aktivnu ulogu u regulisanju brojnih pitanja važnih za sve članice i to čini preko svojih organa: Generalne skupštine, Saveta bezbednosti, Ekonomskog i socijalnog saveta i drugih tela i komisija. U svetlu ubrzanog i planetarnog razvoja informatičkih tehnologija, specijalizovana tela UN preduzela su napore da se na globalnom nivou ispita značaj i uloga informatičkih tehnologija, kao i opasnosti koje dolaze iz ovog „virtuelnog" prostora a koje imaju svoje implikacije kako na život i bezbednost svakog pojedinca, tako i na odnose među suverenim državama i regionalnim i međunarodnim organizacijama. Kroz delatnost Komisije za prevenciju kriminaliteta i krivično pravosuđe učinjeni su napori da se promoviše međunarodna saradnja u oblasti harmonizacije i primene krivičnih zakona u raznim oblastima pa tako i u oblasti borbe protiv visokotehnološkog kriminaliteta. Rezultati ovih napora opredmećeni su u rezolucijama (br. 55/63 i 56/121) o borbi protiv zloupotrebe informatičkih tehnologija, koje je Generalna skupština UN usvojila 2001. i 2002. godine. Ovde valja napomenuti i da je u tzv. milenijumskoj deklaraciji, odnosno Rezoluciji br. 55/2 Generalne skupštine UN od 18. septembra 2000. godine, kao jedan od prioritetnih ciljeva utvrđena i potreba da se nove tehnologije a naročito informatičke i komunikacione učine bezbednim i dostupnim svima.

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

Rezolucija je usvojena na 55. zasedanju Generalne skupštine UN.[35] Uviđajući da slobodan protok informacija podstiče ekonomski razvoj, obrazovanje i demokratiju a istovremeno izražavajući zabrinutost zbog novih mogućnosti za razvoj kriminalnih aktivnosti u svetu informatičkih tehnologija, države članice UN saglasile su se o principima na kojima bi trebalo da počiva borba protiv visokotehnološkog kriminaliteta u budućnosti. Pre nego što izložimo osnovne principe o kojima je postignuta saglasnost,

[35] „Resolution A/res/55/63" General Assembly of the United Nations, 22. januar 2001.

primetićemo da u uvodnom delu Rezolucije donosilac konstatuje da je imao u vidu rezultate do kojih je došla Komisija eksperata Saveta Evrope za pitanja kriminala u sajber prostoru a na osnovu kojih će docnije iste godine u Budimpešti biti usvojena Konvencija o visokotehnološkom kriminalu (ranije smo pomenuli da je ova Konvencija krovni dokument na koji se oslanjaju mnogi pravni akti međunarodnih organizacija, a kao što vidimo harmonizacija je postojala i u fazi neposredno pre usvajanja Konvencije).

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 transnacionalni 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 pravnim mehanizmina zaštititi 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 aktuelnim krivičnim 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 a sve 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 su mnogobrojni, ali najpre treba poći od činjenice da nije jednostavno statistički „brojati" bilo koju vrstu kriminala. Postoje tri osnovna koraka koja su 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 garantovanih svakom pojedincu, sa jedne strane, 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 biti restriktivni samo u onoj meri koja je neophodna za zakonito prikupljanje dokaza i vođenje krivičnog postupka pred nadležnim sudovima.

2.1.2. Rezolucija 56/121 Generalne skupštine UN

Rezolucija je usvojena 23. januara 2002. godine i takođe za predmet ima borbu protiv zloupotrebe informatičkih tehnologija.[36] 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 kao i drugih relevantnih međunarodnih i regionalnih organizacija.

2.1.3. Rezolucija Ekonomsko-socijalnog saveta (ECOSOC) 2007/20

Međunarodna saradnja u oblasti prevencije, istrage, krivičnog progona i kažnjavanja privrednog kriminaliteta i dela povezanih sa zloupotrebom identiteta našla se na dnevnom redu Ekonomsko-socijalnog saveta UN, što je rezultiralo usvajanjem Rezolucije 2007/20 u julu 2007. godine.[37] Neposredan povod za akciju bila je zabrinutost zbog uloge koju informatičke i komunikacione tehnologije imaju u evoluciji, odnosno širenju međunarodnog privred-

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

[37] „Resolution 2007/20", The Economic and Social Council of the United Nations, 26. jul 2007.

nog kriminaliteta, kao i kriminaliteta koji nastaje kao rezultat krađe i zloupotrebe identiteta.

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 s 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 upotrebu 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.

2.1.4. Međunarodna telekomunikaciona unija (ITU)

Organizacija kojoj su Ujedinjene nacije poverile vodeću ulogu u postupku harmonizacije nacionalnih zakonodavstava u oblasti visokotehnološkog kriminala, kao i generalno u materiji bezbednosti u sajber prostoru, jeste upravo Međunarodna telekomunikaciona unija.[38]

Na ovom mestu ukazaćemo na do sada preduzete aktivnosti imajući u vidu da je reč o projektu od globalnog značaja čija bi uspešna realizacija trebalo da rezultira opštom saglasnošću u vezi sa zakonskim i drugim merama koje je neophodno preduzeti u borbi protiv visokotehnološkog kriminaliteta.

Još 2001. godine Generalna skupština Ujedinjenih nacija ukazala je na potrebu za organizovanjem Svetskog samita o informatičkom društvu (World Summit on the Information Society – WSIS). Projekat je zamišljen tako da se odvija u više etapa, tj. faza, a neke od njih su već sprovedene u delo, odnosno preduzeti su značajni koraci ka ostvarenju postavljenih ciljeva sveopšte harmonizacije nacionalnih zakonodavstava. Prva faza projekta odvijala se u Ženevi 2003. godine a druga u Tunisu 2005. godine, kada je Međunarodnoj telekomunikacionoj uniji poveren zadatak u oblasti jačanja međusobnog pove-

[38] Međunarodna telekomunikaciona unija je vodeća agencija u okviru organizacije UN za pitanja komunikacionih i informatičkih tehnologija. Detaljnije o Agenciji i njenom radu pogledaj, internet, *http://www.itu.int* (10. 5. 2009).

renja i sigurnosti u svetu informacionih tehnologija. Kao rezultat dvogodišnjeg rada ITU, generalni sekretar UN je maja 2007. godine predstavio dokument pod nazivom Memorandum o globalnoj sajber bezbednosti (A Global Cybersecuritu Agenda – GCA) kao okvirni (instruktivni) akt o međunarodnoj saradnji i dijalogu na pronalaženju održivih rešenja u okviru globalne informatičke zajednice.[39] Memorandum je predstavio sedam osnovnih strateških ciljeva a među njima kao jedan od prioritetnih i princip o neophodnim zakonodavnim merama. Ovaj princip podrazumeva kritičko ispitivanje svih postojećih legislativnih instrumenata u cilju utvrđivanja opšteprihvaćenog legislativnog modela koji bi bio primenjiv i operativan u svim postojećim nacionalnim i međunarodnim okvirima.

Kao podršku projektu utvrđivanja univerzalnog legislativnog modela za sigurnost u sajber prostoru, generalni sekretar UN formirao je Posebnu grupu eksperata (High Level Experts Group – HLEG) koja broji više od 100 članova i koja je 2008. godine objavila preporuku o pet glavnih pravaca ka kojima bi trebalo usmeriti napore. Najpre, u pitanju su mere legislativnog karaktera, zatim tehničke i proceduralne mere, mere organizacionog karaktera, mere na jačanju kapaciteta u borbi za sajber sigurnost, kao i mere koje se tiču međunarodne saradnje.

Napori ITU usmereni su prvenstveno na postizanje konsenzusa o okviru u kome će se razmatrati pitanja o sajber sigurnosti na međunarodnom nivou kako bi svi učesnici u postupku, na bilo kom stepenu ekonomskog i društvenog razvitka da se nalaze, shvatili potrebu za akcijom na globalnom nivou radi suprotstavljanja pretnjama koje dolaze iz sajber prostora.

Na kraju, ukazujemo da i Memorandum o globalnoj sajber bezbednosti, kao i mnoge druge konvencije, rezolucije i odluke, poziva regulatorna nacionalna tela da prilikom usvajanja zakonodavnih rešenja u oblasti istrage i krivičnog progona visokotehnološkog kriminala obavezno uzmu u obzir postojeće pravne okvire na međunarodnom nivou kao što su rezolucije Generalne skupštine UN 55/63 i 56/121 i regionalne pravne instrumente kao što je Konvencija Saveta Evrope o visokotehnološkom kriminalu (član 40 GCA).

2.2. Savet Evrope

Još od osamdesetih godina prošlog veka, Savet Evrope se bavi pitanjem suzbijanja visokotehnološkog kriminala. U okviru ove organizacije je nastala i zasad jedina međunarodna konvencija koja uređuje pojedina pitanja iz ove oblasti na nadnacionalnom nivou. Donošenju Konvencije prethodili su neo-

[39] „ITU Global Cybersecurity Agenda (GCA): Framework for International Cooperation in Cybersecurity“, internet, *http://www.ifap.ru/library/book169.pdf* (10. 5. 2009).

bavezujući dokumenti i istraživanja, kao što je studija iz 1989. godine u kojoj je po prvi put državama preporučeno da u svoja zakonodavstva uvedu krivična dela vezana za računare i računarske mreže. U tom periodu najveća zabrinutost je vladala kada je reč o nedozvoljenim upadima u računare, ali kako se paleta mogućih zloupotreba povećavala, rastao je i spisak preporuka za inkriminaciju određenih ponašanja. Dve preporuke koje je doneo Komitet ministara, a koje se smatraju prvim međunarodnim dokumentima na temu visokotehnološkog kriminala, uglavnom su posvećene počecima borbe protiv zloupotrebe računarskih tehnologija kao što su: inkriminacija nedozvoljenog ponašanja i jasno razdvajanje legalnih od ilegalnih radnji u nacionalnim zakonodavstvima; odredbe o vršenju istraga povezanih sa korišćenjem i zloupotrebom računara; prisluškivanje i presretanje komunikacija koje su pod istragom; obaveza provajdera novih tehnologija da sarađuju sa policijskim i drugim istražnim organima i sl. U pitanju su preporuke koje nisu bile obavezujuće za države članice, ali čiji je cilj prvenstveno bio da ukažu na pojavu nove vrste kriminalnih aktivnosti koje imaju izraženu međunarodnu komponentu i da se državama stavi do znanja da moraju blagovremeno reagovati da bi se sprečilo širenje takvih nezakonitih i zlonamernih korišćenja novih tehnologija komunikacije.[40] Konačno, kada je tokom druge polovine devedesetih godina postalo jasno da visokotehnološki kriminal sve više uzima maha i da će se s razvojem interneta i novih računarskih tehnologija opasnosti od korišćenja u ilegalne svrhe višestruko uvećati, Evropski komitet za probleme krivičnog prava Saveta Evrope (*European Committee on Crime Problems*, CDPC) osnovao je ekspertsku grupu, Komitet eksperata za krivična dela počinjena u sajber prostoru (*Committee of Experts on Crime in Cyberspace*, PC-CY), sa zadatkom da sačini tekst prve međunarodne konvencije koja bi se bavila kako materijalnim pravom – inkriminacijom određenih štetnih ponašanja – tako i procesnim pravom, u cilju da se olakša prevencija, hvatanje i kažnjavanje počinilaca ove vrste krivičnih dela putem jače i institucionalizovane međunarodne saradnje.[41]

Konvencija Saveta Evrope o visokotehnološkom kriminalu[42] usvojena je 2001. godine. Za njeno stupanje na snagu bilo je potrebno najmanje pet ratifikacija, od toga najmanje tri od strane država članica Saveta Evrope, što se i

[40] U pitanju su preporuke R (89)9 i R (95)13. Tekst Preporuke R (95)13 može se naći na internet adresi: *http://www.usdoj.gov/criminal/cybercrime/crycoe.htm*, 1. 5. 2009.

[41] Odluka CDPC/103/211196 od 21. novembra 1996. godine.

[42] Konvencija 185 Saveta Evrope. Tekst Konvencije i ostali bitni podaci mogu se naći na internet adresi: *http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG*, 1. 5. 2009.

dogodilo 1. jula 2004. godine.[43] Do sada su je potpisale 43 zemlje članice Saveta Evrope, od kojih su je ratifikovale samo 22 države.[44] Srbija se nalazi među državama koje su Konvenciju potpisale (2005. godine) i ratifikovale (2009. godine).[45] Od država koje nisu članice Saveta Evrope potpisale su je Kanada, Japan, Južna Afrika i SAD, ali su je ratifikovale samo SAD.[46]

Godine 2003. donet je Dodatni protokol uz Konvenciju, koji se bavi inkriminisanjem akata rasističke i ksenofobične prirode počinjenih putem računarskih sistema. Dodatni protokol je stupio na snagu nakon što ga je ratifikovalo pet država, 1. marta 2006. godine.[47]

2.2.1. 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.[48]

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. Stoga 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

[43] Konvencija je otvorena za potpisivanje i prema državama koje nisu članice Saveta Evrope.

[44] Konvenciju od država članica SE nisu potpisale Andora, Monako, Rusija i San Marino.

[45] „Službeni glasnik RS“, br. 19/09; Srbija je istovremeno ratifikovala i Dodatni protokol uz Konvenciju. Od država iz regiona, Konvencija je ratifikovana i stupila na snagu u Albaniji, Bosni i Hercegovini, Bugarskoj, Hrvatskoj, Mađarskoj, Rumuniji, Sloveniji i Makedoniji. Crna Gora još nije ratifikovala Konvenciju.

[46] Spisak potpisa i ratifikacija može se naći na internet adresi (stanje na dan 6. 3. 2009. godine): *http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=3/6/2009&CL=ENG*, 1. 5. 2009.

[47] Više na internet adresi: *http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=3/6/2009&CL=ENG*, 1. 5. 2009.

[48] *Convention on Cybercrime – Explanatory Report*, str. 4–5. Tekst dostupan na internet adresi: *http://conventions.coe.int/Treaty/en/Reports/Html/185.htm*, 1. 5. 2009.

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.

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 izvoditi 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 se može podrazumevati 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.[49]

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 eliminisati mogućnost da se u slučaju eventualne ekstradicije počinioca stavi prigovor nedostatka dvostruke inkriminacije.[50]

[49] Član 1 Konvencije.

[50] *Convention on Cybercrime – Explanatory Report*, *loc. cit.*, str. 8.

Prva grupa inkriminisanih dela visokotehnološkog kriminala može se označiti 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:[51]

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*) se ispoljavaju pre svega kao forma nenasilnog preuzimanja kontrole nad tuđim računarom, čega vlasnik računara 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 (otud analogija sa trojanskim konjem). Slično „trojancima" deluju i „logičke bombe", štetni programi poput virusa, ali bez mogućnosti samostalnog izvršavanja 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 barem 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 za krajnji cilj imaju izmenu podataka na računaru ili njihovo slanje autoru štetnog programa (radi dalje zloupotrebe, najčešće preuzimanja identiteta napadnutog računara).

[51] Članovi 2–6 Konvencije.

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 mogu susresti nacionalni zakonodavci ili međunarodna zajednica 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 savremene tehnologije. Stoga, 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 pravo, 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.

Takav 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 se možda ne može primeniti 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, koja sada postoji, između dinamike razvoja pravnih akata i tehničko-tehnoloških mogućnosti za njihovo kršenje.

Druga grupa inkriminisanih dela mogla bi se označiti kao visokotehnološka varijanta klasičnih krivičnih dela. Ova sekcija Konvencije obuhvata dva dela: falsifikovanje i prevaru.[52]

[52] 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.

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.[53]

Države potpisnice se obavezuju da kao krivično delo u domaćim zakonodavstvima inkriminišu 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, inkriminisano je, u stvari, 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.

Evropska konvencija o visokotehnološkom kriminalu, uvidevši ozbiljnost i rasprostranjenost ovog problema, pokušava da autoritativno navede države da harmonizuju svoja zakonodavstva i da 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 koje se osobe 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 ostav-

[53] Član 9 Konvencije.

lja 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.[54] U tri stava, kršenje autorskih prava se ne inkriminiše samostalno, već 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 propisivanjem sankcija za počinjena dela iz Konvencije.[55]

Drugi deo drugog poglavlja pod nazivom „Procesno pravo" bavi se procesnim ovlašćenjima državnih organa prilikom istraživanja krivičnih dela vezanih za nove tehnologije.[56] 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 se mogu podvesti 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.[57]

Prema Konvenciji, nadležni državni organi imaju ovlašćenja da pregledaju i zaplene svaki računar ili nosač podataka na kome se nalaze, ili sumnjaju

[54] Član 10 Konvencije.

[55] 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 vrlo 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.

[56] Članovi 14–22 Konvencije.

[57] Član 15 Konvencije.

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.[58]

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.[59] Ova oblast intervencije državnih organa je i najosetljivija, jer se praktično povređuje pravo na privatnost i pravo na prepisku, a sama Konvencija ne sadrži odgovarajuća 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 dovesti do zloupotrebe ovlašćenja državnih organa. Štaviše, stav 3 pomenutog člana određuje da države moraju propisati uslove pod kojima će provajderi, koji nužno moraju učestvovati u sakupljanju ovih informacija, činjenicu da se određeni korisnik špijunira, kao i sadržinu podataka koji su na taj način prikupljeni, morati da čuvaju kao tajnu. Kada se posmatraju istrage koje mogu dovesti 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

[58] Članovi 19 i 20 Konvencije.

[59] 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.

svake pojedinačne zemlje.[60] 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 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 ustupiti 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[61] – može se na to dodati, iz očiglednih razloga da bi se zahtevanjem od provajdera da sakupljaju sve podatke koji su u vezi sa aktivnostima njihovih klijenata i da ih čuvaju 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).[62] Može se reći da kombinacija teritorijalno-personalne jurisdikcije nije najsrećnije rešenje, iako je to klasični instrument kada je reč o međunarodnim ugovorima. 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, st. 3 i 4 pokušavaju da stvari postave na malo čvršćim osnovama – ako država ne izvrši ekstradiciju svog državljanina, mora mu suditi za počinjena dela na teritoriji druge države potpisnice,[63] 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.

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

[61] *Convention on Cybercrime – Explanatory Report*, *loc. cit.*, str. 25.

[62] Član 22, stav 1 Konvencije.

[63] Na ovaj slučaj se primenjuje i odredba sadržana u članu 24, stav 6.

Treći deo Konvencije se bavi međunarodnom saradnjom država na suzbijanju visokotehnološkog kriminala, i to pre svega na način koji bi trebalo 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.[64]

Otuda su glavne odredbe ovog dela posvećene saradnji država na organizovanoj ili spontanoj razmeni podataka[65] 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 poveriti određenom telu posao saradnje sa drugim državama u oblasti visokotehnološkog kriminala, a u slučaju hitnosti, saradnja može biti 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.[66] Prema članu 31 Konvencije, svaka država potpisnica može tražiti 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 dosta prostora da u praksi, ili u dodatnim bilateralnim sporazumima, dalje preciziraju one vrste saradnje za koje imaju poseban interes.

Kada je reč o ekstradiciji, 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 biti označeno kao ozbiljno u samom zakonu, odnosno za njegovo izvršenje mora biti 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.[67] 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.[68] Ovo rešenje

[64] Članovi 23–35 Konvencije.
[65] Videti član 26 Konvencije.
[66] Član 27, stav 9 Konvencije.
[67] Član 24, stav 1 Konvencije.
[68] Član 35 Konvencije.

se nastavlja na neki način, odnosno ima isti cilj kao odredba iz člana 27, stav 2 Konvencije, koji predviđa angažovanje posebnog državnog organa za saradnju sa drugim državama potpisnicama. Opet, nema reči o specijalizaciji takvog tela – saradnja na polju visokotehnološkog kriminala može biti samo jedan od aspekata njegovog rada. Ovim merama se pokušao ublažiti 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.

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[69] je zato naziva „najgorim internet pravom na svetu", koje predviđa da čak i akti koji nisu predviđeni kao krivična dela u SAD mogu biti gonjeni u ovoj zemlji po zahtevu neke druge države u kojoj se smatraju kažnjivim.[70] 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.[71] Činjenica je da se ovakva kategorizacija Konvencije ne može u potpunosti opravdati, ali veoma dobro ilustruje strah od „sudara" potpuno različitih kul-

[69] EFF (*Electronic Frontier Foundation*) je jedna 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*, 1. 5. 2009.

[70] 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.

[71] Izvor: Nate Anderson, *World's Worst Internet Law*, *http://arstechnica.com/news.ars/post/20060804-7421.html*, 1. 5. 2009.

tura, civilizacija i vrednosti na internetu. Otuda možda i nedostatak relevantnog međunarodnog dokumenta 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. i stupio je na snagu 1. marta 2006. godine.[72] 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.[73]

Kao što 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 biti korisne i edukativne, ali isto tako mogu biti, npr. 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 veoma 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 se ne može pravovremeno i adekvatno reagovati 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 činjenice 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.

[72] Tekst Protokola (na engleskom jeziku) na internet adresi: *http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm*, 1. 5. 2009.

[73] Srbija i Crna Gora je potpisala Protokol 7. 4. 2005. godine. Lista ratifikacija može se naći na internet adresi: *http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=189&CM=&DF=&CL=ENG*, 1. 5. 2009.

U relativno kratkom tekstu, Protokol uvodi obavezu za države potpisnice da u nacionalnom zakonodavstvu inkriminišu sledeća ponašanja:[74]

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 rasi, boji kože, poreklu, nacionalnoj, etničkoj ili verskoj pripadnosti. Država može staviti rezervu na ovaj član i ne primenjivati ga, ili može ograničiti 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, počevši od Međunarodnog vojnog tribunala 1945. godine i nadalje. Kao i kod prvog navedenog dela u Protokolu, ovakav sadržaj se mora na neki način učiniti dostupan 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 koja su utvrđena Protokolom.

[74] Članovi 3–6 Protokola.

2.2.2. Konvencija o zaštiti prava pojedinca u vezi sa automatskom obradom ličnih podataka[75]

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 u svetlu 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 koji su pohranjeni u računarima i računarskim sistemima (socijalna i medicinska zaštita, podaci o zdravstvenom stanju pojedinaca, podaci neophodni za obračun i isplatu zarada itd.). Stoga, 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 a 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 ova konvencija odnosi na lične podatke prikupljene kako u javnom, tako i u privatnom sektoru.

[75] *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).

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 automatski 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 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 pojedinačnim 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).

2.2.3. Konvencija o zaštiti dece od seksualne eksploatacije i seksualnog zlostavljanja[76]

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 u svetlu 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 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 nepo-

[76] *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*, Lanzarote, 25. 10 .2007. godine.

sredno 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.

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 za 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 koja su 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 po-

stupajućeg 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 servisa, 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.

2.2.4. Konvencija o sprečavanju terorizma[77]

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 koja se odnose na sajber terorizam 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 visokotehnološkom 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 zak-

[77] *Council of Europe Convention on the Prevention of Terrorism* (CETS No. 196).

ljučeno 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 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.[78]

Pre nego što analiziramo odredbe Konvencije koje su u vezi sa zloupotrebom računarskih tehnologija za vršenje terorističkih akata ukazaćemo na načine na koje se internet i računarske tehnologije generalno mogu koristiti u navedene svrhe. Najpre, reč je o napadima putem interneta, koji mogu biti 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 se koristiti 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 sredstava i finansiranje terorizma. Konačno, internet kao globalna mreža služi i kao sredstvo za komunikaciju između članova grupe, kao i instrument za planiranje i podršku.

Iz ugla informatičkih tehnologija, značajni su čl. 5–7 Konvencije koji se odnose na određene pripremne radnje koje su 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

[78] *Council of Europe Convention on the Prevention of Terrorism* (CETS No. 196), Appendix.

delo, ili više njih, moglo biti 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 uz pomoć interneta kao globalne mreže. U skladu sa odredbama Konvencije, neophodno je i da je regrutacija izvršena prtivpravno i u određenoj nameri.

Konačno, računarske tehnologije i internet (kao i elektronska pošta, diskusioni forumi, *chat* ili *news* grupe itd.) mogu se upotrebiti 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".

2.3. 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 javih komunikacionih mreža.

2.3.1. Direktiva Saveta Evropske zajednice o pravnoj zaštiti kompjuterskih programa

Direktiva je objavljena u „Službenom listu Evropske zajednice", br. L 122/42 od 17. maja 1991. godine sa obavezom primenjivanja u državama

članicama počevši od 1. januara 1993. godine, do kada su bile dužne da svoja nacionalna zakonodavstva usklade sa sadržinom Direktive.[79]

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 ovi problemi mogli postati složeniji 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 biti 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.

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 razloga za osnovanu sumnju u njenu nedozvoljenost;
- držanje iz komercijalnih razloga kopije kompjuterskog programa, znajući da je kopija nedozvoljena ili imajući razloga za osnovanu sumnju u njenu nedozvoljenost;

[79] „Council Directive of 14 may 1991 on the Legal Protection of Computer Programs", Directive 91/250/EEC, OJ no L 122/42.

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

2.3.2. 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.[80] 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 pod kojima države članice mogu ograničiti navedeni obim prava i obaveza s tim što svako takvo

[80] „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. 4. 2006.

ograničenje mora biti 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[81] 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 ovog 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 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 (člana 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 ispunjavati zahteve nužnosti i srazmernosti i mora služiti tačno određenim, jasnim i legitimnim svrhama i biti 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 i Konvencija Saveta Evrope o zaštiti prava pojedinaca u vezi sa automatskom obradom ličnih podataka iz 1981. godine takođe obuhvataju i

[81] *Convention for the Protection of Human Rights and Fundamental Freedoms,* CETS No. 005, Council of Europe, Rome, 4. 11. 1950.

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 konferencijske 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, 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 taksativno su 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 adresu/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 koji su 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 *(pre-paid)* 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 preduzeti 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. Po dobijanju 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 biti srazmerne i takve da odvraćaju od daljeg kršenja zakona.

2.4. Ostale regionalne organizacije

Istakli smo u uvodnom delu da je za efikasnu borbu protiv visokotehnološkog kriminaliteta neophodna globalna reakcija. Na ovom mestu ćemo u kratkim crtama izložiti i aktivnosti koje na legislativnom planu preduzimaju najznačajnije regionalne organizacije suverenih država. To je neophodno kako

bi pregled međunarodnih dokumenata i aktivnosti bio potpun i kako bi potvrdio da je globalna i usklađena akcija neophodna kako bi se ostvarili značajni rezultati u suzbijanju ove vrste kriminaliteta.

2.4.1. Komonvelt (The Comnonwealth)

Na ministarskoj konferenciji država Komonvelta[82] održanoj 2002. godine usvojen je predlog zakona pod nazivom „Računari i krivična dela povezana sa računarima".[83] Ovaj zakonski predlog u potpunosti je usklađen sa zakonodavnim okvirima koje postavlja Konvencija o visokotehnološkom kriminalu kako bi se izbegle veće nesaglasnosti u pogledu osnovnih mehanizama i pravnih instituta. Ovaj predlog zakona treba da posluži državama članicama kao model za usvajanje nacionalnog zakonodavstva koje bi bilo sinhronizovano i usklađeno sa drugim relevantnim pravnim propisima međunarodnog karaktera.

2.4.2. Organizacija američkih država (Organisation of American States – OAS)

Na sastanku ministara pravde i državnih tužilaca OAS 1999. godine u Peruu preporučeno je formiranje ekspertske grupe za visokotehnološki kriminal, koju bi činili predstavnici vlada svih zemalja članica.[84] Na redovnom sastanku 2002. godine navedenoj grupi eksperata dat je zadatak da pripremi legislativni predlog koji bi se na nivou država članica bavio pitanjima jačanja međudržavne saradnje u oblasti borbe protiv visokotehnološkog kriminaliteta posebno uzimajući u obzir pravo na privatnost, pravo na dostupnost i zaštitu podataka, kao i procesne aspekte.

U Vašingtonu, ministri pravde i državni tužioci članica usvojili su 2004. godine preporuku da se ispita mogućnost primene osnovnih principa Konvencije Saveta Evrope o visokotehnološkom kriminalu u državama članicama i da svaka država pojedinačno razmotri mogućnost ratifikovanja navedene Konvencije.

Konačno, na Konferenciji OAS u Madridu 2005. godine pod nazivom „Visokotehnološki kriminal. Globalni izazov, globalni odgovor", u saradnji sa Savetom Evrope i Španijom, usvojen je zaključak kojim se podstiču države članice da ozbiljno razmotre mogućnost ratifikacije Konvencije o visoko-

[82] Pogledati, internet, *www. thecommonwealth.org* (10. 5. 2009).

[83] „Computer and Computer Related Crimes Act", Legal and Constitutional Affairs Division, Commonwealth Secretariat.

[84] Pogledati, internet, *www.oas.org/juridico/english/cyber.htm* (11. 5. 2009).

tehnološkom kriminalu kako bi u praksi zaživeo jedinstven legislativni okvir za suzbijanje visokotehnološkog kriminaliteta.

Na ovaj način još jednom je ukazano na univerzalni značaj Konvencije Saveta Evrope o visokotehnološkom kriminalu, naročito u oblasti međunarodne saradnje.

Asian Pacific Economic Cooperation (APEC)[85] *i Association of Southeast Asian Nations (ASEAN).*[86]

Na isti način kao i Organizacija američkih država i navedene međudržavne organizacije u okviru svoje redovne delatnosti pozivaju države članice da usvoje i primene osnovne principe i pravne instrumente koji su ustanovljeni Konvencijom Saveta Evrope o visokotehnološkom kriminalu i Rezolucijom Ujedinjenih nacija 55/63 o borbi protiv zloupotrebe informatičkih tehnologija.

[85] Pogledati, internet, *www.apec.org* (11. 5. 2009).
[86] Pogledati, internet. *www.aseansec.org* (11. 5. 2009).

III

ZAKONI I PODZAKONSKI AKTI REPUBLIKE SRBIJE U OBLASTI BORBE PROTIV VISOKOTEHNOLOŠKOG KRIMINALITETA

1. NACIONALNO ZAKONODAVSTVO I VISOKOTEHNOLOŠKI KRIMINAL

1.1. 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,[87] 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 kojim 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[88] koji uspostavlja procesnopravne okvire kojima su predviđeni mehanizni 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 kriminala usvajanjem odgovarajućih zakonodavnih rešenja i unapređenjem međunarodne saradnje. Rezultat takvih napora je, između ostalog, i donošenje Konvencije o sajber kriminalu Saveta Evrope[89] 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 krimi-

[87] „Službeni glasnik RS“, br. 61/05.
[88] „Službeni glasnik RS“, br. 58/04,... 49/07.
[89] Convention on Cybercrime, Budapest, 23. XI. 2001. (ETS No. 185).

nala, u ovom slučaju visokotehnološkog, jeste pitanje koje uvek nameće niz nedoumica i 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 državnim organima omogućio 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, jeste pitanje čiji odgovor mora da pomiri različite zahteve 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 manjih sredstava, ali, s druge strane, može nametnuti i druge probleme 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. Potpuno je jasno da je naša država u pokušaju da obezbedi krivičnopravnu zaštitu u pogledu novih pojavnih oblika kriminala, kao što je visokotehnološki kriminal, odabrala delimične ciljane promene pojedinih zakona, uz donošenje novog zakona, kojima se uspostavljaju novi državni organi za postupanje u ovim krivičnim predmetima, što je imajući u vidu mogućnosti naše države sasvim razumljivo. Međutim, način kako je to učinjeno u pogledu nadležnosti, primene već zastarelih zakonskih rešenja, kako u pogledu materijalnog prava, tako i u pogledu procesnih ovlašćenja u postupku otkrivanja učinilaca ovih krivičnih dela i obezbeđivanju dokaza, u praksi stvara niz problema. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, koji je stupio na snagu 25. jula 2005. godine, predviđa osnivanje posebnih organa za borbu protiv visokotehnološkog kriminala u okviru postojeće sudske i tužilačke organizacije i Ministarstva unutrašnjih poslova. 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 za 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. Ukoliko se uzmu u obzir elementi bića ovih krivičnih dela i mogući načini njihovog izvršenja – da se distribucija sadržaja uglavnom vrši preko interneta te da su, recimo, pribavljanje relevantnih identifikacionih podataka za izradu lažne platne kartice kao i sama izrada i korišćenje nezamislivi bez upotrebe specifičnih elektronskih uređaja i programa koji po svojoj prirodi i nameni jesu računari i računarski programi, vidi se da je veliki propust učinjen činjenicom da se krivično gonjenje učinilaca ovakvih krivičnih dela i dalje nalazi u okviru organa opšte nadležnosti. S druge strane, samo krivično delo prikazivanje pornografskog materijala i iskorišćavanje dece za pornografiju iz člana 185 Krivičnog zakonika Republike Srbije propisuje nedopustivo male kazne (za najteži oblik izvršenja ovog krivičnog dela, koji podrazumeva iskorišćavanje deteta za proizvodnju slika, audio-vizuelnih ili drugih predmeta pornografske sadržine, zaprećena je kazna zatvora u rasponu od šest meseci do pet godina) i ne sankcioniše posedovanje ovakvih materijala. U vezi sa ovim propustom u određivanju stvarne nadležnosti Posebno tužilaštvo za borbu protiv visokotehnološkog kriminala pokrenulo je inicijativu i sačinilo predlog izmena zakona u pogledu ovlašćenja za procesuiranje i ovih krivičnih dela.

Drugu grupu propisa u zakonodavstvu Republike Srbije koji se tiču visokotehnološkog kriminala čine propisi materijalnog karaktera. To je pre svega Krivični zakon Republike Srbije,[90] 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 su da važe Krivični zakon Republike Srbije i

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

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. Predstavljena informacija, kao i znanje, činjenica, koncept ili naredba, smatra se računarskim podatkom 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 krivičnog zakona. Konkretna krivična dela, propisana krivičnim zakonodavstvom, jesu pre svega ona koja se odnose na bezbednost računarskih podataka. Navedena krivična dela sadržana 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, neovlašće-

ni 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 posebno propisana i obuhvaćena Konvencijom i zbog toga 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.

Kada je reč o usklađenosti domaćeg materijalnog prava sa odredbama Konvencije o sajber kriminalu, može se reći da neke od odredaba ispunjavaju zahteve Konvencije, dok neke odredbe ne ispunjavaju zahteve Konvencije, a neke nedostaju. I pre ratifikovanja Konvencije[91] veliki korak je načinjen izmenama postojećeg zakonodavstva, prvobitno izmenama Krivičnog zakona Republike Srbije, a kasnije donošenjem potpuno novog za-

[91] Republika Srbija je ratifikovala Konvenciju Zakonom o potvrđivanju Konvencije o visokotehnološkom kriminalu i Zakonom o potvrđivanju Dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema od 18. 3. 2009. godine.

konika. Činjenica da je Konvencija ratifikovana pruža mogućnost za potpunu implementaciju odredaba koje predviđa, a to je neophodno što pre uraditi u cilju stvaranja pretpostavki za što uspešniju borbu protiv visokotehnološkog kriminala. Analizirajući usklađenost Konvencije i domaćeg materijalnog zakonodavstva, primetno je da Krivični zakonik u definisanju značenja pojmova koji spadaju u oblast visokotehnološkog kriminala koristi niz izraza, od kojih su neki sadržani u pomenutom članu 112 – računarski podatak, računarska mreža, računarski program i računarski virus, dok su ostali sadržani u opisu konkretnih krivičnih dela kao što je slučaj sa pojmovima podatak, računar, elektronska obrada i prenos podataka, javna računarska mreža, računarske usluge i sl. I pored svih pojmova koje definiše, Krivični zakonik ne poznaje definiciju osnovnog hardvera – računara iako koristi izraz računar kada definiše, npr. računarsku mrežu. Ova činjenica može stvoriti probleme u praksi jer ostaje nejasno da li računar obuhvata samo procesorsku jedinicu ili i periferne jedinice i uređaje za skladištenje podataka. Takođe, zbog nepostojanja opšte definicije teško je utvrditi koji još oblici modernih računarskih sistema mogu biti uključeni u pojam računara (palm top uređaji, mobilni telefoni novijih generacija koji koriste operativne sisteme).

U pogledu konkretnih krivičnih dela iz oblasti visokotehnološkog kriminala predviđenih Konvencijom situacija je sledeća:

Odredba vezana za nezakonit pristup iz člana 302 Krivičnog zakonika u skladu je sa zahtevima člana 2 Konvencije.

U pogledu člana 3 Konvencije, koji reguliše nezakonito presretanje, u domaćem zakonodavstvu član 298 KZ može se identifikovati kao odredba koja odgovara ovom članu Konvencije. Pomenuti član 298 inkriminiše nezakonito ometanje računarskih podataka brisanjem, menjanjem ili na neki drugi način činjenjem neupotrebljivim, ali ova odredba ne štiti integritet podatka od neovlašćenog presretanja s obzirom na to da se u procesu presretanja podaci niti brišu niti menjaju. Zbog toga član 298 ne odgovara zahtevima Konvencije, a ostaje nejasno i da li član 303 koji inkriminiše neovlašćeni pristup procesima elektronske obrade podataka inkriminiše i presretanje (ne)javnih prenosa računarskih podataka.

U pogledu člana 4 Konvencije, kojim je regulisano ometanje podataka, u domaćem zakonodavstvu član 300 KZ delimično odgovara zahtevima Konvencije. Član 300 inkriminiše stvaranje kao i unošenje računarskih virusa i, s jedne strane, sledi širi koncept od člana 4 Konvencije jer pokriva svaku vrstu štete dok, sa druge strane, ne ispunjava zahteve Konvencije s obzirom na to da poznaje samo ometanje podataka prouzrokovano virusima, ali nije primenjiv ukoliko je u pitanju ručno brisanje podatka iz računarskog sistema ili

ukoliko je ometanje podataka prouzrokovano nekim zlonamernim softverom.[92]

U vezi sa članom 5 Konvencije, kojim je propisano ometanje sistema, čl. 299 i 300 KZ mogu se identifikovati kao odredbe koje delimično odgovaraju zahtevima Konvencije. U pogledu člana 300 važi ono što je rečeno prethodno u pogledu člana 4, odnosno ovom odredbom domaćeg zakonodavstva sankcionisana je samo šteta prouzrokovana računarskim virusima, ali ova odredba nije primenjiva ukoliko je šteta prouzrokovana napadom onemogućavanja usluga ili napadom računarskim crvom. S druge strane, član 299 inkriminiše ometanje računarskih podataka kao i hardvera, koje se vrši u nameri sprečavanja ili prekida postupka elektronske obrade i prenosa podataka i čak prevazilazi zahteve Konvencije s obzirom na to da je za postojanje krivičnog dela dovoljno da učinilac namerava da omete proces obrade ili prenosa, dok, sa druge strane, osim ometanja vezanog za podatke, poznaje i fizičko ometanje hardvera.

U vezi sa članom 6 Konvencije, kojim je propisana zloupotreba uređaja, čl. 302 i 199, stav 4 KZ mogu se identifikovati kao oni koji delimično odgovaraju zahtevima Konvencije. Ovo stoga što član 302 inkriminiše nezakonit pristup podacima i ne pokriva one pripremne radnje koje su predviđene ovim članom Konvencije, dok član 199, stav 4 inkriminiše radnje u pogledu opreme i uređaja čiji je cilj uklanjanje, zaobilaženje ili osujećivanje tehnoloških mera namenjenih sprečavanju povreda autorskih i srodnih prava, što znači da je ova odredba ograničena samo na kršenje autorskih prava koja nisu na spisku krivičnih dela na koja se ovaj član Konvencije odnosi.

Inkriminisanje računarskog falsifikovanja kako je to ustanovljeno članom 7 Konvencije još nije primenjeno u Krivičnom zakoniku Republike Srbije.

U pogledu člana 8 Konvencije, kojim je propisana prevara sa računarima, odredba člana 301 KZ može se identifikovati kao ona koja odgovara ovom članu Konvencije s obzirom na to da obe odredbe predviđaju radnje koje podrazumevaju određenu interakciju sa računarskim podacima u cilju pribavljanja protivpravne imovinske koristi, čime se nanosi šteta drugim licima. Glavna razlika odnosi se na činjenicu da član 301 ne sadrži sva dela pomenuta u članu 8 Konvencije.

U vezi sa članom 9 Konvencije, kojim je regulisana dečja pornografija, član 185 KZ može se identifikovati kao odredba koja odgovara pomenutom članu Konvencije i koja inkriminiše radnje vezane za proizvodnju i distribuciju dečje pornografije. U načinu kako su ove radnje formulisane izvesno je da proizvodnja dečje pornografije radi distribucije na mrežama nije izričito

[92] Npr. računarski crvi, trojanci i sl.

sankcionisana. Pored navedenog, samo nabavljanje i posedovanje dečje pornografije nije uopšte inkriminisano. Takođe, starosni limit za definisanje ko se smatra detetom drugačije je postavljen s obzirom na to da je po odredbama Konvencije to šesnaest godina, dok je po odredbama Krivičnog zakonika četrnaest godina. Međutim, imajući u vidu činjenicu da član 9, stav 4 Konvencije pruža državama članicama mogućnost da unesu rezerve, inkriminisanje kako je to urađeno u domaćem zakoniku nije u suprotnosti sa Konvencijom, ali se ne može reći ni da je primenjeno na način kako je to propisano Konvencijom.

U vezi sa članom 10 Konvencije, kojim je regulisano kršenje autorskih prava, odredbe čl. 199 i 200 KZ mogu se identifikovati kao one koje odgovaraju odredbama Konvencije, s tim što ne obuhvataju sve elemente koje ima u vidu ovaj član Konvencije.

U pogledu člana 11 Konvencije kojim je propisan pokušaj, pomaganje ili podstrekavanje u izvršenju krivičnih dela visokotehnološkog kriminala treba reći da odredbe člana 30 KZ inkriminišu pokušaj izvršenja krivičnog dela, dok član 35 KZ inkriminiše pomaganje ili podstrekavanje učinioca krivičnog dela.

U pogledu člana 12 Konvencije, kojim je regulisana odgovornost pravnog lica, Zakonom o odgovornosti pravnih lica za krivična dela[93] uređeni su uslovi odgovornosti pravnih lica za krivična dela, krivične sankcije koje se mogu izreći pravnim licima i pravila postupka u kojem se odlučuje o odgovornosti pravnih lica, izricanju krivičnih sankcija, donošenju odluke o rehabilitaciji, prestanku mere bezbednosti ili pravne posledice osude i izvršenju sudskih odluka. Prema odredbama ovog zakona, pravno lice može odgovarati za krivična dela iz posebnog dela Krivičnog zakonika i drugih zakona, što se odnosi i na krivična dela visokotehnološkog kriminala, ako su ispunjeni uslovi za odgovornost pravnog lica predviđeni ovim zakonom. Pomenuti uslovi podrazumevaju da pravno lice odgovara za krivično delo koje u okviru svojih poslova, odnosno ovlašćenja učini odgovorno lice u nameri da za pravno lice ostvari korist. Odgovornost pravnog lica postoji i ako je zbog nepostojanja nadzora ili kontrole od strane odgovornog lica omogućeno izvršenje krivičnog dela u korist pravnog lica od strane fizičkog lica koje deluje pod nadzorom i kontrolom odgovornog lica. Pravnom licu se za krivično delo mogu izreći sledeće krivične sankcije: kazna, uslovna osuda i mere bezbednosti. Kazne su novčana kazna i prestanak pravnog lica. Novčana kazna ne može biti manja od sto hiljada dinara niti veća od pet stotina miliona dinara i izriče se u zavisnosti od kazne zaprećene za konkretno krivično delo. Navedenim zakonom je

[93] „Službeni glasnik RS“, br. 97/08.

takođe propisana shodna primena odredaba Krivičnog zakonika Republike Srbije u pogledu značenja pojmova i Zakonika o krivičnom postupku u pogledu toka postupka. Ovaj zakon, koji je sada po prvi put usvojen u našem zakonodavstvu, predstavlja značajnu novinu i upotpunjuje sistem krivične odgovornosti za izvršeno krivično delo i isključuje dosadašnji sistem individualnog sankcionisanja pojedinačne radnje jednog ili više fizičkih lica, čime se znatno otežava sankcionisanje nedozvoljenog ponašanja privrednog subjekta u privrednom i platnom prometu, pogotovo što pravno lice odgovara i za krivično delo odgovornog lica i ako je krivični postupak protiv odgovornog lica obustavljen ili je optužba odbijena.

U pogledu člana 13 Konvencije, kojim su regulisane krivične sankcije, treba reći da u Krivičnom zakoniku Republike Srbije krivične sankcije nisu pokrivene jednom odredbom, već su određene u okviru definicije svakog krivičnog dela. Vezano za pitanje koje su kazne adekvatne u smislu zahteva Konvencije da one treba da budu delotvorne, proporcionalne i da odvraćaju, te da uključuju i lišavanje slobode, valjalo bi se prilikom izmena Krivičnog zakonika fokusirati na pitanje da li sankcije predviđene u njemu odgovaraju zahtevima Konvencije.

Iz svega iznetog proizlazi da neke od odredaba domaćeg zakonodavstva treba razmotriti i izmeniti kako bi odgovarale zahtevima Konvencije, te da navedene odredbe i rešenja predviđena Konvencijom treba shvatiti kao preporuke koje predstavljaju minimum standarda koji treba ispuniti ukoliko se žele stvoriti adekvatni preduslovi za uspešnu borbu protiv visokotehnološkog kriminala.

Pored Krivičnog zakonika, i Zakonom o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine[94] 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 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.

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

[94] „Službeni glasnik RS“, br. 46/06.

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 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 je informacija ili podatak značajan za istragu, koji je 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 biti smešteni na pojedinačnom računaru, računarskoj mreži ili udaljenom serveru van teritorijalne nadležnosti organa koji ih prikupljaju, mogu biti 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 biti 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 značajne za krivični postupak utvrđuju se kroz radnje dokazivanja strogo propisane u Zakoniku o krivičnom postupku,[95] 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

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

pogledu svih ostalih dokaza. Polazeći od osnovne premise da samo činjenice prikupljene na zakonom propisan način mogu imati karakter dokaza u postupku i doprineti 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. 77 do 81, privremeno oduzimanje predmeta – čl. 82 do 86, postupanje sa sumnjivim stvarima – čl. 87 i 88, saslušanje okrivljenog – čl. 89 do 95, saslušanje svedoka – čl. 96 do 109, uviđaj – čl. 110 do 112 i veštačenje – čl. 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[96] koje su ostale van domašaja organa za borbu protiv visokotehnološkog kriminala imajući u vidu da su prema zakonskim odredbama primenjive 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 i za krivična 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.

U pogledu usklađenosti domaćeg procesnog zakonodavstva važi isto ono što je rečeno i u pogledu materijalnog dela, tj. ocena je da neke od odredaba

[96] Kontrolisane isporuke, prikriveni islednik i sl.

našeg prava ispunjavaju odredbe Konvencije, dok je neke potrebno razmotriti i izmeniti, a neke u potpunosti nedostaju. Situacija je lošija u pogledu procesnopravnih odredaba imajući u vidu da je aktuelni Zakonik o krivičnom postupku zastareo, da je trebalo da bude zamenjen novim, čija je primena već dva puta odlagana i zasad je potpuno neizvesna. U praksi to znači da je u cilju obezbeđenja i prikupljanja dokaza u vezi sa krivičnim delima visokotehnološkog kriminala potrebno tumačenje i upodobljavanje procesnih mehanizama i radnji koje, niti po intenciji zakonodavca koji ih je propisao, niti po svojoj prirodi i nameni, ne odgovaraju konkretnoj procesnoj situaciji u kojoj se primenjuju.

Mehanizam *hitne zaštite sačuvanih računarskih podataka* predviđen članom 16 Konvencije jeste instrument koji nadležnim organima omogućava zaštitu računarskih podataka kako bi se obezbedilo da računarski podaci ne budu izbrisani ili na drugi način kompromitovani pre nego što se ukaže prilika da budu obezbeđeni za potrebe krivičnog postupka, posebno u pogledu podataka o saobraćaju koji se često automatski obrišu u kratkom periodu. U domaćim pravnim okvirima o primeni ovog mehanizma moglo bi se govoriti kroz primenu odredaba iz čl. 85,[97] 225[98] i 232[99] ZKP.[100] Međutim, pobrojane odredbe pružaju mogućnost samo delimičnog ispunjenja zahteva Konvencije, ali nikako ne predstavljaju potpun osnov za hitnu zaštitu sačuvanih računarskih podataka. Naime, odredba člana 85 odnosi se na pisma, pošiljke i telegrame, koji su materijalni predmeti, dok bi se računarski podaci čija je zaštita hitno potrebna mogli posmatrati samo kroz „druge pošiljke", što je u praksi potpuno nemoguće. Takođe, odredba člana 225 sadrži spisak radnji koje u pretkrivičnom postupku mogu preduzeti organi MUP-a, u kome se ne navode eksplicitno računarski podaci, pri čemu ove radnje preduzimaju sami organi, a intencija ove mere Konvencije jeste da se obavežu davaoci usluga ili lica koja poseduju takve računarske podatke da ih sačuvaju. Mogućnost nadzora i

[97] Reguliše izdavanje naredbe istražnog sudije kojom se poštanska, telegrafska i druga preduzeća, društva i lica registrovana za prenos informacija obavezuju da zadrže i njemu predaju pisma, telegrame i druge pošiljke koje su upućene okrivljenom ili koje on odašilje, ako postoje okolnosti koje ukazuju da ove pošiljke mogu poslužiti kao dokaz u postupku.

[98] Propisuje opšta ovlašćenja MUP-a za preduzimanje radnji na otkrivanju učinilaca krivičnih dela i obezbeđenje tragova i dokaza uzimanjem obaveštenja od građana, pregledom prevoznih sredstava, prostorija građana i preduzeća, ostvarivanjem uvida u dokumentaciju i po potrebi njeno oduzimanje i sl.

[99] Reguliše naredbu istražnog sudije za nadzor i snimanje telefonskih i drugih razgovora ili komunikacija drugim tehničkim sredstvima i optička snimanja lica u vezi sa krivičnim delima protiv ustavnog uređenja i bezbednosti, čovečnosti i međunarodnog prava i sa elementima organizovanog kriminala.

[100] Zakonik o krivičnom postupku.

snimanja telefonskih i drugih komunikacija, propisana članom 232, odnosi se na komunikacije koje se trenutno odvijaju, ali ne pruža mogućnost zaštite određenih podataka koji su stvoreni u prošlosti, pri čemu se čak, kao što je već rečeno, i ne može primenjivati na krivična dela visokotehnološkog kriminala. Zahtevi Konvencije u okviru ove mere koji se odnose na obavezu zaštite celovitosti računarskih podataka u roku ne dužem od 90 dana kao i na obavezu čuvanja tajnosti ovakvog postupka uopšte nisu propisani u našem procesnom zakonodavstvu.

Intencija Konvencije u pogledu sledeće mere predviđene članom 17 *hitne zaštite i delimičnog otkrivanja podataka o saobraćaju* jeste da ona faktički premošćuje razdvojenost naredbe za hitnu zaštitu podataka i obavezu predaje takvih podataka. U domaćem zakonodavstvu odredbe već pomenutog člana 85, kao i čl. 84[101] i 233[102] ZKP mogle bi se identifikovati kao odredbe koje odgovaraju ovoj meri Konvencije. Međutim, pomenute odredbe ne ispunjavaju zahteve Konvencije s obzirom na to da se član 85, kao što je već rečeno, ne odnosi na računarske podatke, dok čl. 84 i 233 regulišu formalne aspekte zaplene spisa, odnosno dostavljanje prikupljenih materijala, ali kao takvi ne mogu predstavljati individualni istražni mehanizam, tj. sami po sebi način obezbeđenja dokaza u krivičnom postupku

Svrha naredne mere *izdavanja naredbe* iz člana 18 Konvencije jeste da se nadležni organi jedne države ovlaste da licima na svojoj teritoriji ili davaocima usluga narede da predaju određene podatke koje poseduju ili kontrolišu, odnosno da predaju podatke o pretplatniku u vezi sa uslugama koje taj davalac usluga poseduje ili kontroliše. Nesporna činjenica je da sva nacionalna zakonodavstva poznaju mere pretresa i zaplene u postupku obezbeđivanja dokaza, ali u pogledu računarskih podataka tradicionalne mere mogu stvoriti niz komplikacija. Sasvim je izvesna situacija da se određeni računarski podaci koji mogu biti dokaz u krivičnom postupku nalaze na serveru, što bi značilo da je primenom tradicionalne metode zaplene potrebno zapleniti ceo server. Upravo zbog toga ova mera predstavlja značajan instrument koji je usmeren ka tačno određenim računarskim podacima i licima koja ih poseduju ili kontrolišu. Domaće procesno pravo poznaje samo već pomenuti član 85 ZKP, koji ne odgovara opisanoj svrsi ove mere s obzirom na to da je, s jedne strane, njegova primena ograničena samo na fizičku komunikaciju i ne pokriva razmenu podataka, dok se, s druge strane, odnosi samo preduzeća i lica

[101] Propisuje da će se privremeno oduzeti spisi, koji mogu poslužiti kao dokaz, popisati i zapečatiti i da njihov sadržaj ne saznaju neovlašćena lica.

[102] Propisuje obavezu dostavljanja materijala prikupljenih primenom odredbe o tajnom nadzoru istražnom sudiji i postupak u vezi s njima ukoliko se primenjuju, odnosno ne primenjuju kao dokaz u krivičnom postupku.

registrovana za prenos informacija, ali ne i na svako lice koje poseduje određene podatke. Odredba našeg zakonodavstva kojom je regulisano privremeno oduzimanje predmeta[103] takođe ne odgovara zahtevima Konvencije s obzirom na to da je ograničena samo na oduzimanje samih predmeta.

Mera *pretraživanja i zaplene sačuvanih računarskih podataka* iz člana 19 Konvencije nadovezuje se na prethodnu meru i svoj razlog postojanja u odredbama Konvencije nalazi u činjenici da nacionalna zakonodavstva često ne pokrivaju procedure pretresa i zaplene u pogledu podataka, već samo, kao što je rečeno, u pogledu predmeta. U našem zakoniku, primenom već pomenutih odredaba, nije sporna mogućnost pretresa i privremenog oduzimanja predmeta u njihovom fizičkom obliku, dakle računara ili servera na kome se nalaze potrebni podaci koji mogu poslužiti kao dokaz, ali ne postoji mogućnost pretresa i oduzimanja u pogledu samih podataka. Ovo može prouzrokovati teškoće u slučajevima kada su određeni podaci zapamćeni na računaru ili serveru zajedno sa milionima drugih podataka iste vrste, koji nisu bitni za postupak i neće poslužiti kao dokaz ali čiji je pregled i analizu, ipak, potrebno izvršiti s obzirom na to da se nalaze na serveru ili računaru koji je oduzet i iz istog razloga više neće biti dostupni imaocu servera ili korisnicima dok se postupak ne završi, ili u situaciji kada državnim organima nije poznata lokacija računara ili servera da bi mogli biti fizički oduzeti, ali im se može pristupiti preko interneta i na taj način pribaviti potrebni dokazi.

Sledeća mera predviđena članom 20 Konvencije *prikupljanje podataka o saobraćaju u realnom vremenu* nije regulisana u našem Zakoniku o krivičnom postupku. Ova mera omogućava nadležnim organima da u realnom vremenu prikupljaju i snimaju podatke o saobraćaju određenih komunikacija prenetih preko računarskog sistema. Korišćenjem interneta, ostaju brojni tragovi kao što je IP[104] adresa, čijim se otkrivanjem i praćenjem može ući u trag učiniocu krivičnog dela. IP adresa je klasična informacija o saobraćaju koja nastaje prilikom korišćenja interneta i bez čijeg je prethodnog otkrivanja nemoguće otkriti identitet učinioca i lokaciju korišćenja internet usluga. Svakako da i u našim uslovima postoji mogućnost otkrivanja IP adrese ali samo u pogledu već ostvarenih internet komunikacija, u čemu, pored državnih organa, najvažniju ulogu igraju i internet servis provajderi preko kojih se ostvaruje konekcija na internet i komunikacija, i koji beleže sve podatke o ostvarenom saobraćaju. Međutim, ova mogućnost ponekad nije dovoljna pogo-

[103] Član 82 ZKP.

[104] Internet protocol adresa – može biti statička i dinamička i svakom internet servis provajderu se dodeljuje određeni opseg IP adresa, što znači da se saznavanjem činjenice o tačnom vremenu vršenja određene radnje i IP adrese može utvrditi kom korisniku je bila dodeljena, ime i prezime korisnika, adresa stanovanja.

tovo ako je potrebno otkriti komunikaciju u vezi sa kojom postoji značajan protek vremena i u vezi sa kojom internet servis provajder više ne poseduje podatke. Stoga je ocenjeno da je potrebna upravo ovakva mera Konvencije koja pruža mogućnost nadležnim organima da nalože prikupljanje podataka o internet saobraćaju u realnom vremenu.

Mera *presretanja podataka iz sadržaja* iz člana 21 Konvencije nadovezuje se na prethodnu meru i takođe daje mogućnost nadležnim organima za postupanje u realnom vremenu kada se za tim ukaže potreba. Ova mogućnost može biti veoma važna kada su nadležnim organima poznati partneri u komunikaciji, ali nemaju podatke o vrsti informacija koje se razmenjuju, čime im se daje mogućnost da snime podatke iz komunikacije, što može uključivati dokumente ili informacije preuzete sa internet stranica, poslatu ili primljenu elektronsku poštu i sl. U našim uslovima pomenuti član 85 ZKP pruža mogućnost pribavljanja podataka o elektronskoj pošti ali samo u vezi sa podacima iz prošlosti, dok takođe pomenuti član 232 ZKP, koji je ostao van domašaja primene za krivična dela visokotehnološkog kriminala, pruža mogućnost nadzora nad komunikacijama, pri čemu nije jasno da li izraz komunikacija pokriva samo govornu komunikaciju ili i komunikaciju podataka i ne predviđa eksplicitno mogućnost presretanja u realnom vremenu.

Mere sadržane u Konvenciji, po mišljenju međunarodne zajednice, predstavljaju, kao što je već rečeno, neophodan minimum standarda koje je potrebno ispuniti da bi se obezbedili preduslovi za uspešno suzbijanje visokotehnološkog kriminala i koje bi kao takve trebalo da budu implementirane u nacionalna zakonodavna rešenja, ali ujedno svakoj strani ugovornici, tj. državi koja je potpisala i ratifikovala Konvenciju ostavlja se mogućnost stavljanja rezerve na primenu određenih mera posebno onih koje se odnose na prikupljanje podataka o saobraćaju u realnom vremenu i presretanje podataka iz sadržaja. Svrha stavljanja rezerve jeste da se omogući stranama ugovornicama da uspostavljanje, sprovođenje i primena ovlašćenja iz Konvencije podležu uslovima i ograničenjima predviđenim domaćim zakonodavstvom koje treba da omogući odgovarajuću zaštitu ljudskih prava i sloboda u skladu sa preuzetim međunarodnim obavezama.

Iz svega iznetog može se zaključiti da je revizija našeg procesnog zakonodavstva neophodna. Aktuelni Zakonik o krivičnom postupku je definitivno zastareo i prevaziđen u mogućnostima koje pruža, a ta činjenica je od krucijalne važnosti s obzirom na to da upravo taj zakonik predstavlja okvir kojim su propisana ovlašćenja a samim tim i ograničenja nadležnim državnim organima u postupku otkrivanja učinilaca krivičnih dela i prikupljanja dokaza. Svakako da je Zakonik u pogledu mehanizama koje predviđa odgovarao duhu vremena kada je načinjen, međutim, novi pojavni oblici kriminala kao što su

organizovani ili visokotehnološki kriminal zahtevaju i nove mehanizme ukoliko želimo da govorimo o uspešnoj borbi protiv njih. Akti međunarodne zajednice kao što je Konvencija o sajber kriminalu predstavljaju izraz razumevanja opasnosti koje sa sobom nose novi oblici kriminala i shvatanja potrebe ustanovljavanja novih mehanizama koji će biti stavljeni na raspolaganje državnim organima. U našim uslovima, međutim, pored neadekvatne zakonodavne regulative, problem je upravo i nerazumevanje opasnosti i posledica koje nastaju izvršenjem krivičnih dela visokotehnološkog kriminala. Upravo ovi nedostaci dovode do potrebe za raznovrsnim tumačenjima nenamenskih zakonskih odredaba zajedno sa prebacivanjem te odgovornosti na konkretne državne organe ili sudove i pojedince u okviru njih, uz realnu opasnost da sud u svojoj presudi, ili viši sud postupajući po žalbi na takvu presudu, ne deli mišljenje o prezentovanom tumačenju, što predstavlja probleme koji postoje u svim oblastima prava, pa i u borbi protiv visokotehnološkog kriminala, a koji nikako ne doprinose stvaranju preduslova za efikasno sprovođenje zakona i ostvarivanje svrhe prava i njegove zaštitne funkcije.

1.1.1. Krivična dela protiv računara i računarskih sistema

U skladu sa potrebom prilagođavanja našeg društva promenama koje se dešavaju u savremenom svetu, razvoju informatičkih tehnologija i njihovom prodoru u sve segmente svakodnevnog života, kao i zaštiti od opasnosti koje mogu nastati njihovom zloupotrebom, u domaće zakonodavstvo uvođeni su propisi kojima su sankcionisana krivična dela iz oblasti sajber kriminala. Krivična dela iz ove oblasti prvi put su bila definisana Izmenama Krivičnog zakona Republike Srbije iz 2003. godine, u glavi XVI, kao i Krivičnim zakonikom Savezne Republike Jugoslavije, odnosno Osnovnim krivičnim zakonikom. Novi Krivični zakonik, koji je stupio na snagu u januaru 2006. godine, preuzeo je dotadašnja rešenja iz ove oblasti ali je i propisao jedno novo krivično delo – *Neovlašćeno korišćenje računara ili računarske mreže,* član 304.

Donošenjem Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Službeni glasnik RS“, br. 61/05, 18. jul 2005. god.) uspostavljen je pravnoinstitucionalni okvir za postupanje pravosudnih i policijskih organa u ovoj oblasti, a pojam visokotehnološkog kriminala definisan je kao 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. Iako po svojoj prirodi i načinu izvršenja spadaju u visokotehnološki kriminal, navedenim zakonom nije predviđeno postupanje ovih državnih organa u predmetima pedofilije na internetu i zloupotrebe platnih kartica, već je procesui-

ranje učinilaca navedenih krivičnih dela ostavljeno u nadležnost opštinskim sudovima. Budući da se nadležnost Posebnog tužilaštva odnosi na teritoriju Srbije, ustanovljena je praksa da policijsko Odeljenje za borbu protiv visokotehnološkog kriminala Službe za borbu protiv organizovanog kriminala i tužilaštvo obavljaju celokupan pretkrivični postupak i za ova krivična dela, a da se krivični postupak odvija pred mesno nadležnim opštinskim sudovima.

Iako nije u potpunosti usaglašen sa Konvencijom Saveta Evrope o visokotehnološkom kriminalu iz 2001. godine, koju je srpski parlament ratifikovao u aprilu 2009. godine, može se zaključiti da Krivični zakonik i Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala obezbeđuju pravni okvir za postupanje državnih organa u krivičnopravnim stvarima koje se odnose na visokotehnološki kriminal.

Krivični zakonik u glavi 27. inkriminiše krivična dela protiv bezbednosti računarskih podataka, i to: član 298 – *Oštećenje računarskih podataka i programa,* član 299 – *Računarska sabotaža,* član 300 **–** *Pravljenje i unošenje računarskih virusa,* član 301 – *Računarska prevara,* član 302 – *Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka,* član 303 – *Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži* i član 304 – *Neovlašćeno korišćenje računara ili računarske mreže.*

U ovom tekstu biće reči i o krivičnim delima za čije procesuiranje nije nadležno Tužilaštvo za borbu protiv visokotehnološkog kriminala, koja takođe spadaju u ovaj vid kriminala, a to su: krivično delo *Prikazivanje pornografskog materijala i iskorišćavanje dece za pornografiju* – član 185 KZ, koje spada u krivična dela protiv polne slobode iz glave 18. Krivičnog zakonika, kao i krivično delo *Falsifikovanje i zloupotreba platnih kartica* – član 225 KZ, koje spada u krivična dela protiv privrede.

Pomenućemo i krivično delom *Prevara* – član 208 KZ iz glave 21. Krivičnog zakonika, kojim su propisana krivična dela protiv imovine, kao i različiti vidovi prevarnih aktivnosti – nigerijsko pismo, lažni internet sajtovi, fišing (engl. *phishing*).

Zakonikom su propisana i krivična dela za koja se gonjenje preduzima po privatnoj tužbi, a koja se takođe mogu izvršiti putem računara i računarskih mreža kao što su *Uvreda, Kleveta, Iznošenje ličnih ili porodičnih prilika*.

Izvršioce krivičnih dela iz oblasti visokotehnološkog kriminala često nazivamo hakerima. Iako se termini hak (engl. *hack*) i haker često upotrebljavaju u negativnom smislu i dovode u vezu sa zloupotrebom informacionih tehnologija, pogrešno je izjednačavati sve hakere sa kriminalcima. Neretko, hakeri izvršavaju napade kako bi otkrili slabosti određenih zaštitnih informacionih sistema, koji ma koliko bili usavršavani, uvek imaju slabe tačke i upravo

hakerima dugujemo zahvalnost za neke od najznačajnijih softverskih aplikacija. Ova grupa se naziva etičkim hakerima i oni koriste sva sredstava kao i potencijalni napadači ali, za razliku od njih, ne oštećuju sisteme, nego pronalaze propuste u sistemima zaštite, procenjuju sigurnost sistema i podižu sigurnost na viši nivo.

Jedna od najpoznatijih hakerskih aktivnosti je rušenje veb sajtova, što uglavnom ne ostavlja teže posledice, već više predstavlja zabavu ili čin dokazivanja. Osim toga, hakerski napadi se mogu sastojati i u upadu u zaštićene informacione sisteme, ali i u krađi novca zloupotrebom pribavljenih podataka o kreditnim i platnim karticama ili industrijskoj špijunaži.

Haker je osoba koja dobro poznaje računare i istražuje njihove mogućnosti, konstantno prikuplja i usavršava znanja, upotrebljava informacione tehnologije na kreativan način.[105]

Hakere bismo prema načinu delovanja mogli da podelimo na dobre i loše. *Krekeri* (engl. *crackers*) koriste znanja iz kriminalnih pobuda i težnje za materijalnim bogaćenjem, upadaju u informacione sisteme i kradu različite vrste informacija, najčešće podatke o platnim i kreditnim karticama, a takođe se bave uklanjanjem zaštite od kopiranja sa legalnog softvera.[106] Delovanje *frakera* (engl. *phreakers*) usmereno je na telekomunikacione sisteme i izbegavanje plaćanja telefonskih računa.[107] Posebna grupa hakera je posvećena isključivo stvaranju računarskih virusa, a postoje i hakeri koji su specijalizovani za upade u zaštićene sisteme.

Kao što vidimo, delovanje hakera može biti veoma različito, od relativno bezopasnog poput rušenja veb sajtova, preko krađa novca ili ličnih podataka, do špijunskih aktivnosti i sabotaža, o čemu će biti reči u nastavku teksta.

Usled konstantnog razvoja informacionih tehnologija, računarskih mreža i sve bržeg protoka elektronskih informacija, otvaraju se mogućnosti za vršenje novih, do sada neinkriminisanih oblika kriminalnih aktivnosti upotrebom računarske tehnologije, zbog čega je neophodna stalna edukacija pripadnika državnih organa koji se bore protiv visokotehnološkog kriminala. Neophodno je da zakonodavna aktivnost države na ovom polju bude što intenzivnija, kako bi ažuriranjem propisa bili obuhvaćeni svi novi vidovi visokotehnološkog kriminala i u što većoj meri suzbijena ovakva štetna aktivnost i eliminisane njene posledice.

[105] „Hacker“, Wikipedia, internet, *http://en.wikipedia.org/wiki/Hacker,* 7. 5. 2009.

[106] „Software cracking“, Wikipedia, internet, *http://en.wikipedia.org/wiki/Software_cracking,* 7. 5. 2009.

[107] „Phreaking“, Wikipedia, internet, *http://en.wikipedia.org/wiki/Phreaking,* 7. 5. 2009.

Oštećenje računarskih podataka i programa – član 298 Krivičnog zakonika

Ovo krivično delo se sastoji u neovlašćenom brisanju, menjanju, oštećenju, prikrivanju računarskog podatka ili činjenju neupotrebljivim istog podatka na drugi način, a zaprećena je novčana kazna ili zatvor do jedne godine. Kvalifikovani oblici ovog dela predviđeni su st. 2 i 3 kada šteta prouzrokovana opisanim krivičnim delom prelazi iznos od četiristo pedeset hiljada dinara, odnosno milion petsto hiljada dinara, a zaprećene su kazne zatvora od tri meseca do tri godine, odnosno zatvor od tri meseca do pet godina.

Krivični zakonik u članu 112, tačka 17 definiše pojam računarskog podatka kao predstavljenu informaciju, znanje, činjenicu, koncept ili naredbu koja se unosi, obrađuje ili pamti, ili je uneta, obrađena ili zapamćena u u računaru ili računarskoj mreži, dok računarski program u članu 112, tačka 19 određuje kao uređeni skup naredbi koje služe za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara. Namera zakonodavca je da propisivanjem ovog krivičnog dela zaštiti integritet računarskih podataka od neovlašćenih delovanja.

Krivično delo se može izvršiti na više načina: (1) brisanjem ili (2) izmenom, tako da se računarski program ili podatak potpuno uništava ili menja da postaje neupotrebljiv za dalje izvršavanje namenjene funkcije, (3) oštećenjem, čime se program ili podatak delimično uništava i smanjuje njegova upotrebna vrednost, (4) prikrivanjem, kada dolazi do sklanjanja računarskog programa ili podatka, a delo može biti izvršeno i na bilo koji drugi način kojim se program čini neupotrebljiv za njegovu namenu.[108]

Posledica ovog krivičnog dela je činjenje neupotrebljivim programa ili podatka. Delo je svršeno preduzimanjem bilo koje od navedenih radnji uz ostvarenje ove posledice. Ukoliko je više radnji preduzeto prema jednom objektu, odnosno računarskom podatku ili programu ostvaruje se biće samo jednog krivičnog dela. Izvršilac ovog krivičnog dela može biti svako lice, a u pogledu vinosti potreban je umišljaj.[109]

Za pravilnu kvalifikaciju ovog krivičnog dela neophodno je utvrditi da li je izvršilac postupao neovlašćeno, tačno vreme i mesto izvršenja krivičnog dela, način na koji je delo izvršeno – da li je u pitanju fizički pristup računarskom programu ili podatku, ili je delo izvršeno u okviru računarske mreže internog karaktera ili putem interneta, te ukoliko je izvršeno putem drugog

[108] Ljubiša Lazarević, *Komentar Krivičnog zakonika Republike Srbije,* Savremena administracija, Beograd, 2006, str. 745.

[109] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 115.

računara uz pomoć kog programa, kao i posledice koje su nastale, odnosno da li je objekat dela učinjen neupotrebljivim. Potrebno je utvrditi i svojstvo učinioca krivičnog dela, odnosno da li je reč o službenom ili odgovornom licu u okviru nekog pravnog lica, ili o licu koje je bilo, na osnovu nekog pravom regulisanog odnosa, ovlašćeno da na bilo koji utvrđen način manipuliše računarskim programom ili podatkom, da ga ažurira ili menja.[110] Kako bi činjenično stanje bilo potpuno utvrđeno, neophodno je identifikovati i koju je opremu upotrebio učinilac prilikom izvršenja krivičnog dela i kome ona pripada, s obzirom na to da je stavom 4 člana 298 Krivičnog zakonika predviđeno obavezno oduzimanje uređaja i sredstva kojima je učinjeno krivično delo iz st. 1 i 2 ovog člana, ako su u svojini učinioca.

Prikupljanje validnih dokaza u pojedinačnim slučajevima često je veoma otežano. Jedan od osnovnih principa u prikupljanju digitalno forenzičkog materijala jeste da posle izvršenog krivičnog dela ne treba ništa menjati, što se u praksi veoma retko dešava. Podaci, datoteke i programi koji su objekat izvršenja ovog krivičnog dela služe oštećenima za svakodnevno poslovanje, knjigovodstvenu evidenciju, održavanje poslovnih kontakata ili su u njima sadržani lični podaci koji imaju samo afekcionu vrednost. Oštećeni najčešće sami pokušavaju da otklone štetu koja im je naneta ili angažuju lica koja imaju veći ili manji fond znanja iz informacionih tehnologija, kako bi povratili izbrisane podatke. Ovakvim delovanjem se gotovo uvek uništavaju neposredni dokazi koji bi mogli dovesti do izvršioca, a tužiocu na raspolaganju ostaju samo posredni dokazi, koji uglavnom nisu dovoljni kako bi izvršilac bio otkriven i osuđen.

Potrebno je razmotriti još jedno pitanje koje proističe iz same prirode funkcionisanja računara i procesa zapisivanja i brisanja podataka sa hard diska. Poznato je da se računarski podaci uobičajenim načinom brisanja – smeštanjem fajla u „kantu za đubre“ (engl. *recycle bin*) i davanjem komande za njeno „pražnjenje“ fizički ne brišu sa hard diska. Za trajno i nepovratno brisanje podataka potrebno je upotrebiti neki od vajper (engl. *whipe*) programa, koji vrše „prepisivanje“ hard diska. Razvojem digitalne forenzike nastaju sve savršeniji programi za povraćaj (engl. *recovery*) podataka, koji su u stanju da izvrše povraćaj podataka čak i posle više „prepisivanja“ hard diska. Smatramo da je za postojanje krivičnog dela *Oštećenje računarskih podataka i programa* dovoljno sprovesti uobičajen način brisanja podataka, a da kasniji po-

[110] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 116.

vraćaj podataka ne može biti tretiran kao okolnost koja eliminiše postojanje krivičnog dela.

Najčešći vid izvršenja ovog krivičnog dela predstavlja rušenje veb sajtova, što je svakodnevna aktivnost hakerskih grupa. Prema nepisanim hakerskim pravilima, objekat napada je samo deo sajta, najčešće naslovna strana, koja biva promenjena tako da se na njoj ostavi hakerski „potpis" grupe, poruka ili pozdrav. Jedan od najbizarnijih slučajeva desio se tokom 2008. godine, kada su i dalje nepoznati počinioci na forum sajta jedne beogradske osnovne škole postavili više pornografskih slika i video-klipova. Od napada sa interneta nisu bili zaštićeni ni sajtovi ministarstava odbrane, poljoprivrede, parlamenta, pa čak ni Srpske pravoslavne crkve, s tim što nijedan od ovakvih napada nije prouzrokovao direktnu materijalnu štetu. Izvršenju ovakvih krivičnih dela pogoduje činjenica da svest o opasnostima koje mogu doći sa interneta još nije dovoljno razvijena, kao i slaba zaštita veb sajtova. Napadi na sajtove se odvijaju kontinuirano, ali do očiju javnosti dolaze samo oni napadi koji su bili uspešni. Izvršioce je veoma teško otkriti jer oni koriste alate za skrivanje koji onemogućavaju utvrđivanje mesta sa koga je napad došao, odnosno identifikovanje prave IP adrese koju je izvršilac koristio u vreme izvršenja krivičnog dela.

Posebno treba biti oprezan kada se na ovaj način ostavljaju poruke rasističke prirode ili se predstavljaju sadržaji usmereni na izazivanje i raspirivanje nacionalne ili verske mržnje ili netrpeljivosti, što bi eventualno moglo biti kvalifikovano kao krivično delo protiv ustavnog uređenja i bezbednosti Srbije. Takođe je moguće ostaviti i razne uvredljive poruke ili izneti nečije lične podatke, čime bi moglo biti izvršeno neko iz grupe krivičnih dela protiv časti i ugleda, propisanih u glavi 17. Krivičnog zakonika.

Krivična dela *Oštećenje računarskih podataka i programa* i *Računarska sabotaža* slična su prema načinu izvršenja i posledicama koje mogu ostaviti, zbog čega tužilac mora biti veoma oprezan prilikom pravne kvalifikacije utvrđenog činjeničnog stanja. U zavisnosti od svakog pojedinačnog slučaja, mora se ceniti umišljaj izvršioca krivičnog dela, značaj izbrisanih ili oštećenih podataka za poslovanje i funkcionisanje oštećenog, ali i sve druge okolnosti, kako bi određena protivpravna radnja bila kvalifikovana kao oštećenje podataka ili računarska sabotaža. Razvoj globalne računarske mreže doveo je do toga da se sve veći broj kompanija orijentiše na elektronsko poslovanje. Postoje privredni subjekti koji posluju isključivo elektronski i sa klijentima kontaktiraju koristeći internet (npr. *E-bay*). Napad ili rušenje veb sajtova ovakvih kompanija mogao bi biti kvalifikovan kao računarska sabotaža.

Ta krivična dela se razlikuju i prema težini posledica koje su prouzrokovane. Dok se posledice krivičnog dela *Oštećenje računarskih podataka i pro-*

grama uglavnom lako otklanjaju, dotle su posledice *Računarske sabotaže* mnogo teže i o njima ćemo više govoriti u analizi ovog krivičnog dela.

O važnosti pravilnog obezbeđivanja dokaza nakon izvršenog krivičnog dela, nužnosti zaštite podataka koje koriste privredni subjekti ali i ograničavanja prava njihovom pristupu, govori nam primer jednog pretkrivičnog postupka koji je Tužilaštvo za borbu protiv visokotehnološkog kriminala vodilo tokom 2007. godine. Protiv osumnjičene B. A. iz Subotice bila je podneta krivična prijava zbog osnovane sumnje da je tokom 2007. godine izvršila krivično delo *Oštećenje računarskih podataka i programa* – član 298 Krivičnog zakonika, na štetu svog preduzeća, i to tako što je kao stalno zaposleni administrativni radnik izbrisala foldere i fajlove koji se odnose na ulazne i izlazne fakture i koji predstavljaju osnovnu dokumentaciju značajnu za poslovanje preduzeća, kao i fajlove sa podacima o poslovnim partnerima oštećenog. Nakon saslušanja osumnjičene, zaposlenih u preduzeću i prikupljanja svih drugih potrebnih dokaza nije bilo moguće utvrditi njenu krivicu. Osumnjičena je negirala da je obrisala podatke, nije bilo svedoka koji bi tako nešto potvrdili, a ispostavilo se da računari oštećenog preduzeća nisu bili zaštićeni pristupnom šifrom i da je svako od zaposlenih mogao pristupiti računaru osumnjičene. Iako su posredi bili veoma značajni podaci za funkcionisanje preduzeća, ovo brisanje nije imalo većih štetnih posledica po poslovanje privrednog subjekta jer je oštećeno preduzeće u ovlašćenom servisu računarske opreme već sledećeg dana izvršilo povraćaj obrisanih podataka. Kako je povraćaj podataka bio izvršen pre podnošenja krivične prijave i obaveštavanja nadležnih državnih organa, svi validni dokazi su bili trajno uništeni, zbog čega nije bilo moguće povesti krivični postupak, pa je krivična prijava odbačena.

Računarska sabotaža – član 299 Krivičnog zakonika

Krivično delo se sastoji u unošenju, uništavanju, brisanju, izmeni, oštećenju ili činjenju neupotrebljivim računarskog podatka ili programa na drugi način, odnosno uništavanju ili oštećenju računara ili drugog uređaja za elektronsku obradu i prenos podataka sa namerom da se onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su značajni za državne organe, javne službe, ustanove, preduzeća ili druge subjekte. Procesuiranje ovog krivičnog dela i njegovih izvršilaca odvija se prema pravilima redovnog postupka, a zaprećena je kazna zatvora od šest meseci do pet godina.

Smatramo da je zaprećena kazna suviše blaga, odnosno da zakonodavac nije uzeo u obzir težinu posledica koje mogu nastati izvršenjem krivičnog

dela *Računarska sabotaža,* zbog čega je potrebno propisati veći minimum i maksimum kazne.

Namera zakonodavca je da propisivanjem ovog krivičnog dela zaštiti računare i druge uređaje namenjene elektronskoj obradi i prenosu podataka koji su od posebnog značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte. Ovo krivično delo neće postojati ukoliko je izvršeno prema drugim računarima, odnosno onim računarima koji nisu značajni za navedene subjekte, što znači da u svakom konkretnom slučaju treba utvrditi da li je reč o računarima ovog značaja.[111]

Kao što smo već napomenuli, ovo krivično delo je prema radnji veoma slično krivičnom delu *Oštećenje računarskih podataka i programa,* ali se kod *Računarske sabotaže* pojavljuje i unošenje podataka, kao poseban oblik izvršenja kojim se u računar unosi podatak, a posledica toga je činjenje neupotrebljivim računarskog programa ili podataka, odnosno uništenje ili oštećenje računara.

Izvršilac ovog krivičnog dela može biti svako lice, a u pogledu vinosti potreban je umišljaj. Bitno obeležje ovog krivičnog dela jeste namera učinioca da preduzimanjem radnji onemogući ili omete postupak elektronske obrade ili prenosa podataka značajnih za pomenute subjekte, te je ovu nameru potrebno utvrditi i dokazati, odnosno navedena posledica ne može nastati kao rezultat samo slučaja ili nepažnje.

Za ispravno kvalifikovanje ovog krivičnog dela neophodno je utvrditi svojstvo učinioca kao i njegov umišljaj. Potrebno je tačno utvrditi vreme i mesto izvršenja krivičnog dela, način na koji je delo izvršeno – da li je u pitanju fizički pristup računarskom programu ili podatku, ili je delo izvršeno u okviru računarske mreže internog karaktera ili putem interneta, te ukoliko je izvršeno putem drugog računara, uz pomoć kog programa. Konačno, potrebno je utvrditi da li je nastupila posledica – uništenje ili oštećenje računarskih podataka ili programa preduzimanjem neke od inkriminisanih radnji, a ukoliko posledica nije nastupila, neophodno je utvrditi sve napred navedeno radi kasnijeg procesuiranja s obzirom na to da je pokušaj izvršenja ovog krivičnog dela kažnjiv.[112]

Napadi na veb sajtove državnih organa, institucija i privatnih preduzeća, kao i krađa podataka značajnih za rad navedenih subjekata, najčešće su bili predmet do sada vođenih postupaka za krivična dela *Oštećenje računarskih*

[111] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 117.

[112] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 118.

podataka i programa i *Računarska sabotaža.* Običnim obaranjem veb sajta ne dolazi do prodora u računarske sisteme i njihovog oštećenja, a funkcionisanje napadnutih veb stranica bilo bi uspostavljano posle nekoliko sati. Posledice sabotaže bi bile teže i mogle bi se sastojati u onemogućavanju ili znatnom otežavanju funkcionisanja oštećenog subjekta za duži period, poslovnim gubicima i nanošenju velike materijalne štete.

Zajednička karakteristika gotovo svih izvršenih krivičnih dela bila je slaba zaštita računara, računarskih podataka i veb sajtova. Profil izvršilaca kao i motivi za izvršenje krivičnih dela veoma su različiti, od radnika koji su nezadovoljni uslovima rada i visinom primanja, okrivljenih koji su to shvatali kao dobru zabavu, do onih koji su bili politički motivisani. Iako do sada nije vođeno mnogo krivičnih postupaka, izvesno je da su ova krivična dela u stvarnosti veoma česta, ali da oštećeni zbog neobaveštenosti ili neznanja ne prijavljuju njihovo izvršenje.

U uporednom pravu je ustaljena praksa da se izvršiocima izriču veoma stroge kazne čak i za pokušaj sabotaže. O tome nam govori primer da je početkom 2008. godine u američkoj državi Njujork osuđen na 30 meseci zatvora programer zaposlen u preduzeću „Medco Health Solutions" zbog podmetanja „logičke bombe" u računarski sistem kompanije, što je moglo da dovede do obaranja i oštećenja više od 70 servera koji su sadržali informacije kao što su podaci o izdatim receptima, medicinski podaci, finansijski izveštaji, platni spiskovi itd.[113] Do brisanja navedenih podataka nije došlo jer su zaposleni na vreme otkrili zlonamerni kod.[114]

O tome da se posledice računarske sabotaže teško otklanjaju govori nam i primer spočetka februara 2000. godine, kada došlo je do velikog napada na sajtove kompanija koje svoje poslovanje baziraju isključivo na globalnoj računarskoj mreži – buy.com, ebay.com, zdnet.com, etrade.com, amazon.com i yahoo.com. Sajtovi nisu radili svega nekoliko sati, a šteta koja je načinjena ovim napadom bila je ogromna. Samo jedna od kompanija čiji se sajt našao na udaru – eBay imala je pad akcija od 26 odsto i gubitak od pet miliona u naredna tri meseca.[115]

Da ni najveće svetske informatičke kompanije nisu pošteđene ovih krivičnih dela govori primer kompanije Intel čiji su proizvodni pogoni tokom 1997. godine prestali da rade, kada je jedan otpušteni radnik izbrisao veliki

[113] „Optužen podmetač logičke bombe", Mikro-PC World, internet, *http://www.mikro.rs/main/index.php?q=vestiarhiva&godina=&mesec=&ID=8749*, 7. 5. 2009.

[114] „Man gets record sentence for computer sabotage", ZDNet News & Blogs, internet, *http://news.zdnet.com/2100-1009_22-182571.html ,* 7. 5. 2009.

[115] Boban Aćimović, „Žestok DoS napad na pet gigantskih sajtova", Linux.rs, internet, *http://www.linux.rs/content/view/112/20/,* 7. 5. 2009.

broj datoteka značajnih za funkcionisanje proizvodnih linija. Navedeni radnik je upravljao automatizovanim sistemom za proizvodnju „Workstream", a po dobijanju otkaza opozvana mu je lozinka i oduzet mu je računar. Sledećeg dana radnik je iskoristio činjenicu da je mogao da se prijavi na proizvodni sistem kompanije i sa svog kućnog računara, što je iskoristio da izbriše podatke. Posledica tog čina je bilo znatno usporavanje procesa proizvodnje, a iznos prouzrokovane štete bio je 20.000 dolara.[116]

Ignorisanje problema bezbednosti na internetu može dovesti do teških posledica po poslovanje i šteta koje je nemoguće proceniti. Napadi i oštećenja informacionih sistema centralne banke, kao i drugih finansijskih subjekata, odnosno institucija koje čuvaju lične podatke građana mogli bi prouzrokovati nesagledive posledice. Velikih napada i oštećenja računarskih sistema važnijih državnih institucija do sada nije bilo, ali sve veća prisutnost interneta, kao i opasnosti koje zloupotrebe globalne mreže mogu doneti, nameću potrebu za velikom opreznošću.

Većina privrednih subjekata u Srbiji izdvaja malo sredstava za održavanje informacionih sistema, nema stručnjake koji bi te sisteme održavali i kontrolisali dolazni i odlazni internet saobraćaj. Mali broj privrednih subjekata se pridržava osnovnih bezbednosnih pravila prilikom upotrebe interneta u poslovanju. Kako bi broj izvršenja ovakvih krivičnih dela bio smanjen, neophodno je da državni organi, institucije i privredni subjekti obezbede dobar sistem zaštite informacionih sistema koje koriste, adekvatan nadzor nad internet saobraćajem, da konstantno edukuju zaposlene i da ograniče pristup zaštićenim računarima i poverljivim podacima.

Poznato je da će Vlada Republike Srbije do kraja juna 2009. godine početi sa vođenjem elektronskih sednica, kao i da će se nastaviti proces elektronskog umrežavanja svih opština u Srbiji u okviru projekta elektronske državne uprave. Planirano je uvođenje „E-servisa" za potrebe građana i privrednih subjekata, i to kako na nivou organa centralne vlasti, tako i na nivou organa lokalne samouprave. Pod ovim servisima se podrazumevaju najrazličitije javne usluge, od pitanja koja se tiču ličnog statusa građana, prebivališta i državljanstva, preko servisa vezanih za izdavanje određenih vrsta dozvola, do prijavljivanja poreza i dr. (strategija reforme državne uprave, novembar 2004). Uvođenje informacionih tehnologija u državnu upravu, kao i potpuni prelazak državne uprave na elektronski režim rada, predstavlja veliki izazov, značajno unapređuje rad državnih organa, smanjuje troškove i poboljšava kvalitet života građana i stvara nove mogućnosti da oni utiču na javni život. Zbog

[116] „Bivši radnik Intela priznao računarsku prevaru", Mikro-PC World, internet, *http://www.mikro.rs/main/index.php?q=vestiarhiva&godina=&mesec=&ID=998, 7. 5. 2009.*

toga je veoma značajno da informacioni sistemi državnih organa budu adekvatno zaštićeni, a državni službenici dobro obučeni, jer oštećenje ili uništavanje podataka sadržanih u tim sistemima može imati teške posledice po bezbednost, ekonomiju i život građana.

Pravljenje i unošenje računarskih virusa
– član 300 Krivičnog zakonika

Krivično delo *Pravljenje i unošenje računarskih virusa* ima dva oblika:

1. pravljenje računarskog virusa s namerom njegovog unošenja u tuđ računar ili računarsku mrežu, za šta je propisana novčana kazna ili zatvor do šest meseci;

2. unošenje virusa u tuđ računar ili računarsku mrežu i prouzrokovanje štete na takav način, za šta je propisana novčana kazna ili zatvor do tri meseca.

Krivični zakonik u članu 112, stav 3, tačka 20 definiše računarski virus kao 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.

Za uspešno vođenje krivičnog postupka protiv izvršilaca krivičnog dela neophodno je pribaviti sledeće dokaze: 1) utvrditi vreme i mesto izvršenja krivičnog dela, 2) pribaviti računarski virus, oduzeti alate i uređaje pomoću kojih je virus napravljen, 3) ustanoviti način na koji je računarski virus unet u tuđ računar ili mrežu, odnosno da li je virus unet fizički u određeni računar ili mrežu direktnim pristupom tom računaru ili mreži, ili je to učinjeno u okviru mreže internog karaktera uz pomoć drugog računara kao dela mreže ili putem interneta, 4) utvrditi nastupanje štete.[117]

Prvi računarski virus „Elk Cloner“, pojavio se u julu 1982. godine, napadao je računare Apple II, a širio se tako što se „kačio“ za igricu napisanu za te računare i preko disketa prelazio sa sistema na sistem. Autor virusa je bio srednjoškolac iz američkog grada Pitsburga, a igra je bila podešena tako da se može igrati 49 puta, nakon čega bi došlo do pokretanja virusa koji bi na monitoru ispisivao stihove iz pesme čiji je autor bio pomenuti srednjoškolac.[118]

Sredinom osamdesetih godina dvadesetog veka dolazi do pojave personalnih računara i započinje njihova široka upotreba. Uspostavljaju se prve

[117] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala,* Savet Evrope, 2008, str. 120.

[118] G. B., „Računarski virusi slave 25. rođendan“, Mikro-PC World, internet, *http://www.mikro.rs/main/index.php?q=vest&ID=9520#povezanevesti*, 7. 5. 2009.

računarske mreže, što je stvorilo povoljnu klimu za sve češće i razornije delovanje računarskih virusa. Kada je posle 1990. godine operativni sistem Windows kompanije Microsoft postao dominantan, došlo do pojave tzv. makrovirusa koji su se širili kroz Office Word i Excel fajlove.[119]

Računarski virusi su postali sastavni deo savremenog života, a svakodnevno nastaje na desetine novih virusa. Budući da je danas najveći broj kompjutera povezan na internet ili u lokalne mreže, virusi se veoma lako šire globalnom računarskom mrežom, elektronskom poštom, programima za razmenu poruka (npr. *windows live messenger*) i sistemima za deljenje podataka (*file sharing systems*). Virusi se prenose putem flopi diskova, optičkih diskova, eksternih memorijskih jedinica, s tim što je internet postao njihov glavni izvor. Virusi se mogu preneti i samom posetom određenim veb sajtovima ili preuzimanjem sadržaja sa interneta. Kriju se iza naizgled običnih fajlova – tekstualnih dokumenata, elektronskih čestitki, tabela, fotografija, audio ili video-klipova, a njihovi tvorci im često daju bezazlene nazive (npr. I love you, Melissa, newfolder.exe), što znatno doprinosi njihovom širenju. Do prve „globalne epidemije" došlo je 1999. godine, kada se virus „Melissa" širio kao datoteka priložena uz elektronsku poštu, i samo u Severnoj Americi zarazio više od milion računara.[120]

Kompjuterski virusi su mali programi napravljeni tako da se bez znanja vlasnika računara kopiraju na druge računare i ometaju njihovo normalno funkcionisanje. Virus se obično „kači" na pokretački fajl (npr. setup.exe ili file.com) ili na but (engl. *boot*) sektor hard diska, koji sadrži osnovne naredbe koje se izvršavaju prilikom pokretanja rada računara.[121] Ne postoji nijedna vrsta računara ili operativnog sistema koja je imuna na viruse. Najrašireniji su oni virusi koji napadaju Windows operativne sisteme i personalne (PC) računare, s obzirom na to da je navedeni operativni sistem najzastupljeniji, ali postoje i virusi namenjeni Machintosh Apple računarima ili koji deluju u LINUX ili DOS okruženju. Osim računara, i drugi uređaji poput mobilnih telefona i drugih digitalnih uređaja koji imaju pristup internetu mogu biti meta delovanja virusa. Štetne posledice koje ostavljaju ovi virusi mogu se ogledati u poteškoćama tokom privatne i poslovne komunikacije, nekontrolisanog

[119] „Computer virus", Wikipedia, internet, *http://en.wikipedia.org/wiki/Computer_virus,* 7. 5. 2009.

[120] G. B., „Računarski virusi slave 25. rođendan", Mikro-PC World, internet, *http://www.mikro.rs/main/index.php?q=vest&datum=2007-07-17&ID=9520,* 7. 5. 2009.

[121] „Computer virus", Encyclopedia.com, internet, *http://www.encyclopedia.com/topic/computer_virus.aspx,* 7. 5. 2009.

slanja privatnih podataka korisnika, poput imenika ili šifara kreditnih kartica i bankovnih računa.[122]

Prosečan korisnik često i neće primetiti da mu je kompjuter zaražen, a neki od znakova mogu biti usporen rad računara, prekidi internet konekcije ili iznenadni padovi sistema. Posledice delovanja računarskih virusa veoma su različite. Neki virusi gotovo da i ne ometaju rad računara, a neki imaju komične efekte koji se sastoje u iznenadnom puštanju audio i video-klipova, npr. „kaljinka virus". Mogu prouzrokovati manje štetne posledice kao što su zamena komandi levog i desnog klika na mišu, neplanirano gašenje računara, ali i pričiniti veliku štetu u vidu trajnog brisanja podataka, onesposobljavanja operativnog sistema računara ili oštećenja hardvera.

Postoje brojne podele računarskih virusa i njihova klasifikacija se vrši prema različitim kriterijumima, s tim što se prema jednoj virusi dele na:

- *boot viruse* koji inficiraju but sektor hard diskova ili drugih medija,
- *fajl viruse* koji inficiraju izvesne fajlove,
- *makroviruse* koji su napisani u makrokomandnim jezicima, koji se pokreću u nekom specifičnom aplikativnom okruženju,
- *skript viruse* koji se pišu u jezicima nekih skripti.[123]

Pojmom virusa se uobičajeno nazivaju i druge vrste malicioznih programa koji takođe imaju štetno dejstvo po računar. U ovu grupu spadaju crvi (*worms*) i trojanci.

Crvi (mrežni crvi) su posebna vrsta zlonamernih programa koji se kreću kroz mrežu i u mogućnosti su da prodru u drugi računarski sistem. Poput virusa, crvi takođe kreiraju svoje kopije, ali ne inficiraju druge fajlove. Umesto toga, crv je obično samostalan, kompletan zlonamerni kod (ili skup od nekoliko takvih programskih modula).[124] Danas se najčešće šire elektronskom poštom. Njihova osobina je da se veoma brzo umnožavaju u velikim količinama, obično se šire bez pomoći korisnika i sami distribuiraju sopstvene potpune kopije širom mreža. Crv može da zauzme memoriju ili propusni opseg mreže toliko da računar prestane da reaguje.[125] Crvi se od klasičnih virusa razlikuju pre svega po mogućnosti da se sami kreću kroz računarsku mrežu, odnosno po tome što im nije potreban program-nosilac. Upravo ta činjenica čini ih bržim od klasičnog virusa (npr. 19. jula 2001. godine, crv po imenu „Code

[122] Marko Čavić, „Uhapšen tvorac mobilnih virusa", Mobi, internet *http://www.mobimag.rs/uhapsen-tvorac-mobilnih-virusa/,* 7. 5. 2009.

[123] „Računarski virusi", Singi inženjering, internet *http://www.singi.co.yu/podrska/racunarski_virusi.htm,* 7. 5. 2009.

[124] „Crvi", Singi inženjering, internet, *http://www.singi.co.yu/podrska/crvi.htm,* 7. 5. 2009.

[125] „Šta su virusi, crvi i trojanski konji?", Microsoft, internet *http://www.microsoft.com/scg/security/viruses/virus101.mspx#EJC*, 7. 5. 2009.

Red“ razmnožio se oko 250.000 puta za samo devet sati). Još jedan primer je crv „Mydoom“, koji je u jednom danu 2004. godine ugrozio četvrt miliona računara.[126]

Trojanci su vrsta zlonamernog programa koji ne može da se replicira, već se uglavnom sastoji od koda koji izvršava neke zlonamerne funkcije. Trojanci se klasifikuju prema vrsti štetnih aktivnosti koje prave:

Špijunski programi stoje u memoriji i loguju sve ulazne podatke sa tastature, aktivne aplikacije i sve to prosleđuju napadaču (hakeru). Najčešće su namenjeni za krađu lozinki i drugih poverljivih informacija;

PSW trojanci pretražuju mašinu u pokušaju da nađu fajlove u kojima se čuvaju poverljivi podaci i da ih pošalju napadaču;

Backdoor (zadnja vrata) imaju za cilj da napadaču otvore put za upad na zaraženu mašinu, odnosno da mogu daljinski da preuzmu kontrolu;

Trojan clickers – trojanci koji preusmeravaju računar korisnika na određeni veb sajt, bilo u cilju da izazovu DDoS napad na taj sajt, bilo da se korisnik pristupom tom sajtu zarazi nekim drugim trojancem ili virusom;

Trojan Dropper – trojanac koji vrši prikrivenu instalaciju drugih trojanaca ili programa.[127]

Kao zaštita od ovih štetnih programa koristi se antivirusni softver i ukoliko se redovno vrši njegovo ažuriranje (engl. *update*), korisniku pruža sigurnost prilikom svakodnevnog korišćenja računara. Antivirusne programe treba kombinovati sa „zaštitnim zidom“ (engl. *firewall*) koji može biti softverski ili hardverski i čija je funkcija da pregleda informacije koje dolaze sa interneta i odlaze na internet, prepoznaje i ignoriše informacije koje dolaze sa opasnih lokacija ili lokacija koje deluju sumnjivo.[128] Važno je napomenuti da nijedan program ne pruža apsolutnu zaštitu od računarskih virusa i da je neophodno da sami korisnici budu oprezni prilikom korišćenja računara, posećivanja veb stranica, preuzimanja sadržaja sa interneta, otvaranja elektronske pošte i instaliranja novih programa u računar.

U našem pravnom sistemu do sada nije bilo lica koja su procesuirana zbog izvršenja ovog krivičnog dela. Postoji više prijava protiv nepoznatih učinilaca zbog unošenja virusa, a policija i tužilaštvo rade na otkrivanju njihovog identiteta. U uporednopravnoj sudskoj praksi do sada je bilo više postupaka protiv lica koja su kreirala i širila računarske viruse. Tako je tokom

[126] Snežana Božović, Zoran Prokić, *Put kroz internet*, Nautilus computers d.o.o., Beograd, 2005, internet, *http://www.putkrozinternet.edu.yu/internet4.htm*, 7. 5. 2009.

[127] „Trojanski konji“, Singi inženjering, internet, *ttp://www.singi.co.yu/podrska/crvi.htm*, 7. 5. 2009.

[128] „Zašto treba da koristite računarski zaštitni zid“, Microsoft, internet *http://www.microsoft.com/scg/security/viruses/fwbenefits.mspx*, 7. 5. 2009.

2005. godine u nemačkom gradu Verdenu osuđen osamnaestogodišnji haker na uslovnu kaznu zatvora u trajanju od 21 meseca, jer je napisao i pustio na mrežu crv „Sasser" koji je 2004. godine za samo nedelju dana inficirao skoro 20 miliona računara širom sveta.[129]

Računarski virusi predstavljaju veoma ozbiljnu pretnju u savremenom svetu. Njihovim delovanjem mogu biti ugroženi objekti infrastrukture, sistemi odbrane, nuklearna postrojenja, čime u opasnost mogu biti dovedeni životi velikog broja ljudi. Da delovanje računarskih virusa ne poznaje granice govori i podatak da je Američka svemirska agencija NASA u avgustu 2008. godine objavila podatak da je jedan od računara na Međunarodnoj svemirskoj stanici (International Space Station, ISS) zaražen virusom. U pitanju je bio internet crv „Gammima", a na svemirsku stanicu je verovatno stigao preko nekog prenosivog uređaja – prenosivog računara ili USB fleš diska.[130] Ovaj incident nije ostavio teže posledice na funkcionisanje stanice i bezbednost posade.

Računarska prevara
– član 301 Krivičnog zakonika

Računarska prevara predstavlja krivično delo koje se može izvršiti unošenjem netačnog podatka, propuštanjem unošenja tačnog podatka, odnosno prikrivanjem ili lažnim prikazivanjem podataka, čime izvršilac utiče na rezultat elektronske obrade podataka u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, a propisana je novčana kazna ili zatvor do tri godine. U st. 2 i 3 propisani su kvalifikovani oblici ovog krivičnog dela kada iznos pribavljene protivpravne imovinske koristi prelazi četiristo pedeset hiljada dinara, odnosno iznos od milion petsto hiljada dinara, a zaprećene su zatvorske kazne od jedne do osam godina za stav 2, kao i zatvor od dve do deset godina za delo iz stava 3. U stavu 4 propisan je privilegovani oblik krivičnog dela kada je delo iz stava 1 preduzeto samo u nameri da se drugom pričini šteta, za šta je propisana novčana kazna ili zatvor do šest meseci.

Krivično delo *Računarska prevara* treba razlikovati od krivičnog dela *Prevara* iz člana 208 KZ, koje spada u grupu krivičnih dela protiv imovine. *Prevara* takođe može biti izvršena korišćenjem računarske tehnologije, kada

[129] G. B., „Podignuta optužnica protiv autora Sassera", Mikro-PC World, internet, *http://www.mikro.co.yu/main/index.php?q=vestiarhiva&godina=&mesec=&ID=6192*, 7. 5. 2009.

[130] „Računarski virusi stigli u svemir", Mikro-PC World, internet, *http://www.mikro.rs/main/index.php?q=vestiarhiva&godina=&mesec=&ID=10847,* 7. 5. 2009.

izvršilac u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist, lažnim prikazivanjem nekih činjenica ili njihovim prikrivanjem oštećenog dovede ili održava u zabludi i time ga navede da ovaj na štetu svoje ili tuđe imovine nešto učini, ili ne učini. O krivičnom delu *Prevara* i načinima njegovog izvršenja korišćenjem informacionih tehnologija poput nigerijskog pisma kasnije će biti više reči.

Radnja krivičnog dela je alternativno određena kao unošenje netačnog podatka ili propuštanje unošenja tačnog podatka. Netačan je onaj podatak koji istinito ne odražava ono na šta se odnosi. Ukoliko se delo vrši nečinjenjem, propuštanje treba da se odnosi na neki važan podatak. Važnost podatka je faktičko pitanje koje se raspravlja u svakom konkretnom slučaju, ali to je samo onaj podatak koji može uticati na elektronsku obradu podataka. Ovaj član kao radnju poznaje i prikrivanje ili lažno prikazivanje podataka na drugi način. Prikrivanje podataka znači obmanjivanje o nepostojanju postojećih podataka, što može biti izvršeno na više načina koje je u svakom slučaju potrebno konkretizovati, dok je lažno prikazivanje podataka kada se tvrdi da postoji nešto što ne postoji ili kada se ono što postoji prikazuje neistinito. U bilo kom obliku radnje krivičnog dela potrebno je da je takva radnja podobna da se njome utiče na rezultat elektronske obrade podataka i da je upravo zbog te radnje došlo do drugačije elektronske obrade.[131]

Namera zakonodavca je da propisivanjem ovog krivičnog dela zaštiti verodostojnost i integritet podataka koji se elektronski obrađuju ili se oni prenose elektronskim putem. Neophodno je utvrditi u svakom konkretnom slučaju i nameru učinioca koja se sastoji u tome da se za sebe ili drugog pribavi protivpravna imovinska korist i da se time drugom prouzrokuje imovinska šteta.

Izvršilac ovog krivičnog dela može biti svako lice, a u pogledu vinosti potreban je umišljaj. Delo je svršeno kada je preduzeta neka od radnji izvršenja, uz postojanje opisane namere i kada je time drugome prouzrokovana imovinska šteta, pri čemu nije neophodno da usled preduzete radnje bude i ostvarena protivpravna imovinska korist.

Za pravilnu kvalifikaciju krivičnog dela *Računarska prevara* i njegovo uspešno dokazivanje neophodno je utvrditi vreme i mesto izvršenja krivičnog dela, tačnu radnju koja je preduzeta, kao i način na koji je unet netačan podatak. U pogledu unetih podataka potrebno je ustanoviti njihovu neistinitost, u čemu se ta neistinitost ogleda i kako je time uticano na rezultat elektronske obrade i prenosa podataka, zatim ukoliko je u pitanju propuštanje unosa tač-

[131] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 121.

nog podatka, na koji način je to propušteno, odnosno na koji drugi način je prikriven ili lažno prikazan podatak, i to u cilju uticanja na rezultat obrade i prenosa. U vezi sa ovim potrebno je utvrditi način kako je podatak unet ili je propušteno njegovo unošenje, da li putem fizičkog pristupa uređaju podobnom za elektronski prenos ili obradu podataka ili je to učinjeno putem mreže, koji je softver bio korišćen tom prilikom, koliki je iznos koristi bio obuhvaćen umišljajem učinioca, odnosno da li je hteo da je pribavi sebi ili nekom drugom, te koliki je iznos nastale štete, čak ukoliko korist i nije ostvarena. Za dokazivanje dela iz stava 4 potrebno je utvrditi vrstu štete koja je bila obuhvaćena namerom i da li je takva šteta i nastupila, kao i postojanje namere učinioca da svojim delovanjem prouzrokuje štetu. Potrebno je utvrditi kojim je sredstvima izvršeno krivično delo i ukoliko je moguće, izvršiti njihovo oduzimanje kako bi bili obezbeđeni svi neophodni dokazi.[132]

Elektronska obrada podataka i očuvanje njenog integriteta i verodostojnosti od izuzetnog su značaja za svaku državu, naročito zbog toga što elektronsko poslovanje postaje dominantan vid aktivnosti privrednih subjekata u savremenoj ekonomiji. Poslovne transakcije koje se obavljaju elektronskim putem naročito su pogodne za razne vidove zloupotreba. Sa rastom njihovog obima povećava se broj krivičnih dela iz te oblasti, a posledice postaju sve teže. Ovim krivičnim delom mogu biti pogođeni svi privredni subjekti, od velikih korporacija i državnih preduzeća, banaka, do najmanjih poput knjigovodstvenih firmi ili sportskih kladionica.

U dosadašnjoj domaćoj sudskoj praksi bilo je nekoliko slučajeva procesuiranja učinilaca ovog krivičnog dela, a navedeni primeri govore o tome da računarska prevara postaje sve učestalije krivično delo. Tako je Tužilaštvo za borbu protiv visokotehnološkog kriminala pokrenulo istragu protiv osumnjičenog Č. A. zbog osnovane sumnje da je tokom 2007. i 2008. godine u dva navrata koristeći računar ulazio u sisteme banaka u Australiji i Švajcarskoj i izdavao lažne naloge za transfer sredstava, čime je pribavio protivpravnu imovinsku korist u iznosu od 51.990 CHF, odnosno da je pokušao da iz jedne švajcarske banke neovlašćeno izvrši transfer sredstava u iznosu od 19.000 USD.

Budući da u našoj zemlji postoji veliki broj sportskih kladionica koje imaju razgranatu mrežu poslovnica i čije je poslovanje nezamislivo bez računarskih mreža, neretko se dešavaju zloupotrebe ovakvih sistema. Izvršioci na različite načine pokušavaju da utiču na rezultat elektronske obrade podataka i da koristeći softverska rešenja falsifikuju odigrane tikete. Protiv M. D. po-

[132] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 122.

krenuta je istraga zbog osnovane sumnje da je 22. juna 2008. godine, u prostorijama sportske kladionice koja se nalazi u Čačku, vlasništvo ošt. „LES FOLIES DOO“ u svojstvu lica zaposlenog na poslovima prijema i naplate sportskih tiketa, u nameri da sebi i drugom pribavi protivpravnu imovinsku korist, prilikom unosa podataka u računar – izmenila sistemsko vreme na računaru, i to za uplate po tiketima Sportske prognoze serijskih brojeva F1... i F16..., unoseći, umesto realnog vremena, vreme kada je ishod utakmica po uplaćenim tiketima već bio poznat, čime je uticala na rezultat elektronske obrade podataka u vidu registrovanja novčanog dobitka po uplaćenim tiketima navedenih serijskih brojeva – koji je N. N. licu, istog i narednog dana, isplaćen u iznosu protivpravno pribavljene imovinske koristi od ukupno 120.438 dinara.

Tužilaštvo je tokom 2008. godine pokrenulo istragu protiv jednog od radnika preduzeća „Telekom“ zbog osnovane sumnje da je periodu od 2003. do 2007. godine oštetio preduzeće za više od deset miliona dinara tako što je lažno prikazivao podatke koji se odnose na tarifiranje telefonskog saobraćaja i na osamnaest telefonskih priključaka omogućio besplatno telefoniranje u lokalnom, međugradskom i međunarodnom saobraćaju, kao i u svim mrežama mobilne telefonije. Sličan primer možemo naći i u susednoj Crnoj Gori, kada je tokom 2005. godine crnogorski „Telekom“ oštećen za iznos od 6.120.000 evra, i to tako što su dvojica Budvana, bez licence koju izdaje Agencija za telekomunikacije Vlade Republike Crne Gore i prijavljene delatnosti, koristili servis „Voice over IP“ prebacujući međunarodne telefonske pozive na lokalnu mrežu, naplaćivali ovu uslugu u inostranstvu.[133]

Neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka – član 302 Krivičnog zakonika

Ovo krivično delo vrši lice koje se, kršeći mere zaštite, neovlašćeno uključi u računar ili računarsku mrežu, ili neovlašćeno pristupi elektronskoj obradi podataka, za šta je propisana novčana kazna ili zatvor do šest meseci. Kao poseban oblik izvršenja ovog krivičnog dela predviđena je upotreba podatka koji je dobijen na opisani način, a predviđena je novčana kazna ili zatvor do dve godine. Najteži oblik ovog krivičnog dela propisan je u stavu 3 kada je usled izvršenja dela opisanog u stavu 1 došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili mreže, ili su nastupile druge teške posledice. Za ovaj kvalifikovani oblik krivičnog dela propisana je kazna zatvora do tri godine.

[133] „Računarska prevara teška šest miliona eura“, *Pobjeda*, internet, *http://www.pobjeda.co.me/citanje.php?datum=2005-11-19&id=75425,* 7. 5. 2009.

Objekat zaštite ovog krivičnog dela su zaštićeni računari ili računarske mreže, odnosno podaci koji se elektronski obrađuju. Posledica ovog krivičnog dela je neovlašćeno uključivanje ili pristup, odnosno upotreba tako dobijenog podatka.

Stavom 3 propisan je kvalifikovani oblik osnovnog krivičnog dela, ako je usled radnji iz stava 1 došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili su nastupile druge teške posledice, pri čemu je ovo potrebno utvrditi u svakom konkretnom slučaju.

Izvršilac krivičnog dela može biti svako lice, a u pogledu vinosti potreban je umišljaj. Izvršilac mora imati svest da se vrši neovlašćeno uključenje u računar ili računarsku mrežu, da se upotrebljava podatak dobijen na ovakav način i da usled toga mogu nastupiti navedene posledice.[134] Izvršilac krivičnog dela iz stava 2 može biti i lice koje je izvršilo delo iz stava 1, ali to može biti i svako drugo lice koje je došlo u posed podataka. Ukoliko je isto lice preduzelo radnje iz st. 1 i 2, tada postoji krivična odgovornost tog lica samo za stav 2 s obzirom na to da radnje iz stava 1 predstavljaju samo pripremne radnje, koje nisu samostalne i nisu kažnjive.[135] S obzirom na to da pristup zaštićenom računaru i zaobilaženje postavljenih barijera zahteva dobro poznavanje funkcionisanja računara i mreža, dâ se zaključiti da izvršilac ovog krivičnog dela može biti samo ono lice koje poseduje veliki fond stručnih informatičkih znanja.

Za pravilnu kvalifikaciju krivičnog dela najpre je potrebno utvrditi vreme i mesto izvršenja krivičnog dela, kakva je ovlašćenja imao izvršilac, jer samo lice koje nije ovlašćeno da se uključi u računar ili pristupi elektronskoj obradi podataka može biti izvršilac oblika ovog krivičnog dela iz stava 1. Izvršilac krivičnog dela iz stava 2 može biti svako lice, jer pojam ovlašćenosti pristupa ili uključivanja ne mora u sebi sadržavati i dozvolu da se takav podatak upotrebi. Neophodno je tačno ustanoviti način na koji je izvršeno uključivanje u računar ili pristup elektronskoj obradi podataka, te kako je i na koji način taj podatak upotrebljen. Takođe, neophodno je u svakom konkretnom slučaju na precizan način utvrditi koje mere zaštite su kršene i na koji način, što je bitno obeležje ovog krivičnog dela. Za dokazivanje krivičnog dela propisanog stavom 3 ovog člana potrebno je na nesporan način utvrditi da li je usled radnji iz stava 1 došlo do zastoja ili ozbiljnog poremećaja u funkcionisanju elektronske obrade i prenosa podataka ili mreže, u

[134] Ljubiša Lazarević, *Komentar Krivičnog zakonika Republike Srbije,* Savremena administracija, Beograd, 2006, str. 750.

[135] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 125.

čemu se ogleda taj zastoj ili poremećaj funkcionisanja ili koje su to druge teške posledice koje su nastupile.[136]

Do sada je u našem pravosuđu nekoliko lica bilo optuženo zbog izvršenja krivičnog dela *Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka.* Tako je protiv T. N. i V. R. podnet optužni predlog jer su se u periodu od 25. oktobra 2007. do 15. septembra 2008. godine kršeći mere zaštite provajdera „BUS COMPUTER DOO", koje se sastoje od dodeljivanja korisničkog imena i pristupne lozinke svakom korisniku, neovlašćeno uključivali u mrežu na taj način što su od B. R. pribavili korisnička imena i lozinke drugih, a zatim su njihovim korišćenjem optuženi T. N. i V. R. zaobilazili sistem zaštite provajdera i neovlašćeno pristupali mreži, kao da je reč o drugim korisnicima, sa svojih računara, pričinivši štetu navedenom preduzeću u iznosu od 39.250 dinara. Navedenim licima je sudija Posebnog odeljenja za borbu protiv visokotehnološkog kriminala Okružnog suda u Beogradu, 24. marta 2009. godine, izrekao uslovnu osudu u trajanju od tri meseca zatvora, sa rokom proveravanja od godinu dana.

Još jedan sličan primer je i optužni predlog protiv V. M. koji je 8. februara 2007.godine, u vremenskom intervalu od 22:39:50 do 22:49:08 časova, u Kragujevcu, neovlašćeno pristupio računarskoj mreži ošt. preduzeća „Yunicom" sa sedištem u Beogradu, na taj način što je – putem interne računarske mreže hotela u kojem je boravio – konektovao svoj računar na globalnu računarsku mrežu i pristupajući sa IP adrese broj: 87.116.169.10, prekršio mere zaštite uspostavljene od strane ošt. preduzeća „Yunicom" – unoseći u svoj računar veb adresu broj: 217.24.2… dodeljenu ošt. preduzeću „Yunicom" za pristupanje veb – mejl serveru „World Client for MDaemon" preko kojeg su zaposleni iz ošt. „Yunicom"-a ostvarivali poštanski saobraćaj, nakon čega je – znajući kao bivši radnik „Yunicom"-a adrese elektronske pošte i lozinke zaposlenih lica – iste unosio i na svom računaru neovlašćeno pregledao sadržaj njihove elektronske pošte.

Kompjuterski sistemi američke vlade, vojske i raznih drugih agencija privlače radoznalost velikog broja hakera, koji skoro svakodnevno pokušavaju da provale njihove sisteme zaštite i dođu do „dragocenih" informacija. O tome nam govore dva aktuelna primera.

U novembru 2008. godine sud u rumunskom gradu Aradu osudio je hakera Viktora Faura na uslovnu kaznu zatvora u trajanju od jedne i po godine i na novčanu kaznu od 238.000 evra, jer je u periodu od novembra 2005. do

[136] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 126.

septembra 2006. godine ulazio u računarske sisteme vojnopomorskih snaga, Ministarstva odbrane SAD i svemirske agencije NASA.[137]

Drugi primer predstavlja britanski haker Gary McKinnon koji je optužen da je izvršio najveći upad u američke vojne sisteme ikada, u periodu od februara 2001. do marta 2002. godine. Ovaj haker se tereti da je ulazio u kompjutere američke vojske, mornarice, vazduhoplovstva, ministarstva odbrane, a sada mu preti kazna od sedamdeset godina zatvora. Advokati odbrane su, objašnjavajući postupke svog klijenta, tvrdili da je „posetom" dobro čuvanim računarskim sistemima okrivljeni samo hteo da dođe do podataka o postojanju vanzemaljskog života.[138]

Osude izvršilaca ovakvih krivičnih dela na zatvorske kazne u dugom trajanju i izricanje visokih novčanih kazni ne odvraćaju hakere od izazova koji predstavlja upad u dobro čuvane sisteme. Iako do sada nije bilo potvrđenih upada u sisteme naših državnih organa, institucija od javnog značaja, državnih preduzeća i dugih preduzeća koja obavljaju delatnosti od opšteg značaja, ne znači da ovakvi napadi nisu pokušavani ili da ih neće biti. Iskustvo razvijenih zemalja govori nam da ne postoji nijedan neprobojan sistem niti prepreka koju hakeri ne mogu da zaobiđu.

Krivično delo *Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka* prema načinu izvršenja može biti slično krivičnom delu *Špijunaža* iz člana 315 Krivičnog zakonika, koje spada u grupu krivičnih dela protiv ustavnog uređenja i bezbednosti Republike Srbije, ukoliko bi potencijalni izvršioci upadom u računarske sisteme došli do vojnih, ekonomskih ili službenih podataka ili dokumenata koji su zakonom, drugim propisom ili odlukom nadležnog organa donetom na osnovu zakona proglašeni tajnim. Odavanje takvih podataka moglo bi da prouzrokuje štetne posledice za bezbednost, odbranu ili za političke, vojne ili ekonomske interese zemlje. Zbog toga je važno da se u svakom konkretnom slučaju utvrdi umišljaj učinioca krivičnog dela, značaj zaštićenog računara ili računarske mreže koji su bili predmet napada, kao i priroda podataka koji bi bili pribavljeni na takav način.

[137] „Rumun osuđen zbog upada u računarsku mrežu američkih institucija", CyberBulevar.com, internet, *http://www.cyberbulevar.com/tehnologija/kompjuteri/rumun-osudjen-zbog-upada-u-racunarsku-mrezu-americkih-institucija/20081111/*, 7. 5. 2009.

[138] „Britanskom hakeru preti zatvor", ITsvet.com, internet, *http://www.itsvet.com/arhiva/2009-03-18,* 7. 5. 2009.

Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži – član 303 Krivičnog zakonika

Krivično delo se sastoji u neovlašćenom sprečavanju ili ometanju pristupa javnoj računarskoj mreži, a zaprećena je novčana kazna ili zatvor do jedne godine. Kvalifikovan oblik ovog krivičnog dela postoji kada opisane radnje preduzme službeno lice u vršenju službe, za šta je zaprećena kazna zatvora do tri godine.

Krivični zakonik u članu 112, tačka 18 definiše javnu računarsku mrežu kao skup međusobno povezanih računara koji komuniciraju razmenjujući podatke.

Sprečavanje pristupa javnoj mreži predstavlja potpuno onemogućavanje drugog da se koristi javnom računarskom mrežom, dok se ometanje sastoji u otežavanju pristupa takvoj mreži. Izvršilac ovog krivičnog dela mora postupati neovlašćeno, a ukoliko je postojao pravni osnov za sprečavanje nekoga da pristupi javnoj računarskoj mreži, ne može biti reč o ovom krivičnom delu.

Objekat zaštite ovog krivičnog dela predstavljaju javne računarske mreže dostupne neograničenom broju lica, a koje građani koriste u svakodnevnom životu za informisanje, obavljanje finansijskih transakcija, elektronsku trgovinu ili održavanje društvenih kontakata.

Izvršilac ovog krivičnog dela može biti svako lice i mora postupati sa umišljajem. Krivično delo je svršeno kad je preduzeta bilo koja radnja koja se može povezati sa sprečavanjem ili ometanjem pristupa javnoj računarskoj mreži, odnosno kada je službeno lice preduzelo neku od radnji koje spadaju u domen njegovog delovanja u cilju sprečavanja, odnosno ometanja pristupa javnoj računarskoj mreži.[139]

Za pravilnu kvalifikaciju ovog krivičnog dela neophodno je utvrditi sledeće činjenice: neovlašćenost, odnosno nepostojanje pravnog osnova za sprečavanje ili ometanje pristupa, vreme i mesto izvršenja krivičnog dela, način na koji je izvršeno sprečavanje ili ometanje, kao i svojstvo mreže, odnosno da li je u pitanju javna računarska mreža. Za dokazivanje krivičnog dela iz stava 2 potrebno je utvrditi svojstvo službenog lica izvršioca i radnju koju je on preduzeo. U praksi, potrebno je obratiti pažnju na to da li je navedeno krivično delo izvršeno u funkciji nekog drugog krivičnog dela ili je praćeno još nekom radnjom koja po svojim elementima predstavlja biće nekog drugog krivičnog dela, u kom slučaju se postavlja pitanje njihovog međusobnog odnosa i povezanosti.[140]

[139] Ljubiša Lazarević, *Komentar Krivičnog zakonika Republike Srbije,* Savremena administracija, Beograd, 2006, str. 751.

[140] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 126.

Jedan od najčešćih načina sprečavanja ili ograničavanja pristupa javnoj mreži predstavljaju takozvani DoS (engl. *Denial of service*) i DDoS (engl. *Distributed Denial of Service*) napadi. Organizovanju ovakvih napada prethodi stvaranje tzv. botneta – mreže zaraženih računara, koja nastaje tako što se pomoću određenog malicioznog softvera ostvaruje kontrola nad velikim brojem računara. Napadači skeniraju internet, pronalaze računare koji nisu adekvatno zaštićeni i na njih instaliraju navedeni softver. Broj zaraženih kompjutera može biti i nekoliko hiljada, npr. kod DDoS napada. Posle preuzimanja kontrole napadač izdaje komandu računarima u mreži da na određeni server pošalju veliki broj beskorisnih informacija, čime se saobraćaj zagušuje i onemogućuje pristup mreži i uslugama koje ona pruža.

Naročito opasnu vrstu predstavljaju PDoS napadi (engl. *Permanent denial of service*), koji mogu trajno da oštete hardver na serverima sa daljinskim pristupom. Napad se zasniva na iskorišćavanju *firmware* apdejta koji se serverima šalje preko mreže ili interneta, a koji je sposoban da prevari hardver i flešuje (engl. *flash*) bilo koji deo sistema, što bi moglo dovesti do trajnog i potpunog hardverskog pada.[141] Mišljenja smo da bi ovakva vrsta napada mogla biti kvalifikovana kao računarska sabotaža. Termin firmver (engl. *firmware*) označava skup programa – softver, koji su fabrički ugrađeni u hardverske uređaje i komponente. S vremenom, proizvođači opreme pronalaze bolja softverska rešenja za funkcionisanje tih uređaja. Postupak zamene postojećeg firmvera novim naziva se flešovanje. Loše upisivanje firmvera ili upisivanje pogrešnog ili neispravnog firmvera obično znači „kliničku smrt" za uređaj i zahteva posebne intervencije stručnih servisera.[142]

Tokom 2008. godine u Srbiji je bilo više DDoS napada. Izdvojićemo primere napada na internet sajt Srpske pravoslavne crkve, koji se smatra jednim od najžešće izvedenih napada ikad, kao i obaranje internet prezentacije radioemisije „Peščanik". Identitet izvršilaca napada gotovo je nemoguće identifikovati upravo zbog činjenice da upiti dolaze sa velikog broja „zaraženih" računara, čiji korisnici nisu ni svesni da im je računar zloupotrebljen i da je deo botnet mreže, a informacije koje šalje botnet ne mogu se razlikovati od informacija legalnih korisnika. Utvrđivanje činjenica koje se odnose na mesto, vreme i način „inficiranja" kompjutera programom koji ga je učino delom mreže sa koje je izvršen napad, u svakom pojedinačnom slučaju povezano je sa velikim troškovima i angažovanjem velikog broja istražitelja, zbog čega je

[141] „Denial-of-service attack", Wikipedia, internet, *http://en.wikipedia.org/wiki/Denial-of-service_attack,* 7. 5. 2009.

[142] Bojan Živković, „Operacija visokog rizika", *Svet kompjutera*, internet, *http://www.sk.co.yu/2004/09/skse01.html*, 7. 5. 2009.

dokazivanje ovog krivičnog dela veoma otežano. Napadači maskiraju IP adrese sa kojih se upućuju napadi tako što ih menjaju i lažiraju (engl. IP *spoofing*) te je veoma teško doći do njihovog izvora.

Važnija javna preduzeća bila su u skorijoj prošlosti meta ovakvih napada. Prvi slučaj velikog i organizovanog ataka na kompjuterske sisteme u našoj zemlji desio se tokom avgusta 2001. godine na link preduzeća „Telekom", kada je posle podizanja cene telefonskih impulsa grupa hakera napala servere preduzeća velikim brojem nepotrebnih poruka. Napad koji je dolazio sa ostrva u Pacifiku bio je ograničenog karaktera, trebalo je nakratko da zaguši veze na internetu i obori sistem, pa je šteta koja je tom prilikom pričinjena iznosila oko 250.000 dinara.[143] Hakeri su pretili da će izvršiti i ozbiljniji napad, ali do toga nije došlo.

Iz uporednopravne prakse možemo izdvojiti primer šesnaestogodišnjeg hakera iz Kanade sa nadimkom Mafiaboy, koga je Sud za maloletnike u Montrealu osudio na kaznu od osam meseci boravka u popravnom domu.[144] Ovaj mladić je u februaru 2000. godine izvršio DDoS napad na servere kompanija Yahoo, eBay Amazon, Buy.com, ZDNet, CNN, E-Trade i MSN, čime je prouzrokovao prekid njihovog rada koji je trajao od nekoliko sati do nekoliko dana, a šteta nastala prekidom njihovog rada bila ogromna i merila se milionima dolara.[145]

Hakeri koji se služe DDoS napadima usavršavaju tehnike za njihovo izvođenje. Iako nije moguće sprečiti DDoS napade, moguće je preduzeti mere kojima bi se ublažile njihove posledice i ograničio broj pristupa određenom serveru u skladu sa njegovim kapacitetom, odnosno uspostaviti softversko-hardverska rešenja kojima bi se filtrirali upiti koje stižu na server.

Neovlašćeno korišćenje računara ili računarske mreže – član 304 Krivičnog zakonika

Ovo krivično delo izvršava lice koje neovlašćeno koristi računarske usluge ili računarsku mrežu u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist, a predviđena je novčana kazna ili zatvor do tri meseca. Gonjenje za ovo krivično delo preduzima se po privatnoj tužbi.

---

[143] M. Lakić , M. Ž. Lazić, „Danas ističe ultimatum koji su hakeri dali Telekomu", *Politika,* 18. 8. 2001.

[144] „'Mafiaboy' Sentenced to 8 months in Detention", The Industry Standard, internet, *http://www.thestandard.com/article/0,1902,28975,00.html,* 7. 5. 2009.

[145] Thomas C. Greene, „Canadian Feds charge Mafiaboy in DDoS attacks", The Register, internet, *http://www.theregister.co.uk/2000/04/19/canadian_feds_charge_mafiaboy/*, 7. 5. 2009.

Radnja krivičnog dela je određena kao neovlašćeno korišćenje računarskih usluga ili računarske mreže. Za postojanje ovog krivičnog dela neophodno je utvrditi i nameru izvršioca da sebi ili drugom pribavi protivpravnu imovinsku korist. Izvršilac može biti svako lice, a u pogledu vinosti potreban je direktan umišljaj.[146]

Međutim, i u slučaju ovog krivičnog dela ovlašćena službena lica su dužna da preduzmu radnje iz svoje nadležnosti i da prikupe potrebne dokaze, ukoliko postoje osnovi sumnje da je u vezi sa radnjama koje spadaju u ovo krivično delo izvršeno i neko drugo krivično delo za koje se gonjenje preduzima po službenoj dužnosti, u kom slučaju za to delo važe ovlašćenja i odredbe koje se odnose na podnošenje krivične prijave.[147]

Ovde ćemo pomenuti i krivična dela iz glave 17. Krivičnog zakonika, koja su uperena protiv časti i ugleda, a za koja se gonjenje takođe preduzima po privatnoj tužbi.

Globalna računarska mreža je stvorila nove načine komunikacije među ljudima. Brojni imejl serveri i onlajn društvene mreže pružaju mogućnost besplatnog povezivanja njihovih korisnika, ma gde se oni nalazili. Pored pogodnosti koje pružaju, ovakvi vidovi korišćenja interneta stvorili su i brojne mogućnosti za zloupotrebu.

Internet je naročito pogodno okruženje za izvršenje krivičnih dela protiv časti i ugleda iz glave 17. Krivičnog zakonika, odnosno krivičnih dela *Uvreda* – član 170, *Kleveta* – član 171 i *Iznošenje ličnih i porodičnih prilika* – član 172 Krivičnog zakonika. Svakodnevno u medijima saznajemo kako su na internetu, bez odobrenja, objavljene eksplicitne fotografije ili video-zapisi javnih ličnosti, kao i detalji iz njihovog intimnog života, odnosno da se računarska mreža koristi za vređanje drugih, iznošenje neistinitih činjenica koje mogu štetiti nečijem ugledu ili časti.

Izvršenju ovakvih krivičnih dela pogoduje činjenica da svest o opasnostima koje mogu doći sa interneta i dalje nije dovoljno razvijena. Građani neoprezno i bez bilo kakve kontrole ostavljaju svoje detaljne lične podatke na raznim stranicama namenjenim druženju ili kupovini, nesvesni mogućnosti da isti podaci mogu postati predmet zloupotrebe. Broj ovako izvršenih krivičnih dela je u svakodnevnom porastu, a do javnosti dopiru samo slučajevi koji se tiču poznatih ličnosti. Tužilaštvu za borbu protiv visokotehnološkog kriminala podnet je veliki broj prijava zbog krivičnih dela za koja se gonjenje

[146] Ljubiša Lazarević, *Komentar Krivičnog zakonika Republike Srbije,* Savremena administracija, Beograd, 2006, str. 751

[147] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 128.

preduzima po privatnoj tužbi, s tim što je reagovalo u slučaju kada je na sajtu „Fejsbuk“ postavljena slika maloletne devojčice i zatražilo od administratora sklanjanje takvog sadržaja.

Sve češća je krađa identiteta, bilo da neko ukrade nečije korisničko ime i lozinku ili da pod tuđim imenom otvori nalog na nekom imejl serveru ili društvenoj grupi. Registrovanje lažnih naloga na različitim sajtovima koji su namenjeni „druženju“ (*facebook*, karike...) i objavljivanje kompromitujućih podataka, fotografija i video-zapisa može oštećene izložiti velikoj sramoti, zbog čega se oni i ne obraćaju državnim organima za pomoć. Veliki problem je u tome što se krivično gonjenje za ova dela preduzima po privatnoj tužbi, a oštećeni nemaju dovoljno sredstava ili znanja da sami otkriju identitet izvršilaca. Jedino što mogu jeste da se obrate administratorima navedenih internet stranica i zatraže ukidanje spornih naloga, odnosno brisanje neprikladnog sadržaja, što ne može imati veliki značaj, jer jednom objavljen podatak na internetu gotovo je nemoguće više ukloniti.

Prikazivanje pornografskog materijala i iskorišćavanje dece za pornografiju – član 185 Krivičnog zakonika

Ovo krivično delo ima tri oblika, a prvi čini lice koje detetu proda, prikaže ili javnim izlaganjem ili na drugi način učini dostupnim tekstove, slike, audio-vizuelne ili druge predmete pornografske sadržine ili mu prikaže pornografsku predstavu, a zaprećena je novčana kazna ili zatvor do šest meseci. U stavu 2 inkriminisano je iskorišćavanje deteta za proizvodnju slika audio-vizuelnih ili drugih predmeta pornografske sadržine ili za pornografsku predstavu, a propisana je kazna zatvora od šest meseci do pet godina. Stavom 3 propisano je kažnjavanje lica koje prodaje, prikazuje, javno izlaže ili elektronski ili na drugi način čini dostupnim slike, audio-vizuelne ili druge predmete pornografske sadržine nastale izvršenjem dela iz stava 2 ovog člana, za šta je zaprećena kazna zatvora do dve godine.

Propisivanjem ovog krivičnog dela i velikog broja kažnjivih radnji zakonodavac je imao nameru da zaštiti psihofizički i polni integritet dece. Krivični zakonik u članu 112 definiše pojam deteta kao lice koje nije navršilo četrnaest godina, a maloletnika kao lice koje je navršilo četrnaest godina a nije navršilo osamnaest godina.

Zakonodavac opravdano propisuje veliki broj radnji ovog krivičnog dela. Delo iz stava 1 može se izvršiti prodajom, prikazivanjem, javnim izlaganjem ili činjenjem dostupnim na drugi način audio-vizuelnih ili drugih predmeta pornografske sadržine ili prikazivanjem pornografske predstave. Ove radnje moraju biti usmerene prema detetu. Zakonik ne daje definiciju pornografskog mate-

rijala niti je bilo kojim drugim propisom taj pojam preciznije određen, zbog čega je ovo pitanje prepušteno oceni u svakom konkretnom slučaju. Smatramo da je pornografska ona sadržina koja na eksplicitan i specifičan način prikazuje seksualne odnose sa isticanjem pojedinih detalja. Ovo delo je svršeno preduzimanjem ma koje od alternativno postavljenih radnji izvršenja, a u pogledu vinosti potreban je umišljaj. Krivično delo opisano u stavu 2 sastoji se u iskorišćavanju deteta za proizvodnju pornografskih sadržaja ili pornografske predstave, što podrazumeva zloupotrebu deteta koje često nije ni svesno činjenice da je iskorišćeno ili u koje se svrhe iskorišćava. Stavom 3 kao radnje predviđene su prodaja, prikazivanje, javno izlaganje ili na drugi način činjenje dostupnim predmeta pornografske sadržine nastale izvršenjem stava 2 ovog člana. To znači da ovo krivično delo može biti izvršeno samo prema punoletnom licu ili maloletnom licu starijem od četrnaest godina, jer bi, u suprotnom, bilo reči o izvršenju ovog dela ali iz stava 1. U pogledu vinosti potreban je umišljaj.[148]

Zakonodavac je načinio propust kada je za krivično delo *Prikazivanje pornografskog materijala i iskorišćavanje dece za pornografiju* propisao ovako blage kazne, pogotovo za krivična dela opisana u st. 2 i 3. Potrebno je što pre uskladiti tekst Krivičnog zakonika sa stavovima nedavno ratifikovane Konvencije Saveta Evrope o visokotehnološkom kriminalu iz 2001. godine i inkriminisati i samo posedovanje materijala nastalog iskorišćavanjem dece za pornografiju, ali i dati što precizniju zakonsku definiciju pornografskog materijala. Takođe, potrebno je vratiti ovo krivično delo u nadležnost okružnih sudova, odnosno preneti ga Posebnom odeljenju Okružnog suda u Beogradu za borbu protiv visokotehnološkog kriminala.

Za dokazivanje krivičnog dela potrebno je na nesumnjiv način utvrditi vreme i mesto izvršenja krivičnog dela, način izvršenja – koja od radnji izvršenja je sprovedena i prema kom licu, a za pojedine oblike ovog dela potrebno je utvrditi da je reč o maloletnom licu mlađem od četrnaest godina. Takođe, potrebno je utvrditi u kom obliku je navedeni pornografski sadržaj manifestovan, da li je reč o slikama, audio-vizuelnim zapisima, kao i način na koji je učinjen dostupnim. Veoma je važno istaći činjenicu da je u slučaju ovog krivičnog dela reč o maloletnim licima, što zahteva posebnu pažnju u postupanju imajući u vidu njihove godine, specifično psihofizičko stanje i proces razvoja i sazrevanja, bilo da je u pitanju maloletno lice kao izvršilac krivičnog dela ili takvo lice kao oštećeni ili svedok.[149]

[148] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 147.

[149] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 148

Prema pozitivnom zakonodavstvu Republike Srbije, kao oblici izvršenja ovog krivičnog dela nisu predviđeni: posedovanje audio-vizuelnih materijala nastalih iskorišćavanjem dece za pornografske svrhe, preuzimanje ovakvog sadržaja sa interneta, niti poseta pedofilskim sajtovima. Smatramo da bi u zavisnosti od načina preuzimanja tzv. daunlouda (engl. *Download*) ovakvog materijala, takav čin mogao biti kvalifikovan kao krivično delo *Prikazivanje pornografskog materijala i iskorišćavanje dece za pornografiju.* Bitna karakteristika torenta, odnosno „P2P" preuzimanja jeste da korisnik koji preuzima fajlove u isto vreme postaje „sider", odnosno deli – čini dostupnim te iste fajlove drugim korisnicima. Da bi se dokazala krivica osobe koja je na ovakav način preuzela i činila dostupnim pedofilski materijal, potrebno je utvrditi njen umišljaj, odnosno da je znala sadržinu preuzetog materijala, kao i postojanje namere za dalju distribuciju.

Uz zloupotrebu platnih kartica i pirateriju, zloupotreba dece za pornografiju putem interneta predstavlja najčešći vid visokotehnološkog kriminala. Globalna mreža je stvorila nove mogućnosti za delovanje izvršilaca ove vrste krivičnih dela, njihovo povezivanje i razmenu pedofilskog materijala. U ranijim fazama razvitka interneta bilo je relativno lako otkriti i locirati ove kriminalne grupe i utvrditi sadržinu materijala koji razmenjuju ili prodaju. Danas je običnom pretragom interneta nemoguće pronaći pedofilske veb stranice ili forume. Ovakvi sajtovi su zaštićeni šiframa, imaju više nivoa pristupa, a zainteresovane osobe moraju same ponuditi materijal kako bi postale članovi. Materijal koji se razmenjuje takođe je zaštićen nekim od metoda kriptovanja. Da izvršioci ovog krivičnog dela nisu samo nastrane osobe izmenjenog seksualnog nagona, govore nam karakteristike ovog vida kriminala, a to su dobra organizovanost i zatvorenost grupa, kao i unosnost, jer su prihodi koji se ostvaruju ovakvom zloupotrebom dece ogromni. U SAD je sprovedena akcija hapšenja pedofila nazvana „Projekat Lavina", kada je u Teksasu uhapšeno dvoje ljudi koji su se bavili prodajom pedofilskih sadržaja preko interneta. Njihov biznis Landslide Productions Inc. uvećavao se za čitavih 1,4 miliona američkih dolara mesečno, s tim što su „klijenti" plaćali tek 14,95 dolara da bi pristupili sajtovima poput „Cyber Lolita" i „Child Rape". Ridijevi su za članarinu dozvoljavali pristup sajtovima na 30 dana.[150]

U borbi protiv pedofilije na internetu angažovan je veliki broj ljudi, postoje posebne policijske jedinice koje periodično otkrivaju izvršioce ovih krivičnih dela i njihove organizacije. Brojna udruženja građana bave se ovim problemom i pomažu žrtvama, a često i sami hakeri pomažu državnim

[150] Danijela Ćirović, Nebojša Janković, Milan Lađević, „Cyber podzemlje u Srbiji", *Reporter,* 16. 11. 2005, str. 12.

organima u otkrivanju ovakvih grupa. Tokom 2008. godine u SAD su tri velika internet provajdera, Sprint Nextel, Time Warner Cable i Verizon, postigla dogovor o blokiranju pristupa sajtovima sa dečjom pornografijom i ulaganju sume od 1,1 milion dolara radi pronalaženja i brisanja sa mreže pedofilskih materijala.[151]

Iako Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Službeni glasnik RS“, br. 61/05) nije predviđena nadležnost Tužilaštva za borbu protiv visokotehnološkog kriminala za postupanje u krivičnopravnim stvarima koje se odnose na dečju pornografiju, ustanovljena je praksa da policija i tužilaštvo obavljaju celokupan pretkrivični postupak a da se krivični postupak odvija pred mesno nadležnim opštinskim sudovima. Tužilaštvo intenzivno sarađuje i sa međunarodnim organizacijama u cilju suzbijanja dečje pornografije i otkrivanja izvršilaca ovih krivičnih dela. Uspostavljena je intenzivna saradnja sa Nacionalnim centralnim biroom Interpola u Beogradu, na osnovu čijih obaveštenja su, uz asistenciju MUP RS, otkrivani korisnici interneta u Srbiji preko čijih su IP adresa preuzimani i razmenjivani pedofilski materijali. Tako je u okviru operacija „Malj“, „Myosis“ i „Duga“ identifikovano više lica koja su se bavila ovom vrstom kriminalnih aktivnosti.

Do sada su pred Okružnim sudom u Beogradu vođeni postupci protiv izvršilaca ovog krivičnog dela, a ova lica su osuđivana na višegodišnje zatvorske kazne. Tako je nepravosnažnom presudom K br. 1930/05 osuđen J. S. na kaznu zatvora u trajanju od dvanaest godina zatvora zbog četiri krivična dela *Iskorišćavanje maloletnih lica za pornografiju* iz člana 111a, stav 2 u vezi sa stavom 1 KZ RS u sticaju sa krivičnim delom *Obljuba ili protivprirodni blud sa licem koje nije navršilo 14 godina* iz člana 106, stav 1 KZ RS. Ovo lice je preko interneta rasturalo fotografske snimke pornografskog sadržaja maloletnih lica koja nisu navršila 14 godina, muškog i ženskog pola, kao i beba, na kojima su prikazane radnje obljube, seksualnog zlostavljanja i protivprirodnog bluda, ali i 211 fotografija koje je sam sačinio dok je zlostavljao maloletnu devojčicu. Drugi, ne tako drastičan primer je nepravosnažna presuda K br. 1207/05, kojom je B. N. osuđen na tri godine zatvora, jer je u periodu između 12. marta 2005. godine i 18. juna 2005. godine u Beogradu, u dva navrata prodao i pokušao da proda fotografske, filmske i druge snimke pornografskog sadržaja maloletnih lica koja nisu navršila 14 godina, tako što je preko interneta oglašavao prodaju ovakvog materijala, a zatim stupao u kontakt sa zainteresovanim licima i ugovarao prodaju po ceni od 100 do 150 evra.

[151] „Three US ISPs agree to block child pornography sites“, Tech Connect Magazine, internet, *http://www.tcmagazine.info/comments.php?id=20354&catid=6&highlight=child+pornography,* 7. 5. 2009.

Iz uporednopravne sudske prakse možemo izdvojiti primer kada su tokom akcije britanske policije iz 2001. godine, nazvane „Operation Cathedral", uhapšena sedmorica članova grupe, organizatora mreže „Wonderland Club", u okviru koje je razmenjivano 750.000 fotografija i 1.800 video-klipova sa dečjom pornografijom. Osuđeni su na kazne zatvora u trajanju od 12 do 30 meseci, a grupe za zaštitu dečjih prava u Velikoj Britaniji bile su veoma nezadovoljne ovakvim kaznama.[152] Ova lica su organizovala jednu od najvećih ikada otkrivenih svetskih mreža dečje pornografije na internetu, a uslov za „članstvo" bio je da svako zainteresovano lice ima najmanje 10.000 fotografija dece predtinejdžerskog uzrasta i da te fotografije razmenjuje s drugim članovima. U koordiniranoj policijskoj akciji uhapšeno je 107 ljudi u 12 država – SAD, nekoliko evropskih zemalja i Australiji.[153]

Pedofilija na internetu je savremena pojava koja zahteva sveobuhvatnu društvenu akciju radi njene prevencije, suzbijanja i otklanjanja posledica. Danas je sprovode mnoge kampanje čiji je cilj edukacija o bezbednom korišćenju interneta, upoznavanje potencijalnih žrtava sa opasnostima koje im prete sa interneta, ali i odvraćanje potencijalnih učinilaca od izvršenja krivičnih dela.

1.1.2. Krivična dela protiv intelektualne svojine

Navedena krivična dela su sadržana u glavi XX Krivičnog zakonika i u njih spadaju: Povreda moralnih prava autora i interpretatora – član 198, Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava – član 199, Neovlašćeno uklanjanje ili menjanje elektronske informacije o autorskom i srodnim pravima – član 200, Povreda pronalazačkog prava – član 201 i Neovlašćeno korišćenje tuđeg dizajna – član 202, s tim što ćemo dati prikaz najzastupljenijeg krivičnog dela iz oblasti visokotehnološkog kriminala.

Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava – član 199 Krivičnog zakonika

Ovo krivično delo je veoma široko definisano. Stavom 1 propisana je kazna zatvora do tri godine za lice koje neovlašćeno objavi, snimi, umnoži ili na drugi način javno saopšti u celini ili delimično autorsko delo, interpretaciju, fonogram, videogram, emisiju, računarski program ili bazu podataka. Ista kazna je propisana u stavu 2 za lice koje stavi u promet ili u nameri stavljanja u

[152] „Wonderland sentences a 'joke'", BBC News, internet, *http://news.bbc.co.uk/2/hi/uk_news/1169457.stm*, 7. 5. 2009.

[153] „Razbijena mreža dečje pornografije na Internetu", Mikro-PC World, *http://www.mikro.rs/main/index.php?q=vest&ID=1646#povezanevesti,* 7. 5. 2009.

promet neovlašćeno drži umnožene ili neovlašćeno stavljene u promet primerke autorskog dela, interpretacije, fonograma, videograma, emisije, računarskog programa ili baze podataka. Stavom 3 propisana je kazna zatvora od tri meseca do pet godina za lice koje je delo iz st. 1 i 2 učinilo u nameri pribavljanja imovinske koristi za sebe ili drugog. Stavom 4 predviđeno je da će se lice koje proizvede, uveze, stavi u promet, proda, dâ u zakup, reklamira u cilju prodaje ili davanja u zakup, ili drži u komercijalne svrhe uređaje ili sredstva čija je osnovna ili pretežna namena uklanjanje, zaobilaženje ili osujećivanje tehnoloških mera namenjenih sprečavanju povreda autorskih i srodnih prava, ili koje takve uređaje koristi u cilju povrede autorskog ili srodnog prava, kazniti novčanom kaznom ili kaznom zatvora do tri godine.

Radnja krivičnog dela je alternativno postavljena, kao objavljivanje, snimanje i umnožavanje, odnosno saopštavanje na drugi način autorskog dela, interpretacije, fonograma, videograma, emisije, računarskog programa ili baze podataka. Potrebno je utvrditi da su navedene radnje preduzete neovlašćeno. Snimanje predstavlja pravljenje fotografskog ili drugačijeg snimka autorskog dela, interpretacije, fonograma, videograma, emisije, računarskog programa ili baze podataka, dok je umnožavanje pravljenje kopija pobrojanih predmeta, pri čemu za postojanje krivičnog dela nije značajan broj kopija, ali navedeno jeste značajno sa aspekta nadležnosti za postupanje u ovom krivičnom delu u smislu člana 3 Zakona o organizaciji i nadležnosti državnih organa u borbi protiv visokotehnološkog kriminala. Stav 2 ovog člana propisuje radnju koja dopunjuje prethodni stav inkriminišući stavljanje u promet ili neovlašćeno držanje u nameri stavljanja u promet navedenih predmeta. Stavljanje u promet je, kao i kod prethodnog krivičnog dela, činjenje dostupnim javnosti primeraka tuđeg autorskog dela, a pod tim treba podrazumevati prodaju, razmenu, rasturanje, poklanjanje i sve druge delatnosti kojima se ostvaruje suština neovlašćenog činjenja dostupnim.[154]

Piraterija je oduvek postojala, ali je sa pojavom modernih informacionih tehnologija i računarskih mreža doživela ekspanziju i poprimila globalne razmere. Danas skoro svaki film, muzički album, kompjuterski program, videoigra ili knjiga, pored legalnog, ima i „piratsko“ izdanje. Širenju piraterije doprinosi činjenica da izvršilac ovih krivičnih dela može biti bilo koje lice, odnosno da za izvršenje dela nisu potrebna specijalizovana znanja iz oblasti računarske tehnologije, kao i činjenica da su sredstva za izvršenje ovih dela jeftina i svima lako dostupna.

[154] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 133.

Tokom 2008. godine Tužilaštvu za borbu protiv visokotehnološkog kriminala podneto je 319 krivičnih prijava protiv 332 lica zbog izvršenja ukupno 379 krivičnih dela koja se odnose na povredu intelektualne svojine, a ukupno su oduzeta 131.232 optička diska i 50 tehničkih uređaja. Imajući u vidu opisano stanje kriminaliteta, postignut je dogovor sa istražnim odeljenjem Okružnog suda u Beogradu da se u cilju što efikasnijeg rešavanja ovih predmeta primenjuje postupak za kažnjavanje i izricanje presude od strane istražnog sudije, saglasno članu 455 Zakonika o krivičnom postupku. Ova vrsta postupka primenjuje se kada je to opravdano, a naročito se uzima u obzir ranija osuđivanost osumnjičenih lica i motivi za izvršenje krivičnog dela.

Piraterija je veoma unosna jer prihod od prodaje znatno prevazilazi iznos sredstava koja su uložena, a u praksi smo se do sada sreli sa nekoliko izvršilaca koji su baveći se ovom vidom kriminalnih aktivnosti ostvarili velike prihode. Pirati najčešće nude naslove kojih još nema u bioskopskom ili bilo kom drugom vidu distribucije, što znatno otežava postupak utvrđivanja nosilaca autorskih prava na neovlašćeno kopiranim i distribuiranim sadržajima. Piraterija ima i svoju socijalnu dimenziju, s obzirom na to da su izvršioci ovih krivičnih dela najčešće mlađa maloletna lica ili stariji ljudi, kao i lica sa posebnim potrebama, koja ne mogu da pronađu posao i koja prodajući diskove na ulici za račun „šefa“ obezbeđuju sebi i svojim porodicama osnovna sredstva za život.

Sa povećanjem broja korisnika interneta i uvođenjem većih brzina internet protoka, pirati su svoje delovanje preselili na internet, o čemu govori veliki broj sajtova sa kojih se mogu naručiti piratska izdanja novih filmova ili kompjuterskih igara. Sve češće kod izvršilaca ovih krivičnih dela ne možemo fizički pronaći piratske kopije, već oni po porudžbini navedene sadržaje preuzimaju sa interneta i zatim ih prodaju naručiocima. „Pirati“ na svojim internet stranicama neretko nude i više desetina hiljada naslova a da policija kod njih pronađe svega nekoliko stotina kopija. U pretkrivičnom postupku potrebno je sačiniti potvrdu o predmetima koji su oduzeti od okrivljenog, u kojoj moraju biti navedeni naslovi svih filmova, programa ili muzičkih dela stavljenih u promet. Popisivanje je neophodno kako bi bila obavljena identifikacija ovlašćenih distributera koji su oštećeni izvršenjem krivičnog dela. Ovo stvara teškoće i oduzima mnogo vremena policijskim službenicima, naročito kada se broj naslova meri desetinama hiljada i predstavlja glavni razlog zbog koga se broj uličnih prodavaca piratskih diskova ne smanjuje. Identifikacija nosilaca prava opterećuje i tužioce, pa je radi ubrzavanja pretkrivičnog postupka, Tužilaštvo za borbu protiv visokotehnološkog kriminala napravilo bazu podataka sa naslovima filmova, muzičkih dela i softvera, kao i ovlašćenim distributerima istog sadržaja. Smatramo da je neophodno promeniti stav suda

po kome je potrebno popisati naslove svakog autorskog dela koje je oduzeto od okrivljenog i utvrditi nosioce prava na svim tim delima, što bi znatno ubrzalo vođenje postupka i smanjilo troškove njegovog vođenja, povećalo efikasnost rada pravosudnih i policijskih organa, a što je najvažnije, dovelo do znatnog opadanja broja izvršenih krivičnih dela ove vrste.

Pirati za svoje delovanje zloupotrebljavaju kompanije koje nude usluge čuvanja (engl. *host*) datoteka na svojim serverima, poput Rapidshare, Megaupload i dr. Pre postavljanja (engl. *upload*) originalni fajl se podeli na više manjih delova korišćenjem nekih od programa za deljenje poput „Winzip", „Filesplitter" ili „HjSplit", koji se potom zaštićuju šifrom. Mali fajlovi dobijeni na ovaj način obično nemaju originalan naziv filma ili programa, zbog čega je nelegalan sadržaj teško otkriti. Linkovi koji vode ka ovim fajlovima nalaze se na veb sajtovima i forumima specijalizovanim za razmenu piratskih sadržaja. Navedene kompanije ostavljaju mogućnost svojim korisnicima da u svakom trenutku prijave zloupotrebu, što pirate ne odvraća da i dalje postavljaju nelegalne sadržaje, zbog čega se serveri ovih kompanija danas smatraju glavnim izvorima piraterije na internetu.

Još jedan veoma popularan način razmene fajlova koji se zloupotrebljava za pirateriju predstavljaju torenti, programi koji se baziraju na „P2P" (engl. *peer to peer*) tehnologiji, kojom se ostvaruje direktna veza između dva kompjutera radi razmene podataka između korisnika. Uspostavlja se veza između korisnika koji imaju određeni fajl na svom kompjuteru, tzv. „sideri" (engl. *seeders*) i klijenata koji traže isti fajl, tzv. „ličeri" (*leechers*), a na ovaj način se najčešće razmenjuju veliki video-fajlovi, muzička dela i softver. Kako bi inicirao preuzimanje fajla (engl. *download*), „ličer" pokreće torent, program koji ostvaruje vezu sa centralnim serverom – „trekerom" (engl. *tracker*) na kome se nalaze podaci o „siderima". Nakon toga klijent uspostavlja više simultanih „P2P" konekcija sa „siderima" i počinje da preuzima traženi fajl sa više lokacija odjednom. Karakteristika ovog procesa je da korisnik koji preuzima fajlove u isto vreme postaje „sider", odnosno deli te iste fajlove sa drugim korisnicima.[155]

Činjenica koja u velikoj meri doprinosi raširenosti ovog krivičnog dela jeste da građani nemaju predstavu o visini štete koju ono nanosi. Kupujući jeftine piratske diskove, građani veruju da uskraćuju prihod moćnim softverskim kompanijama poput Majkrosofta, odnosno holivudskoj filmskoj industriji. Istina je, međutim, sasvim drugačija.

[155] „BitTorrent (protocol)", Wikipedia, internet, *http://en.wikipedia.org/wiki/BitTorrent_(protocol),* 10. 5. 2009.

Prema studiji Međunarodne analitičarske kuće IDC (engl. International Data Corporation), tokom 2007. godine stopa piraterije u Srbiji iznosila je 76 procenata i opala je za dva odsto u odnosu na 2006. godinu. Procenjuje se da je zbog ovako visoke stope piraterije domaća ekonomija pretrpela gubitke od 72 miliona dolara, uglavnom kroz nenaplaćena poreska potraživanja.[156] Ova studija, nažalost, nije dala procenu koliko je novih radnih mesta moglo biti otvoreno, niti koliko je zaposlenih u preduzećima koja se bave prodajom filmskih i muzičkih izdanja i softvera zbog toga izgubilo radno mesto. Nedavno je iz beogradskih bioskopa povučen film „Righteous Kill" zbog činjenice da se isti naslov našao u uličnoj prodaji nekoliko meseci pre početka njegovog prikazivanja. Šteta koju trpe distributeri usled izmakle dobiti od bioskopske eksploatacije i prodaje legalnih kopija velika je, a gubici koji nastaju neminovno vode ka gašenju njihove delatnosti.

Izvršiocima krivičnih dela protiv intelektualne svojine sudovi najčešće izriču uslovne kazne zatvora, mada je u 2008. godini Posebno odeljenje Okružnog suda u Beogradu osudilo dvojicu izvršilaca na zatvorske kazne, i to okrivljenog Ž. D. presudom K1 16/08 na kaznu zatvora u trajanju od šest meseci, a okrivljenog M. J. presudom K1 17/08 na kaznu zatvora u trajanju od jedanaest meseci. Ova lica su bila višestruki povratnici, a ranije su osuđivani isključivo zbog izvršenih krivičnih dela protiv intelektualne svojine.

Interesantan je i primer presude Okružnog suda u Beogradu K1 VTK broj 19/08, kojom su okrivljeni J. Ž. i M. S. osuđeni na uslovnu kaznu zatvora u trajanju od šest meseci sa rokom proveravanja od dve godine jer su u periodu od 21. juna 2005. godine do kraja novembra 2007. godine u prostorijama preduzeća „Excalibur net DOO Kraljevo" putem bežične internet mreže neovlašćeno stavili u promet preko 500 primeraka autorskih dela – filmova, muzike i softvera, u nameri da time pribave sebi imovinsku korist, na taj način što su na FTP servere preduzeća „Excalibur net DOO Kraljevo" postavljali autorska dela – filmove, muziku, računarske programe i druge multimedijalne sadržaje i korisnicima internet usluga koje je pružalo njihovo preduzeće, za mesečnu naknadu od 10 do 20 evra, omogućavali da preuzimaju navedene sadržaje.

Iz uporednopravne prakse možemo izdvojiti nedavni primer kada je sud u Švedskoj osudio četvoricu vlasnika čuvene stranice pajratbej – „The Pirate Bay" na kazne zatvora od po godinu dana, s tim što im je naloženo da plate odštetu od tri i po miliona dolara kompanijama kao što su Warner Brothers,

[156] „Softverska piraterija oštetila budžet za 72 miliona dolara", *Danas,* 29. 5. 2008, internet, *http://www.danas.rs/vesti/ekonomija/softverska_piraterija_ostetila_budzet_za_72_miliona_dolara.4.html?news_id=92482,* 10. 5. 2009.

Sony i EMI.[157] Na navedenoj stranici se nezakonito razmenjuju muzika, filmovi i kompjuterske igrice, a ima oko 22 miliona korisnika.[158]

Pirateriju je skoro nemoguće iskoreniti, ali je merama države i zajedničkim delovanjem pravosuđa i policije moguće suzbiti taj vid kriminalnih aktivnosti, što prema evropskom proseku iznosi 30 odsto.

1.1.3. Ostala krivična dela

Prevara – član 208 Krivičnog zakonika

Krivično delo *Prevara* izvršava lice koje u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist dovede koga lažnim prikazivanjem ili prikrivanjem činjenica u zabludu ili ga održava u zabludi i time ga navede da ovaj na štetu svoje ili tuđe imovine nešto učini, ili ne učini, a zaprećena je novčana kazna ili zatvor do tri godine. U stavu 2 propisan je privilegovan oblik ovog krivičnog dela, kada je izvršilac imao samo nameru da drugog ošteti, za šta je zaprećena novčana kazna ili zatvor do šest meseci. Prevara ima i dva kvalifikovana oblika kada pribavljena imovinska korist ili iznos štete prouzrokovane radnjama opisanim u st. 1 i 2 prelazi četiristo pedeset hiljada dinara, za šta je propisana kazna zatvora od jedne do osam godina, odnosno kada ovaj iznos prelazi milion petsto hiljada dinara, za šta je propisana kazna zatvora od dve do deset godina.

Radnja krivičnog dela je navođenje nekog lica da učini, ili ne učini, nešto što je štetno za njegovu ili tuđu imovinu. Navođenje predstavlja stvaranje odluke kod drugog da preduzme neku aktivnost, odnosno da se uzdrži od toga i ono mora biti usmereno na imovinu. Uslov za postojanje ovog krivičnog dela jeste da je oštećeni pod uticajem pogrešno stvorene predstave o nekoj činjenici nešto učinio ili propustio da učini i time naneo štetu svojoj ili tuđoj imovini. Neophodno je utvrditi i nameru izvršioca krivičnog dela, koja se sastoji u pribavljanju sebi ili drugome protivpravne imovinske koristi. Izvršilac krivičnog dela može biti svako lice koje mora postupati sa umišljajem.[159]

Globalna računarska mreža predstavlja novu oblast delovanja izvršilaca krivičnih dela, koji na prevaran način ostvaruju imovinsku korist. Iako pojava interneta nije donela oblike prevara koji nisu postojali i ranije, stvorila je neograničene mogućnosti za njihovo vršenje, jer je učinila dostupnim daleko

[157] „Osuđeni osnivači Pirate Bay-a“, BBC Serbian, internet, *http://www.bbc.co.uk/serbian/news/2009/04/090417_swedennetpiracy.shtml,* 10. 5. 2009.

[158] Vesna Knežević-Ćosić, „Švedski pirati na naftnoj platformi prave piratsku državu“, *Borba*, 23. 4. 2009, internet, *http://www.borba.rs/content/view/5127/36/,* 10. 5. 2009.

[159] Ljubiša Lazarević, *Komentar Krivičnog zakonika Republike Srbije,* Savremena administracija, Beograd, 2006, str. 585.

veći broj potencijalnih žrtava i skoro sasvim eliminisala troškove koji su potrebni za organizovanje ovog krivičnog dela. O tome nam govori intervju jednog od prevaranata putem interneta, koji je na pitanje novinara o visini troškova izvođenja jedne prevare odgovorio: „Dva dolara! Jedan dolar da se plati sat interneta u kafeu i jedan dolar da se popije kafa.“[160]

Izvršioci se služe pogodnošću da im internet pruža skoro potpunu anonimnost, kao i činjenicom da je digitalne finansijske tokove, koji obično vode preko više država, veoma teško pratiti i utvrditi krajnju destinaciju sredstava. Sociološki profili oštećenih se veoma razlikuju, a žrtva prevare izvršene putem interneta može postati gotovo svako, zbog čega je neophodno uvek biti na oprezu, jer izvršioci ovakvih krivičnih dela usavršavaju načine obavljanja svojih kriminalnih aktivnosti i menjaju ciljne grupe svog delovanja. Grupe ovih kriminalaca su veoma dobro organizovane, specijalizovane su za određene regione, a da bi prevare putem interneta bile uspešne, služe se najrazličitijim metodama za pribavljanje podataka o potencijalnim žrtvama i sklapanje njihovog sociološkog profila. Najbolji izvor informacija predstavljaju sami oštećeni, koji posetom lažnim reklamnim sajtovima, ili odgovorom na posebnu vrstu reklamnih imejl poruka, tzv. spam, ostavljaju svoje lične podatke, a na osnovu prikupljenih materijala pravi se mehanizam prevare.

Od brojnih načina prevara putem interneta izdvojićemo nigerijsko pismo, koje predstavlja sinonim za lažne imejl poruke u kojima potencijalna žrtva dobija različita obaveštenja:

- da joj je neka bliska osoba u inostranstvu i da se nalazi u nevolji, zbog čega je neophodno poslati joj određen novčani iznos;
- o nasledstvu za koje je potrebno platiti takse – pismo u kome se traži pomoć za transfer novčanog iznosa za koji „pomoćnik“ dobija veliku proviziju;
- povoljna ponuda za atraktivan posao;
- ponuda za sklapanje braka.

Da su prevare putem interneta prisutne i u Srbiji govori nam primer dvoje naših građana, koji su na ovakav način oštećeni za više hiljada evra, s tim što organizatori prevare još nisu otkriveni. Oštećeni su elektronskom poštom primili obaveštenje da su u inostranstvu dobili milionske novčane nagrade. Nakon što su odgovorili na inicijalne poruke, oštećenima su poslata detaljnija obaveštenja o načinu podizanja dobitka, obrasci ugovora koje je trebalo popuniti, uputstva za otvaranje računa u inostranstvu na koji će nagrada biti

[160] „Nigerijska šema (šema 419)“, prevara.info, internet *http://www.prevara.info/index.php?option=com_content&task=view&id=42&Itemid=7*, 11. 5. 2009.

uplaćena, čak i aktivacioni kodovi za račune na kojima se nalazi novac, podaci o ljudima koji su navodno već dobijali nagrade na ovakav način, ali i iznos „takse“ i broj računa na koji je neophodno izvršiti uplatu kako bi nagrada bila isplaćena. Kada bi oštećeni uplatili tražene iznose, njihova novčana sredstva su preusmeravana na više drugih računa u inostranstvu, što je praćenje ovakvog novčanog toka učinilo nemogućim.

Poseban način za sticanje protivpravne imovinske koristi predstavlja i kreiranje lažnih veb sajtova namenjenih kupovini robe. Pred Posebnim odeljenjem Okružnog suda u Beogradu za borbu protiv visokotehnološkog kriminala u toku je krivični postupak protiv šestoro lica koja su tokom 2003. godine napravila sajt *www.escroweurope.net* dovodeći izgledom, sadržinom i adresom navedene internet stranice oštećene u zabludu da komuniciraju sa legalnim *escrow* servisom koji pruža uslugu posredovanja prilikom obavljanja robnonovčanih transakcija na internetu, koje se realizuju tek nakon isporuke predmeta kupoprodaje. Okrivljeni su objavljivali oglase neistinitog sadržaja i lažnim prikazivanjem činjenica da kao prodavci poseduju određenu robu koju će nakon izvršenog plaćanja isporučiti kupcu, odnosno da će kao navodni kupci naručenu i isporučenu robu prodavcu platiti, dovodili i održavali u zabludi veći broj oštećenih američkih državljana i time ih navodili da im na štetu svoje imovine putem specijalizovanih servisnih službi „DHL“, „FedEx“, ili „UPS“ pošalju određenu robu, odnosno da im kao kupci plate robu koju okrivljeni kao navodni prodavci nisu ni posedovali, što su oštećeni činili putem servisa za transakciju novca „Western Union“, ili upotrebom kreditnih kartica. Vrednost stvari i novca, koju su okrivljeni pribavili na ovakav način, iznosi više desetina hiljada evra.

Falsifikovanje i zloupotreba platnih kartica – član 225 Krivičnog zakonika

Stavom 1 propisano je da ovo krivično delo čini onaj ko napravi lažnu karticu ili ko preinači pravu platnu karticu u nameri da je upotrebi kao pravu ili ko takvu lažnu karticu upotrebi kao pravu, a zaprećena je kazna zatvora od tri meseca do tri godine. U st. 2 i 3 propisani su kvalifikovani oblici, kada je izvršenjem ovog krivičnog dela pribavljena protivpravna imovinska korist, za šta je zaprećena kazna zatvora od šest meseci do pet godina**,** a ako visina ove koristi prelazi iznos od milion petsto hiljada dinara, učinilac će se kazniti zatvorom od dve do deset godina. Stav 4 predviđa kažnjavanje učinioca koji delo iz st. 2 i 3 učini neovlašćenom upotrebom tuđe kartice. U stavu 5 propisano je da će se lice koje nabavi lažnu platnu karticu u nameri da je upotrebi kao pravu, odnosno koje pribavlja podatke u nameri da ih is-

koristi za pravljenje lažne platne kartice, kazniti novčanom kaznom ili zatvorom do jedne godine.

Propisivanjem ovog krivičnog dela zakonodavac je imao nameru da zaštiti platne kartice kao sredstvo koje se koristi u platnom prometu i ima istu funkciju kao novac.

Radnja krivičnog dela je propisana alternativno kao pravljenje lažne platne kartice, preinačavanje prave platne kartice u nameri da se upotrebi kao prava ili upotreba lažne platne kartice. Pravljenje podrazumeva izradu lažne platne kartice od predmeta koji nije platna kartica korišćenjem određenih uređaja i procesa, a preinačenje znači prepravljanje prave platne kartice. Upotreba podrazumeva stavljanje takvih kartica u promet i njihovo korišćenje, npr. na bankomatima, u prodavnicama ili plaćanjem preko interneta. U pogledu vinosti potreban je umišljaj, a delo je svršeno kada je lažna platna kartica napravljena, ili je prava preinačena u nameri upotrebe ili kada je upotrebljena. Izvršilac može biti svako lice, ali po prirodi stvari lice koje pravi ili preinačava pravu platnu karticu mora posedovati određena znanja i tehničke uređaje za to. Stav 4 ovog člana sankcioniše neovlašćenu upotrebu tuđe kartice. Stav 5 inkriminiše nabavljanje lažne platne kartice u nameri njene upotrebe kao prave ili pribavljanje podataka u nameri da se oni iskoriste za pravljenje lažne platne kartice.[161]

Za dokazivanje ovog krivičnog dela potrebno je utvrditi vreme i mesto izvršenja, da li je kartica koja je upotrebljena lažna, na koji način je napravljena i uz pomoć kojih tehničkih uređaja. Naročito je potrebno obratiti pažnju na moguće radnje saučesništva, jer ovo krivično delo i njegove radnje, kao i način njegovog izvršenja, mogu obuhvatati više lica sa različitim zaduženjima u okviru kriminalne grupe – nabavka blanko kartica, nabavka uređaja, nabavka kodova, izrada lažnih platnih ili preinačenje pravih platnih kartica, kasnija upotreba u prometu ili distribucija radi upotrebe u prometu itd. Kada je izvršeno krivično delo iz stava 1, neophodno je utvrditi nameru učinioca da preinačenu platnu karticu upotrebi kao pravu. Potrebno je, ukoliko je moguće, utvrditi i kada i gde su ovakve kartice upotrebljene, kao i visinu štete koja je pričinjena njihovom upotrebom. Kada su izvršena krivična dela iz st. 2 i 3, potrebno je utvrditi da li je i u kom iznosu pribavljena protivpravna imovinska korist. Za krivično delo iz stava 4 potrebno je utvrditi način pribavljanja i korišćenja takve kartice i da li je izvršilac postupao neovlašćeno. Za krivično delo iz stava 5 potrebno je utvrditi na koji način je nabavljena lažna platna kartica, da li je nabavljena u nameri upotrebe, te koji podaci su nabavljeni, na

[161] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 149.

koji način, krug lica, da li su nabavljeni u nameri pravljenja lažnih platnih kartica, te na koji način, od strane koga i gde je takve kartice trebalo da budu napravljene.[162]

Upotreba platnih i kreditnih kartica godinama beleži konstantan rast. Da plastični novac polako zamenjuje papirni, govori nam podatak da je tokom 2008. godine u Srbiji registrovano oko 5,8 miliona platnih kartica i preko njih je u prvih devet meseci ove godine ostvaren rekordni promet od oko 250 milijardi dinara.[163]

Sa porastom broja platnih kartica i prometa koji se preko njih odvija, zloupotreba platnih kartica postala je jedno od najzastupljenijih krivičnih dela iz oblasti visokotehnološkog kriminala. Povećanje broja krivičnih dela ove vrste, ipak, nije u srazmeri sa povećanjem broja platnih kartica, s obzirom na to da je u našoj zemlji ustanovljen veoma dobar pravnoinstitucionalni okvir za sprečavanje ovakvih zloupotreba, koji čine Forum za prevenciju zloupotrebe platnih kartica pri Privrednoj komori Srbije, policijski i pravosudni organi. Treba napomenuti i da banke imaju svoje centre koji 24 časa vrše monitoring prometa platnim karticama, dok je pri Narodnoj banci Srbije formiran Nacionalni centar za platne kartice.

Kako smo već napomenuli, za izvršenje ovih krivičnih dela potrebna je dobra organizacija, a radnja krivičnog dela se odvija u nekoliko faza. Do zloupotrebe platnih kartica dolazi tako što izvršioci prvo nabavljaju podatke sa kartica služeći se raznim prevarnim metodama (skimovanje, krađa pin kodova, libanska kragna), zatim iste podatke prodaju preko interneta „krajnjim korisnicima" koji prave falsifikovane kartice nanoseći ukradeni zapis na tzv. „bele" kartice. Ovakve kartice se uglavnom ne koriste u zemljama u kojima su podaci ukradeni, pa su u praksi izvršioci ovih krivičnih dela najčešće stranci. Falsifikovane kartice se najčešće koriste na bankomatima.

Postoji nekoliko načina za pribavljanje podataka sa platnih i kreditnih kartica.

Fišing (engl. Phishing)

Predstavlja pribavljanje poverljivih informacija kao što su korisnička imena, lozinke ili detalji o kreditnim karticama, korišćenjem lažnih imejl poruka, odnosno postavljanjem lažnih veb sajtova. Poruka koju oštećeni dobija od „banke" sadrži obaveštenje i link koji vodi ka lažnom veb sajtu, identič-

[162] Grupa autora, *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*, Savet Evrope, 2008, str. 150.

[163] „U Srbiji registrovano 5,8 miliona platnih kartica", *Biznis novine,* 11. 11. 2008, internet, *http://www.biznisnovine.com/cms/item/stories/sr.html?view=story&id=24555*, 11. 5. 2009.

nom sajtu njegove banke. Kada pristupi takvom sajtu, od korisnika se traži da ostavi lične podatke, broj platne ili kreditne kartice, kao i njen pin kod.[164] Kriminalci se služe neznanjem žrtava, odnosno činjenicom da one ne proveravaju poreklo poruke, niti zapažaju tako očigledne stvari kao što je domen sajta na koji je doveden, npr. www.banka.com umesto www.banka.net. Mnogi antivirusni programi imaju antispam filtere koji sprečavaju da ovakve neželjene poruke dođu do klijenata, ali postoje i posebni programi koji proveravaju elektronske poruke, odnosno koji u sebi imaju baze podataka o lažnim sajtovima.

Farming (engl. Pharming) – redirekcija, preusmeravanje

Sofisticiraniji način pribavljanja podataka nego što je to fišing. Slično opisanom metodu i ovde se potencijalne žrtve preusmeravaju na klonirane veb sajtove koje je veoma teško razlikovati od pravih. Tehnika koja se primenjuje naziva se maskiranje (engl. *spoofing*) domena, a brauzer (engl. *browser*) će pokazati da se korisnik nalazi na pravoj adresi.[165] Ovi napadi se realizuju preko kompromitovanja *domain name* sistema (DNS) koji pretvara veb i imejl adrese u numeričke nizove. Kada se ovaj sistem izmeni tako da sadrži lažne informacije o tome koja veb adresa odgovara kojem nizu brojeva, svi korisnici koji otkucaju odgovarajuću (ispravnu) veb adresu biće preusmereni na lažnu.[166]

Skimovanje (engl. Skiming)

Vrlo jednostavna tehnika koju može primeniti svako ko dođe u kontakt sa karticom – prodavac, radnik na benzinskoj pumpi, konobar u restoranu, a poseduje skimer – čitač magnetnog zapisa. Dovoljno je da kartica bude provučena kroz ovaj mali aparat i da podaci sa nje budu očitani. Postoji mogućnost da se skimer postavi i u bankomat, s tim što tada treba postaviti i skrivenu kameru koja će snimiti pin kod koji unosi oštećeni.

Libanska kragna

U otvor za karticu bankomata postavlja se štipaljka koja zaglavljuje karticu. Tada oštećenom prilazi „slučajni prolaznik“ koji nudi pomoć i predlaže

[164] „Phishing“, Wikipedia, internet, *http://en.wikipedia.org/wiki/Phishing,* 11. 5. 2009

[165] „Pharming“, Webopedia, Internet, *http://www.webopedia.com/TERM/p/pharming.html,* 11. 5. 2009.

[166] Dušan Katilović, „Ekstenzivni uzgoj žrtava“, *Svet kompjutera,* 2005, internet, *http://www.sk.co.yu/2005/04/skin06.html,* 11. 5. 2009.

oštećenom da ponovo ukuca pin kod. Po odlasku oštećenog kriminalac vadi karticu iz bankomata i nastavlja da je koristi.

Do podataka sa kartica može se doći i upotrebom hakerskih alata, kada se u računar oštećenog ubaci maliciozni program, tzv. trojanac, što se najčešće čini elektronskom poštom, a koji snima ekran monitora oštećenog i aktivnosti njegove tastature, o čemu obaveštava pošiljaoca poruke.

Zloupotrebom platnih kartica kriminalci mogu doći do velikih novčanih svota. Njihovo delovanje često ostaje neotkriveno jer izvršioci ovih krivičnih dela od velikog broja oštećenih uzimaju male iznose 5–10 evra, pa oštećeni i ne primete da su im sa računa skinuta sredstva ili takve transfere tretiraju kao neku vrstu bankarske takse. Kako bi sprečili eventualne zloupotrebe, korisnici „plastičnog novca" trebalo bi da se pridržavaju detaljnih uputstava za bezbedno korišćenje kartica koje donosi svaka banka.

Izazivanje nacionalne, rasne i verske mržnje i netrpeljivosti – član 317 Krivičnog zakonika

Stavom 1 ovog člana predviđeno je kažnjavanje lica koje izaziva nacionalnu, rasnu ili versku mržnju ili netrpeljivost među narodima ili etničkim zajednicama koje žive u Srbiji, a propisana je kazna zatvora od šest meseci do pet godina. U stavu 2 propisani su kvalifikovani oblici krivičnog dela iz stava 1 kada je ono učinjeno prinudom, zlostavljanjem, ugrožavanjem sigurnosti, izlaganjem poruzi nacionalnih, etničkih ili verskih simbola, oštećenjem tuđe stvari, skrnavljenjem spomenika, spomen-obeležja ili grobova. Zaprećena je kazna zatvora od jedne do osam godina. U stavu 3 propisan je najteži oblik kada se delo iz st. 1 i 2 vrši zloupotrebom službenog položaja ili ovlašćenja, ili ako je usled tih dela došlo do nereda, nasilja ili drugih teških posledica za zajednički život naroda, nacionalnih manjina ili etničkih grupa u Srbiji, a zaprećena kazna za delo iz stava 1 je zatvor od jedne do osam godina, dok je za delo iz stava 2 propisan zatvor od dve do deset godina.

Radnja krivičnog dela iz stava 1 određena je kao izazivanje mržnje – stvaranje do tada nepostojeće mržnje, odnosno raspirivanje – razvijanje i produbljivanje već postojećih osećanja, a što se može postići vređanjem, ismejavanjem ili potcenjivanjem nacionalnih, rasnih ili verskih osećanja, izlaganjem poruzi simbola, nipodaštavanjem istorijskih, kulturnih i drugih vrednosti.[167] Krivično delo postoji samo ako su pobrojane delatnosti usmerene na nacionalnu, versku ili rasnu pripadnost, s tim što broj lica prema kojima su radnje

[167] Ljubiša Lazarević, *Komentar Krivičnog zakonika Republike Srbije,* Savremena administracija, Beograd, 2006, str. 782.

preduzete nije od značaja, tačnije delo će postojati ako je izvršeno i prema samo jednom licu.

Kvalifikatorne okolnosti ovog dela opisane u stavu 2 predstavljaju način na koji je delo izvršeno, a to može biti prinudom, zlostavljanjem, ugrožavanjem sigurnosti, skrnavljenjem spomenika, spomen-obeležja ili grobova, njihovim oštećenjem. Kvalifikatorne okolnosti opisane u stavu 3 jesu svojstvo izvršioca i način izvršenja, odnosno teže posledicama kao što su neredi ili nasilje.[168]

Zloupotreba interneta predstavlja veoma pogodno sredstvo za izazivanje nacionalne, rasne i verske mržnje. Izvršioci ovog dela mogu uz male troškove da otvore veb sajt ili da potpuno besplatno naprave blog, gde bez ikakvog ograničenja iznose rasističke stavove, vređaju ili ismejavaju druge narode i etničke zajednice, što za posledicu može imati izazivanje mržnje ili njeno raspirivanje. Posredstvom interneta ovakvi stavovi mogu doći do neograničenog broja ljudi, što njihovo delovanje čini naročito opasnim. Krivično delo može izvršiti i samo jedno lice, ali to danas uglavnom čine različita udruženja i organizacije. Definisanje i označavanje organizacija koje imaju za cilj stvaranje nacionalne, verske i rasne mržnje veoma je teško, a često se svodi na pitanja dnevne politike.

U bivšoj SFRJ postojala su udruženja i politički pokreti čiji je rad bio zabranjivan sa različitim obrazloženjima, a sa početkom raspada te države dolazi do pojave ekstremističkih političkih stranaka čije je delovanje usmereno na izazivanje i raspirivanje međunacionalne mržnje, iako u njihovim programima najčešće nisu postojale odredbe kojima su drugi narodi omalovažavani.

Jedan od najpoznatijih internet foruma koji mnoge organizacije opisuju kao neonacistički i optužuju ga da promoviše ideje rasizma, govor mržnje i nasilje jeste „Stormfront". Na ovom forumu su dostupni regionalno-jezički potforumi, među kojima je jedan od najaktivnijih po broju diskusija i postova „Stormfront Srbija", sa preko 88.000 postova, a odmah iza njih po brojnosti su posetioci iz Hrvatske.[169]

U Srbiji postoji više organizacija i udruženja građana čije delovanje i stavovi koje propagiraju mogu izazvati sumnju u pogledu njihove legalnosti. Prema podacima Ministarstva unutrašnjih poslova, na teritoriji Srbije u takve ekstremističke organizacije ubrajaju se: „Nacionalni stroj", „Krv i čast", „Skinhedsi", „Rasni nacionalisti-rasonalisti" i „Otačastveni pokret Obraz".[170]

---

[168] Ljubiša Lazarević, *Komentar Krivičnog zakonika Republike Srbije,* Savremena administracija, Beograd, 2006, str. 783.

[169] „Stormfront", Wikipedia, internet, *http://sr.wikipedia.org/sr-el/%D0%A1%D1%82%D0%BE%D1%80%D0%BC%D1%84%D1%80%D0%BE%D0%BD%D1%82,* 11. 5. 2009.

[170] „Inicijativa za zabranu delovanja Nacionalnog stroja", *Politika,* 15. 10. 2008, internet,

Do sada nije bilo zabrane nijedne organizacije zbog rasističkih stavova ili širenja verske i nacionalne mržnje, mada je Republičko javno tužilaštvo u oktobru 2008. godine uputilo inicijativu Ustavnom sudu Srbije za zabranu rada i delovanja organizacije „Nacionalni stroj". Članove ove grupe je u novembru 2006. godine osudio Okružni sud u Novom Sadu na kazne u rasponu od uslovnih do osam meseci zatvora, a njenog vođu D. G. na godinu dana zatvora.

Delovanje sajtova nacionalističkih organizacija i njihovih foruma ne može se blokirati, jer su uglavnom registrovani na serverima u inostranstvu, a pojedini sajtovi omogućavaju postavljanje stranice sa garancijom da je server anoniman, što omogućuje i anonimnost IP adrese. Ove organizacije najčešće svoje sajtove postavljaju u SAD, koje zbog svojih zakonskih odredaba o slobodi govora i izražavanja odbijaju da dostave podatke o licima koja su ih postavila ili ih administriraju. Jedna od najstarijih rasističkih organizacija „Kju kluks klan" (engl. *Ku klux klan*), nastala još u XIX veku i danas deluje u SAD, a svoje stavove propagira i preko interneta. Ova organizacija zagovara nadmoćnost „bele rase" nad ostalim rasama: crncima i hispanosima (Meksikancima, Kubancima, Urugvajcima i Portorikancima), kao i antisemitizam, mržnju prema katolicima (ovo se naročito odnosi na imigrante iz Poljske, Italije i Irske) i homofobiju. Poznata je po zastrašivanju i surovim egzekucijama koje su u prošlosti sprovodili njeni članovi. Imala je veliki broj pristalica, ali je s vremenom njen značaj opadao a broj njenih članova sveo se na 5.000 do 8.000.[171]

Definisanje granice između slobode govora i „govora mržnje, koji u sebi sadrži elemente ovog krivičnog dela jeste pitanje na koje će pravna teorija tek morati da pruži odgovor. S obzirom na delikatnost ovog problema, potrebno je biti veoma oprezan prilikom označavanja neke organizacije kao političke ili rasističke i u svakom konkretnom slučaju utvrditi okolnosti koje su pratile izvršenje eventualnog krivičnog dela, prikupiti validne dokaze, ali i utvrditi umišljaj učinilaca. Zabrana rada neke organizacije može biti okarakterisana kao uskraćivanje političkih prava i ograničavanje slobode govora, pa je potrebno ustanoviti jasnu razliku između političkih partija sa ekstremnim stavovima od delovanja organizacija čiji je cilj širenje rasne, nacionalne i verske mržnje. Sprečavanje izvršenja ovog krivičnog dela je problem koji zahteva angažovanje celokupnog društva, naročito obrazovnog sistema, jer primena isključivo represivnih mera u borbi protiv izazivanja nacionalne, rasne i verske mržnje ne može postići zadovoljavajuće rezultate.

---

http://www.politika.rs/rubrike/Hronika/Inicijativa-za-zabranu-delovanja-Nacionalnog-stroja.lt.html, 11. 5. 2009.

[171] „Ku Klux Klan", Wikipedia, internet, *http://sh.wikipedia.org/wiki/Ku_Klux_Klan*, 11. 5. 2009.

1.2. Podzakonski akti

1.2.1. Pravilnik o uslovima za pružanje Internet usluga i ostalih usluga prenosa podataka i sadržaju odobrenja

Pravilnikom koji je u okviru svojih nadležnosti usvojila Republička agencija za telekomunikacije utvrđeni su osnovni tehnički i drugi uslovi za pružanje internet usluga i ostalih usluga prenosa podataka, kao i način izdavanja i sadržaj odobrenja za obavljanje ove delatnosti.[172] Ovim pravilnikom utvrđeno je i značenje pojedinih izraza koji su u vezi za pružanjem internet usluga pa se tako pod pojmom „Internet" podrazumeva globalni elektronski komunikacioni sistem međusobno povezanih računarskih mreža i uređaja, namenjen razmeni svih vrsta informacija u skladu sa internet standardima. Pravilnik pod „Internet standardima" smatra dokumente koji se odnose na koncepte, procedure umrežavanja, protokole, interfejse i metode identifikacije u okviru interneta. „Internet usluge" su javne telekomunikacione usluge prenosa podataka koje se realizuju u skladu sa internet standardima i za čije je ostvarivanje neophodna upotreba javnih IP adresa, osim komercijalnih usluga prenosa govora, radio i televizijskih programa u realnom vremenu. Konačno, „IP adresa" je numerički identifikator, koji jednoznačno identifikuje mrežu ili pristupnu tačku u sklopu interneta, a za čije je dodeljivanje na svetskom nivou nadležna organizacija *Internet Assigned Numbers Authority* (IANA).

Pravilnik u članu 15, stav 7 sadrži i obavezu za imaoca odobrenja da o svom trošku obezbedi opremu, uređaje i instalacije, koji će omogućiti čuvanje relevantnih podataka najmanje šest meseci, a najviše dve godine, pristup tim podacima nadležnim državnim organima i elektronski nadzor u slučajevima predviđenim zakonom, na način i u obimu kako je predviđeno odgovarajućim propisima. Ovde je zapravo reč o obavezi internet provajdera da određene podatke o izvršenoj komunikaciji „zadrže" određeno vreme i da ih, po zahtevu organa otkrivanja ili gonjenja, dostave radi vođenja krivičnog postupka. Podaci koji su ovde u pitanju trebalo bi da budu oni koje predviđa Direktiva EU o „čuvanju podataka" (o kojoj je već bilo reči), međutim, u primeni ove odredbe moglo bi da dođe do problema koji bi bili izazvani nejasnom definicijom vrste i kvaliteta podataka koje je neophodno sačuvati. Naime, navedena odredba ne pruža pouzdan osnov državnim organima za borbu protiv visokotehnološkog kriminala za prikupljanje svih potrebnih dokaza u vezi sa izvršenjem krivičnih dela iz ove oblasti. Rok od šest meseci je neprimereno kratak, a još veći problem predstavlja sloboda tumačenja ove obaveze koja

[172] „Pravilnik o uslovima za pružanje Internet usluga i ostalih usluga prenosa podataka i sadržaju odobrenja", „Službeni glasnik RS", broj 100/08.

je ostavljena internet provajderima, i to u pogledu podataka koje je neophodno sačuvati imajući u vidu formulaciju koja se koristi – relevantni podaci. To u praksi znači da državni organi ne mogu sa sigurnošću očekivati da će u postupanju u okviru konkretnog krivičnog predmeta moći da pribave sve neophodne dokaze budući da to umnogome zavisi od poimanja pojma relevantan podatak svakog pojedinačnog internet provajdera. U praksi pojedinih evropskih zemalja, koje mnogo više pažnje posvećuju preciznosti u regulisanju ovih pitanja, obaveza internet provajdera je uspostavljena imperativnim odredbama[173] ili komercijalizacijom[174] ove obaveze, ali u svakom slučaju daje veće mogućnosti nadležnim organima u pogledu prikupljanja relevantnih elektronskih dokaza.

1.2.2. Pravilnik o uslovima za pružanje usluga prenosa govora korišćenjem Interneta i sadržaju odobrenja

Ovim pravilnikom Republičke agencije za telekomunikacije utvrđuju se uslovi neophodni za pružanje usluga prenosa govora korišćenjem interneta (VoIP), na komercijalnoj osnovi i bez dodeljivanja posebnih brojeva operateru za potrebe krajnjih korisnika.[175]

VoIP obuhvata sledeće načine govorne komunikacije putem interneta:

- *računar/IP telefon – računar/IP telefon*, odnosno između računara/IP telefona jednog i drugog korisnika;
- *računar/IP telefon – telefon*, odnosno između računara/IP telefona jednog korisnika i drugog korisnika koji koristi telefonski aparat koji je povezan na javnu telekomunikacionu mrežu u Srbiji;
- *telefon – telefon*, odnosno između korisnika koji koriste telefonske aparate povezane na javnu telekomunikacionu mrežu u Srbiji ili inostranstvu, gde se deo komunikacije obavlja preko interneta a deo preko javne telekomunikacione mreže.

Imajući u vidu ovako definisanu sadržinu pojma VoIP-a, odredbe ovog pravilnika ne odnose se na pružanje usluga prenosa govora u sledećim slu-

[173] U Norveškoj ne samo da je propisana obaveza internet provajdera u pogledu dostavljanja svih potrebnih podataka državnim organima već je, imajući u vidu da je prema norveškom zakonodavstvu kažnjiv i sam pristup internet sajtovima sa sadržajem dečje pornografije, obaveza internet provajdera da izrade filtere koji sprečavaju korisnike da pristupe ovakvim internet sajtovima i da ih konstantno dopunjuju novim adresama.

[174] U Francuskoj, u cilju olakšanja ove obaveze internet provajdera i smanjenja troškova postoji cenovnik prema kome, npr. dostavljanje podataka u vezi sa jednom IP adresom košta osam evra.

[175] „Pravilnik o uslovima za pružanje usluga prenosa govora korišćenjem Interneta i sadržaju odobrenja“, „Službeni glasnik RS“, broj 94/08.

jevima: unutar privatnih mreža fizičkih i pravnih lica isključivo za sopstvene potrebe i na osnovi koja nije komercijalna, korišćenja interneta kada se zahteva dodela posebnih brojeva iz Plana numeracije posebnim korisnicima, kao ni na komunikaciju *računar/IP telefon – računar/IP telefon*.

Kao i pravilnik koji se odnosi na pružanje internet usluga, i ovaj pravilnik u članu 13, stav 4 propisuje obavezu za davaoca usluge da o sopstvenom trošku obezbedi opremu, uređaje i instalacije, koji će omogućiti čuvanje relevantnih podataka, pristup tim podacima od strane nadležnog organa i elektronski nadzor u slučajevima predviđenim zakonom. Pored toga, VoIP operater dužan je da podatke o saobraćaju svojih krajnjih korisnika trajno obriše ili učini anonimnim kada isteknu rokovi koji definišu obavezu čuvanja. Kao mehanizam zaštite podataka o korisnicima i komunikaciji koju ostvaruju, operater je u obavezi da obezbedi uređaje, opremu, instalacije, procedure i internu organizaciju, što će garantovati zaštitu navedenih podataka i onemogućiti zloupotrebu od strane trećih lica.

Iz izloženog vidimo da se i Pravilniku o VoIP-u, načelno, može staviti ista primedba kao i Pravilniku koji se odnosi na pružanje internet usluga. Reč je, da podsetimo, o nejasnom pojmu „relevantni podatak“ i opasnosti da organi otkrivanja i gonjenja neće moći da dobiju elektronske dokaze neophodnog kvaliteta i sadržaja. Stoga je neophodno da se pojam relevantni podatak bliže odredi tako što će se odrediti kategorije i potkategorije podataka koji se čuvaju u zavisnosti od toga da li je reč o upotrebi interneta ili VoIP-a. Kao vodilja može da posluži kategorizacija podataka kako je izložena u Direktivi EU o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža. Da podsetimo, reč je o pet kategorija podataka, i to: podaci neophodni za pronalaženje i identifikaciju izvora komunikacije, za otkrivanje odredišta komunikacije, utvrđivanju datuma, vremena i trajanja komunikacije, za otkrivanje vrste komunikacije i za identifikaciju komunikacijske opreme korisnika ili njihove navodne opreme.

Konačno, nikako ne treba izgubiti iz vida da je isključivo reč o podacima *o prometu i lokaciji* pravnih i fizičkih lica i na uz to vezane podatke nužne za identifikaciju pretplatnika ili registrovanog korisnika, a *ne o podacima koji se odnose na sadržaj* elektronske komunikacije, kao ni na informacije do kojih se dolazi korišćenjem mreža elektronske komunikacije.

IV

PROBLEMI PRI PROCESUIRANJU DELA VISOKOTEHNOLOŠKOG KRIMINALA

SPECIFIČNOSTI PROCESUIRANJA DELA VISOKOTEHNOLOŠKOG KRIMINALA

Visokotehnološki kriminal je po mnogim svojstvima specifičan u odnosu na vršenje drugih krivičnih dela. Pre svega, reč je o relativno novoj pojavi. Do pre nekoliko godina zakonodavstva država nisu adekvatno reagovala na njegovu pojavu; danas su različita dela koja se mogu počiniti upotrebom računara deo mnogih pravnih sistema. Ipak, među rešenjima koja su upotrebljena ne postoji konzistentnost, a često ni minimum potrebne komplementarnosti kako bi se neko delo uspešno procesuiralo. Sa druge strane, visokotehnološki kriminal ima veoma izraženu nadnacionalnu dimenziju – dela te vrste se po pravilu vrše u međunarodnom prostoru, odnosno uključuju na direktan ili posredan način više država.

Osim pomenute Evropske konvencije o visokotehnološkom kriminalu, ne postoje drugi relevantni dokumenti koji bi imali obaveznu snagu. To je posebno važno kada se govori o nedostatku univerzalnog instrumenta međunarodnog prava u ovoj oblasti. Istovremeno, ne postoji ni jednoobrazna, nedvosmislena praksa nacionalnih sudova u vezi sa pojedinim veoma važnim pitanjima koja se tiču nadnacionalnog elementa, ali ni kada je reč o nekim praktičnim problemima koji su, čini se, neminovni prilikom procesuiranja ovih dela pred sudom.

Zbog svega navedenog, kao i mnogih drugih činjenica koje čine visokotehnološki kriminal specifičnim, postoji niz problema koji se javljaju prilikom istraživanja i procesuiranja ovih dela, od kojih ćemo na ovom mestu ukazati na neke koji imaju posebnu težinu i gotovo redovno se javljaju u praksi:

– *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 od-

ređenu 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 sudiće se u Austriji, ostalim okrivljenim u zemljama čiji su državljani. Situacija, međutim, ne mora uvek biti takva, a čak i ovaj slučaj povlači za sobom još jedno veliko pitanje, odnosno problem: kako goniti počinioce dela koje u državama čiji su državljani ili na čijoj su teritoriji izvršena nije kažnjivo? Odgovor je, nažalost, nikako. Ukoliko postoji mogućnost, država koja želi da zasnuje nadležnost može tražiti ekstradiciju, ali nijedan međunarodni dokument ne poznaje mogućnost ekstradicije u pomenutom slučaju. Ove „sigurne države" većinom imaju manjkavo zakonodavstvo, i to ne zbog svoje politike nekažnjavanja visokotehnološkog kriminala, već zbog neprepoznavanja društvene opasnosti koju on nosi. Jedan od rasprostranjenih razloga je i relativna nerazvijenost zemlje u pogledu savremenih tehnologija, nedostatak stručnjaka koji bi se mogli baviti ovom problematikom, kao i nedostatak političke volje da se na ovom polju nešto promeni.

– *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 tome 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? Odgovor bi bio: praktično nikakva. O tome se pre svega mora voditi računa prilikom odluke da li povesti sudski postupak, što nije uvek slučaj – pojedine države praktikuju veoma strogu kaznenu politiku kao deo preventive daljeg širenja visokotehno-

loškog kriminala u najširim krugovima stanovništva, tj. među onim delovima stanovništva koji se ne bave time radi sticanja određene materijalne koristi.

– Međutim, da bi se u samom postupku pravilno odvagale okolnosti slučaja, *sudija mora imati zavidno predznanje o stvarima o kojima je reč*. Isto se odnosi i na tužioca, kao i na ostale državne institucije koje učestvuju u postupku. Ipak, gotovo nijedna država ne poznaje specijalizaciju i posebnu obuku sudija i ostalih učesnika u suzbijanju visokotehnološkog kriminala, iako je u mnogim postupcima praksa pokazala da veštaci ne mogu interpretirati činjenice na način koji bi sudija bez ikakvog predznanja mogao da shvati u dovoljnoj meri da na osnovu njih odluči o nečijoj krivičnoj odgovornosti.
– *Kako biti siguran ko je počinilac dela?* Iako ovo pitanje može delovati 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 da se mora veoma pažljivo postupati sa eventualnim osumnjičenima dok se ne dođe do nedvosmislenog saznanja da su oni na bilo koji način mogli biti umešani u izvršenje krivičnog dela. Slučajeve koji pripadaju „sivoj zoni", kada nije sasvim jasno da li je neka osoba izvršila delo samo zato što je verovatnije da je ona počinilac nego neko drugi, ko bi u teoriji mogao da ima i motiv, i sredstvo, i priliku, sudovi rešavaju u hodu, stvarajući zanimljivu praksu na koju se potonji delioci pravde mogu osloniti. Jedan od skorašnjih slučajeva u SAD to najbolje potvrđuje. Tamo je izvesni J. P. iz Ostina u Teksasu poslao imejl koji je sadržao pornografsku sliku maloletnika. Kada je utvrđena IP adresa sa koje je elektronska pošta poslata, policija je pretresla sobu njenog vlasnika, pomenutog J. P. Prilikom pretresa, pronašla je CD sa dečjom pornografijom i slučaj bi mogao da se smatra jednostavnim za rešavanje pred sudom da nije postojala i druga strana priče. Naime, J. P. je stan delio sa cimerom. Imejl adresa je, prema korisničkom imenu, zaista upućivala na to da je cimer njen vlasnik, ali je ovaj to negirao, a nije postojala mogućnost da se zaista utvrdi ko je otvorio imejl nalog. Istovremeno, pretresom nije bio uključen deo stana koji koristi cimer J. P. tako da se ne može sa sigurnošću tvrditi da li je on koristio i po-

sedovao dečju pornografiju. WiFi mreža preko koje se J. P. konektovao na internet bila je otvorenog karaktera, dakle bez zaštite i svako ko je fizički hvatao signal bežičnog interneta mogao je da ga koristi i da poseduje IP adresu koja je i dovela policiju do J. P. Postojale su, dakle, dve mogućnosti: jedna da je J. P. otvorio imejl nalog, koji je namerno podsećao na ime i prezime njegovog cimera, i koristeći svoju WiFi mrežu slao slike dečje pornografije. Druga mogućnost, koja je takođe u domenu realnosti, bila je da je cimer J. P., koristeći svoj nalog i nezaštićenu mrežu J. P., počinio ovo krivično delo. U drugom slučaju, J. P. bi svejedno bio osuđen za posedovanje dečje pornografije na CD-u koji je nađen, ali da li se cimer izvukao izvan domašaja pravde? Iako je J. P. svoju odbranu zasnovao na činjenici da se otvorena WiFi mreža može koristiti sa bilo kog računara, sud nije imao mnogo razumevanja za ovu odbranu i J. P. je osuđen pred osnovnim sudom, a presudu je potvrdio nadležni apelacioni sud, na skoro pet godina zatvora. Iako je faktička procena policije i tužioca bila da nema elemenata da se goni i cimer J. P., ostaje veliko pitanje da li je samo J. P. odgovoran, kao i još šira nedoumica – kako će precedent koji je sud u ovom slučaju doneo, da otvorena WiFi mreža nije opravdanje za njenu eventualnu zloupotrebu i korišćenje u ilegalne svrhe – dakle, da uvek odgovara pretplatnik?[176]

– U vezi sa prethodnim pitanjem se otvara 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 lokacija 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

[176] Više o ovom slučaju na internet adresi: *http://arstechnica.com/tech-policy/news/2007/04/child-porn-case-shows-that-an-open-wifi-network-is-no-defense.ars*, 1. 5. 2009.

ne može valjano proceniti da li se može prihvatiti kao dokaz, kao i težinu takvog dokaza?[177]

– 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, priroda visokotehnološkog kriminala je takva da je on „skriven" i da je potrebno veliko znanje i iskustvo da bi se uopšte percipirao.[178]
– *Kako uspostaviti efikasnu međunarodnu saradnju između različitih pravnih sistema širom sveta?* Globalni instrumenti međunarodnog prava koji bi regulisali saradnju u ovoj oblasti ne postoje; ono je ostavljeno na volju državama koje se različitim bilateralnim sporazumima i regionalnim konvencijama, poput one Saveta Evrope, mogu 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 ostvarivi kontakti i saradnja između relevantnih tela dveju ili više država, procedure su spore (visokotehnološki kriminal zahteva brzinu reagovanja) a rezultati neizvesni.

---

[177] 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*, 1. 3. 2009; *Electronic Crime Scene Investigation: A Guide for First Responders*, *http://www.ojp.usdoj.gov/nij,* 1. 5. 2009.

[178] 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*, 1. 3. 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*, 1. 5. 2009.

– *Kako postupati sa maloletnim učiniocima?* Naravno, sva zakonodavstva imaju posebnu regulativu u slučaju da su počinioci delimično ili potpuno neodgovorni sa stanovništa 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 kako i 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 koristile na početku razvoja zakonodavstava pojedinih država o visokotehnološkom kriminalu – kao što je kućni pritvor, jednostavno ne mogu biti efikasne. Zabrana „kontakta" osobe sa računarom je takođe besmislena, posebno kada se ima na umu hiperrazvoj ovih tehnologija i mogućnost da se mnoga od ovih dela izvrše i uz pomoć neke druge savremene naprave.
– Procesnopravne probleme ne možemo razmatrati 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 se razvijajati 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 priključio 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.*[179]

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 ove 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 za krivična dela protiv ustavnog uređenja i bezbednosti, kao i za krivična dela protiv čovečnosti i međunarodnog prava.

U ovakvoj situaciji, susretanje sa procesnopravni 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[180] 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

[179] Treba imati na umu 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.

[180] 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, treba imati na umu 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.

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.

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 biti od prvorazrednog značaja. Ovakve slučajeve višestruke nadležnosti sudova različitih država, isključivo specifične za *cyber*[181] *crime*, svojim odredbama nisu regulisali ni KZ ni ZKP.[182]

Nadnacionalni i transnacionalni karakter visokotehnološkog kriminala u praksi ne implicira isključivo probleme u pogledu pravilnog određivanja mesne nadležnosti. Prikupljanje dokaza, u cilju rasvetljivanja 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 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.

[181] Engleska reč izvedena od grčke Κυβερνήτης – kybernetes – uravljač, pilot, kormilar. U duhu srpskog jezika pravilno je izgovarati „kiber".

[182] Takva situacija, gde bi više od jedne države moglo da zahteva nadležnost, može biti veoma 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 broju informacionih sistema na globalnom nivou.

Zakon o pružanju međunarodne pravne pomoći u krivičnim stvarima,[183] 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[184] u postupanju od presudnog značaja za uspešno vođenje krivičnog postupka.

Osim što je previdео postojanje mreže 24/7,[185] zakon je propustio da predvidi i upotrebu modernih načina komuniciranja,[186] 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.

Jedan od potencijalnih procesnopravnih problema svakako bi mogao da bude problem nekažnjavanja i nepostojanja odgovornosti zbog izvršenih krivičnih dela iz oblasti VT kriminala, lica mlađih od 14 godina.[187] Pri postojanju argumentacije koja se tiče sve ubrzanijeg polnog i mentalnog sazrevanja ljudskih jedinki, te pri postojanju činjenice da su deca od 13 do14 godina, neretko, vrsni poznavaoci korišćenja IT-a, mišljenja smo da bi starosnu granicu krivične odgovornosti trebalo „spustiti" na odgovarajući kalendarski uzrast, a u prilog tome govori i statistika u pogledu kalendarskog uzrasta učinioca krivičnih dela uopšte. U sklopu navedenog, moralo bi se preispitati i pitanje stvarne nadležnosti sudova za suđenje maloletnim licima[188] zbog izvršenih krivičnih dela iz oblasti VT kriminala, s obzirom na to da u ovom trenutku pozitivnopravnim propi-

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

[184] 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.

[185] 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 trebalo bi da bude u stanju da obezbedi trenutnu pomoć u istragama i sudskim postupcima.

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

[187] Deca koja nisu krivično odgovorna.

[188] Kategorija lica od 14 do 18 godina.

sima ona nije data Posebnom odeljenju Okružnog suda u Beogradu za borbu protiv VT kriminala, pred kojim Posebno tužilaštvo za VT kriminal postupa.

Najzad, ne sporeći argumentaciju pravnog stava Vrhovnog suda Republike Srbije, u pravnom stavu iznetom u presudi Kzz. br. 10/06 od 16. 3. 2006. godine, da radnja izvršenja krivičnog dela Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199 KZ-a opisana u presudi,[189] mora biti 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, dužni su da u svojim pismenim aktima navedu sve naslove autorskih dela, pri čemu tužilaštvo i sud i podatke koji se odnose na oštećene 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.

Budući 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[190] kojim se definiše značenje izraza *spis, pismeno, pošiljka i drugi dokumenti*,[191] na koji način bi prepisi optužnih akata tužilaštva i odluka suda, osim eventualno izvornika, mogli biti u celosti, ili samo delom – i u elektronskoj formi. U tom smislu ova odredba morala bi pretrpeti određene izmene, utoliko što bi se u 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 biti i u pismenoj formi*. Ovakvo rešenje uvelo bi „na velika vrata" primenu elektronskog potpisa i elektronskog sertifikata, što podrazumeva ozbiljnu pripremu za njihovu primenu.

[189] Dakle, i u optužnim aktima tužilaštva.

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

[191] Spis, pismeno, pošiljka i drugi dokumenti mogu biti 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.

U sklopu drugih problema s kojima se u svakodnevnom radu susreću državni organi na suzbijanju 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 i dalje rezultat nedovoljnog postojanja svesti o opasnostima koje VT kriminal nosi i srazmerama štete koju prouzrokuje.

V

VISOKOTEHNOLOŠKI KRIMINAL U UPOREDNOM PRAVU

1. KRATKA ANALIZA ZAKONODAVSTAVA POJEDINIH ZEMALJA

Uporednopravna analiza ne može obuhvatiti sve zemlje koje su u poslednjih nekoliko godina aktuelizovale ovaj problem. Za razliku od stanja koje je postojalo doskora, danas u svetu gotovo da nema „sigurnih država" za savremene kriminalce. Ipak, razlike u stepenu implementacije su velike – dok neke države imaju posebno zakonodavstvo o visokotehnološkom kriminalu, koje podrazumeva i postojanje posebnih policijskih i drugih jedinica specijalizovanih za njegovo otkrivanje, neke zemlje su se zadovoljile opštim pristupom i uvođenjem pojedinih krivičnih dela koja se tiču nedozvoljene upotrebe savremenih tehnologija. Na ovom mestu ukazaćemo samo na neka od rešenja zemalja iz neposrednog okruženja, kao i zemalja koje imaju izuzetno razvijene sisteme za suzbijanje *cyber* zločina.

Internet je izvor velikog broja istraživanja nacionalnih zakonodavstava i međunarodnih organizacija o visokotehnološkom kriminalu. Pogledati, npr. *http://www.legi-internet.ro/en/laws.htm*, 1. 5. 2009. (ova internet stranica sadrži linkove prema svim važnijim odlukama međunarodnih organizacijama koje su na neki način povezane sa savremenim tehnologijama – posebno kada je reč o odlukama Evropske unije); *http://www.cybercrimelaw.net/*, 1. 5. 2009. (najnovije vesti kada je reč o međunarodnom pravu i nacionalnim zakonodavstvima u ovoj oblasti); *http://www.interpol.int/Public/TechnologyCrime/default.asp*, 1. 5. 2009. (deo internet prezentacije Interpola posvećen visokotehnološkom kriminalu); *http://www.mosstingrett.no/info/legal.html*, 1. 5. 2009. (pregled nacionalnih zakonodavstava; nažalost, predstavljeno je stanje iz 2003. godine, tako da se treba dodatno informisati o eventualnim promenama koje su u međuvremenu nastale).

Ako se pogleda uporedna analiza iz tabela 4.1-12., može se videti kako su države dostigle različite stepene razvoja zakonodavstva u oblasti visokotehnološkog kriminala.[192] Kao osnov za analizu poslužile su osnovne odredbe Evropske konvencije o visokotehnološkom kriminalu, koja je, kao što je ranije rečeno, otvorena i za vanevropske zemlje. Može se odmah videti da posto-

[192] Iako je ova analiza sprovedena pre svega u odnosu na implementaciju odredaba Evropske konvencije o visokotehnološkom kriminalu, treba naglasiti da su pojedine države u svojim zakonodavnim rešenjima otišle i dalje od standarda koji su njome ustanovljeni. Pogledati, npr. članak o novom zakonodavstvu Švedske, koje je direktno upereno na smanjenje internet piraterije: *Swedish traffic halves, no more pirating*, *http://www.rlslog.net/swedish-traffic-halves-no-more-pirating/*, 1. 5. 2009.

je države koje su ovu Konvenciju ratifikovale i u potpunosti implementirale njene odredbe u svoje unutrašnje zakonodavstvo – npr. Francuska, Mađarska, Finska, Slovačka, Rumunija, Jermenija. Najveći broj ovih država izmenio je postojeće krivično zakonodavstvo – krivične zakone i zakone o krivičnom postupku. Rumunija je, međutim, odlučila da donese poseban zakon koji bi se bavio ovom oblašću. Na isti način su postupile i neke države koje nisu ratifikovale Konvenciju, ali imaju odlično razvijeno zakonodavstvo – npr. Portugal, Dominikanska Republika, Indonezija. Implementaciju odredaba Konvencije, iako je još zvanično nisu ratifikovale, obavile su kroz postojeće krivično zakonodavstvo – npr. Turska, Nemačka, Slovačka, Austrija. Konačno, analiza pokazuje da postoje i zemlje koje nemaju u potpunosti usklađeno zakonodavstvo sa Konvencijom, iako je ona deo njihovog unutrašnjeg zakonodavstva – npr. u Bugarskoj i Albaniji nedostaje implementacija pojedinih odredaba, dok je situacija nešto ozbiljnija u Hrvatskoj, na Kipru i u Makedoniji. Pojedine države, npr. Rusija, nisu uložile mnogo napora da svoje zakonodavstvo prilagode Konvenciji, niti su izrazile spremnost da je ratifikuju.[193]

[193] Analiza je sačinjena na osnovu nacionalnih izveštaja Savetu Evrope, koji se mogu naći na internet adresi: *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp*, 1. 5. 2009.

2. ZAKONODAVSTVO SJEDINJENIH AMERIČKIH DRŽAVA IZ OBLASTI VISOKOTEHNOLOŠKOG KRIMINALA

Budući da je internet nastao na tlu SAD, a uzimajući u obzir i činjenicu da najmoćnije svetske IT korporacije imaju svoje sedište u SAD (Microsoft, Oracle, Google, Apple, IBM…) logično je da SAD pripadaju grupi zemalja koje su najdalje otišle po pitanju zakonske regulative visokotehnološkog kriminala. Ako pogledamo registar zakona,[194] koji se na neki način dotiču oblasti IT, videćemo kojim se svim temema pristupalo prilikom zakonodavnih aktivnosti. Istorijski gledano, možemo preko reakcije zakonodavaca pratiti razvoj određenih oblasti računarskih tehnologija, odnosno njihovu moguću zloupotrebu. Uzmimo kao ilustraciju *Communications Decency Act of 1995* (Zakon o pristojnosti u komunikaciji, i sekcije koje proširuju Zakon o komunikacijama iz 1932. godine)**,** gde se, u oblasti *TITLE V – BROADCAST OBSCENITY AND VIOLENCE, pod SEC. 502. OBSCENE OR HARASSING USE OF TELECOMMUNICATIONS FACILITIES UNDER THE COMMUNICATIONS ACT OF 1934* (Naslov 5, Emitovanje sramotnog i nasilnog sadržaja, pod sekcijom 502, O upotrebi telekomunikacionih sredstava u svrhu opscenosti i maltretiranja, po Zakonu o komunikaciji iz 1934. godine) kažnjava zloupotreba telefona ili nekog drugog telekomunikacionog sredstva, a u svrhe uznemiravanja, maltretiranja, upućivanja pretnji osobi koja prima poziv ili učestvuje u komunikaciji: znači, zloupotreba bazičnog uređaja za komunikaciju. Član Zakona glasi: „Svako ko preko sredstava telekomunikacije (a) svesno pozove broj telefona ili iskoristi sredstvo telekomunikacije bez obzira na to da li se uspostavi komunikacija ili ne, i bez otkrivanja svog identiteta a sa namerom da uznemirava, zloupotrebljava, preti ili maltretira osobu koja prima telefonski poziv ili učestvuje u komunikaciji predmetnim sredstvima, (b) ko izazove da tuđi telefon više puta ili neprestano zvoni sa namerom da uznemirava osobu čiji je broj pozvan, ili (c) svesno i sa namerom omogući da telekomunikaciono sredstvo koje se nalazi pod njegovom kontrolom bude upotrebljeno u svrhe aktivnosti navedenih u ovoj sekciji, biće kažnjen po članu 18 *US Code*, ili kaznom zatvora do dve godine ili oboje.“ Kasnije je, nakon ove sekcije, dodata podsekcija kojom se uvode računarske tehnologije u Zakon o pristojnosti u komunikaciji. Podsekcija glasi: „Ko u unutrašnjoj ili

[194] Izvor: *http://www.legi-internet.ro/en/laws.htm*, 1. 5. 2009.

međunarodnoj komunikaciji svesno (a) koristi interaktivni kompjuterski servis da pošalje određenoj osobi ili osobama mlađim od 18 godina, ili (b) koristi interaktivni kompjuterski servis da prikaže, na način koji je dostupan osobama mlađim od 18 godina, komentar, sugeriše, predloži, prikaže sliku ili na drugi način komunikacijom, koja opisuje ili oslikava očigledno uvredljiv sadržaj, po standardima zajednice, seksualne organe ili njihove izlučevine bez obzira na to da li je korisnik te usluge inicirao poziv ili započeo komunikaciju; kao i ko svesno i sa namerom omogući da telekomunikaciono sredstvo koje se nalazi pod njegovom kontrolom bude upotrebljeno u svrhe aktivnosti navedenih u ovoj podsekciji, biće kažnjen po članu 18 *US Code*, ili kaznom zatvora do dve godine ili oboje." Vidimo da je uočena opasnost od zloupotrebe komunikacije preko računara, tačnije interaktivnih računarskih servisa i da je taj vid komunikacije izdvojen iz opšte formulacije „i druga telekomunikaciona sredstva". Dalje, u Zakonu stoji da se neće smatrati odgovornim onaj ko: „isključivo omogućava pristup ili uspostavlja komunikaciju iz ustanove, sistema ili mreže, koji nisu pod kontrolom te osobe, uključujući i transmisiju, preuzimanje, privremeni smeštaj podataka, pristupanje računarskom softveru, kao i druge kapacitete koji, bez namere i znanja te osobe, samo pružaju pristup ili omogućavaju komunikaciju koja ne podrazumeva kažnjivu radnju izvršenja".[195]

U vezi sa ovim je i *TITLE XIV – CHILD ONLINE PROTECTION ACT*[196] (Zakon o zaštiti dece od onlajn sadržaja). Iz teksta ovog zakona jasno proizlazi namera zakonodavca da, iako se dete/maloletnik nalazi na vaspitanju i pod zaštitom roditelja, dodatno zaštiti dete od sve prisutnijeg štetnog sadržaja na *World Wide Web*-u. Ovim zakonom je proširen i, već pomenuti, Zakon o komunikacijama iz 1934. godine, sa *SEC. 231. RESTRICTION OF ACCESS BY MINORS TO MATERIALS COMMERCIALLY DISTRIBUTED BY MEANS OF WORLD WIDE WEB THAT ARE HARMFUL TO MINORS* (sekcija 231, zabrana pristupa maloletnicima materijalu koji se komercijalno distribuira preko interneta i koji je po njih štetan), pa će tako: „…biti kažnjen svako ko je dobro upoznat sa sadržajem materijala i ko svesno, u unutrašnjoj ili međunarodnoj komunikaciji preko *World Wide Web*-a, uspostavi komunikaciju u komercijalne svrhe, koja je dostupna svakom maloletniku i koja sadrži materijal koji je štetan za maloletnike, i to sa ne više od 50.000 dolara i/ ili kaznom zatvora do šest meseci". Ovim zakonom se nalaže i formiranje Komisije za zaštitu dece od štetnog onlajn sadržaja, koja će svoje delovanje usmeravati ka pronalaženju najboljih rešenja u zaštiti maloletnika u ovoj oblasti.

[195] Izvor: *http://www.legi-internet.ro/cda.htm*, 1. 5. 2009.
[196] Izvor: *http://www.legi-internet.ro/copa.htm*, 1. 5. 2009.

U *US Code*, pod glavom 18, deo I, poglavlje 47, paragraf 1030,[197] regulisana je „prevara i slične aktivnosti u vezi sa računarom". U stavu (1), koji štiti infomacije značajne za Vladu SAD, stoji da će biti kažnjen onaj: „Ko je svesno pristupio računaru kao autorizovani korisnik ili je prekoračivši autorizaciju na ovaj način došao u posed informacija koje su okvalifikovane od strane Vlade SAD, ili statutom ili nekim drugim aktom, kao informacije koje zahtevaju autorizovani pristup iz razloga nacionalne bezbednosti ili međunarodnih odnosa, ili bilo kojih podataka koji su restriktivni po pitanju pristupa, ili definisani pod paragrafom y, sekcije 11. Zakona o atomskoj energiji iz 1954. godine, a sa razlogom se veruje da će se informacije pribavljene na ovaj način iskoristiti protiv SAD, ili ko je pružio mogućnost da bilo koja druga strana sila primi ili dođe u posed ovih informacija, ili je došao, nenamerno u posed ovih informacija a nije ih prosledio nadležnom organu SAD." U stavu (2) štite se finansijski podaci/informacije, odnosno kažnjava se gore pomenuta radnja koja za objekat ima finansijske podatke (preuzete od finansijskih institucija) ili bilo koje podatke koji se nalaze u posedu neke od agencija Vlade SAD. Zatim, u stavu (3) susrećemo se sa zabranom neovlašćenog korišćenja računara koji su u posedu neke od agencija Vlade SAD, tako da to ponašanje utiče na upotrebu tih računara od strane ovlašćenih korisnika. Stavom (4) predviđeno je ponašanje neovlašćenog pristupa računaru, sa namerom pribavljanja protivzakonite imovinske koristi veće od 5.000 dolara u jednogodišenjem periodu. U stavu (5) imamo podstavove koji se tiču nedozvoljenog unošenja programa, sa namerom da se napravi šteta na računaru, čijem je pristupu neophodna autorizacija, ili neovlašćenog pristupa računaru, koji kao nenamernu posledicu ima oštećenje računara, ili neovlašćenog pristupa računaru, koji kao namernu posledicu ima oštećenje računara. Kazne se razlikuju od jednog do drugog krivičnog dela, ali su uglavnom u pitanju kazne zatvora, i to do pet, deset ili dvadeset godina.

Kongres SAD, kao federalno zakonodavno telo, donosi 1998. godine Digtal Millenium Copyright Act (Zakon o zaštiti autorskih prava za digitalni milenijum). Ovim zakonom zaštićena su sva originalna autorska dela koja su prezentovana u formi bilo kog dodirljivog medijuma izražavanja.[198] Zakon dalje ohrabruje vlasnike autorskih dela, koja se postavljaju na internet, da ih zaštite preko dostupnih tehnologija (razlikujemo dve vrste, one koje onemogućavaju pristup autorskim delima, i one koje sprečavaju kopiranje autorskih dela). Pored ovih mera, zakon uvodi i novi institut, CMI (*copyright management information* – informacija o tome ko upravlja autorskim pravom), koji predstavlja liniju teksta na zaštićenom delu pomoću koje se može identifikovati vlasnik autorskog dela. Zakonom je predviđena

[197] Izvor: *http://www.law.cornell.edu/uscode/18/1030.shtml*, 1. 5. 2009.
[198] Izvor: *http://www.acm.org/ubiquity/views/j_gibbs_1.html*, 1. 5.2009.

mogućnost vođenja parnice, ali i krivična odgovornost zbog kršenja njegovih normi. Ilustracije radi, kazne za krivičnu odgovornost kreću se do pet godina zatvora, i do 500.000 dolara novčane kazne za prvi put učinjeno krivično delo, ali i do 1.000.000 dolara novčane kazne ili kazna zatvora do 10 godina za recidiv, odnosno za povrat. U vezi sa zaštitom autorskih prava (*copyright*) jeste i *No Electronic Theft Act* 199 (Zakon o zabrani elektronske krađe). Sekcija 2. *CRIMINAL INFRINGEMENT OF COPYRIGHTS* (Krivičnopravna zaštita autorskih prava) kaže: „Svako ko prekrši autorska prava svesno, a sa namerom komercijalnog preimućstva, ili finansijske dobiti, ili reprodukcijom ili distribucijom, uključujući elektronska sredstva, tokom 180 dana jednog ili više fonozapisa ili jednog ili više autorskih dela, koji imaju ukupnu vrednost preko 1.000 dolara, biće kažnjen pod sekcijom 2319 člana 18 *US Code*." Zakon dalje zabranjuje i neautorizovanu distribuciju nastupa uživo autora, a uvodi i institut *Victim Impact Statement* (Izjava žrtve o šteti), kojim se uspostavlja obaveza na strani oštećenog da dostavi ovu izjavu, kojom će potvrditi svoj identitet, odnosno identitet nosioca povređenog autorskog prava, kao i štetu koju je pretrpeo usled kršenja autorskog prava.

Treba spomenuti da se u krivičnom zakonodavstvu SAD susrećemo i sa zaštitom prava na privatnost, u smislu tumačenja člana 42, poglavlja 21A, potpoglavlja I, Dela A, paragrafa 2000,[200] gde se zabranjuje Vladinim agentima ili drugim zvaničnicima da traže i zaplene bilo koji materijal u posedu nekog lica koje namerava da ga objavi, prikaže preko sredstava javnog informisanja, kao i drugim sličnim komunikacionim sredstvima (gde ovo možemo tumačiti, putem interneta), osim u slučajevima kada se posedovanje ili objavljivanje tog materijala krivično goni. Temom zaštite privatnosti bavi se i *Electronic Communication Privacy Act* (Zakon o zaštiti privatnosti za vreme elektronske komunikacije) iz 1986. godine, koji u odnosu na prethodnu verziju širi zaštitu i na polje računara. Ovim zakonom se štiti individualna komunikacija protiv prisluškivanja od strane vlasti, bez sudskog naloga, od trećih lica, bez legitimnog prava da imaju uvid u komunikaciju, kao i od ISP-a (*Internet Service Provider*). Ali nije dovoljno osigurano pravo na privatnost kada je u pitanju komunikacija zaposlenih na opremi koja je u vlasništvu poslodavaca.[201]

Na kraju, treba spomenuti i svedočenje gospodina Rendala Boea, pomoćnika glavnog savetnika iz firme *America Online, Inc* (AOL), po pitanju spama, tj. neželjene pošte, koje je održano pred Komitetom za trgovinu Predstavničkog doma SAD još 1998. godine.[202] On tvrdi da od 15.000.000 dnevno primljenih elektron-

[199] Izvor: *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ147.105*, 1. 5. 2009.

[200] Izvor: *http://www.law.cornell.edu/uscode/42/2000aa.shtml*, 1. 5. 2009.

[201] Izvor: *http://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act*, 1. 5. 2009.

[202] Izvor: *http://www.legi-internet.ro/spamcr.htm*, 1. 5. 2009.

skih poruka, od pet do 30 odsto čine neželjenu poštu. AOL je te godine tužio preko 40 privatnih i pravnih lica zvog slanja neželjene pošte. Postupajući po ovim predmetima, sud je u 16 slučajeva naložio zabranu daljeg širenja ovakve pošte. Što se tiče tehničkih detalja iznesenih prilikom svedočenja, vredi pomenuti metode kojima pošiljaoci neželjene pošte izbegavaju zaštitu koju AOL i drugi ISP-ovi postavljaju na svoje sisteme. Tako se ova lica služe zasebnim softverom za prikrivanje identiteta pošiljaoca neželjene pošte, kao i lažnim informacijama u zaglavljima imejlova, kako bi sakrili svoj identitet. Zbog svega navedenog Rendal Boe predlaže da AOL i Kongres zajedno rade na zakonodavnoj aktivnosti radi zaštite i sprečavanja zloupotreba, inače legitimne komunikacije putem elektronske pošte. Zanimljivo je da se na saslušanju spominje i Prvi amandman Ustava SAD, u kome je, između ostalog, zagarantovana i sloboda govora, a u svrhu prepreke koja se stavlja pred Kongres da spreči slanje neželjene pošte. Stoga, predloženo je da se barem zabrani falsifikovanje informacija o pošiljaocu, da se pojača *Computer Fraud and Abuse Act* (Zakon o prevari i zloupotrebi pomoću računara) na taj način čineći ga jakim oružjem protiv prenošenja neželjenih poruka, kao i razvoj i distribucija softvera koji masovno generiše neželjenu poštu, te da se zakonom propišu kazne, kao i mogućnosti, na strani ISP-ova da nadoknade sudske i advokatske troškove. U vezi sa ovom temom treba spomenuti i raspravu u Senatu u vezi sa neželjenom poštom,[203] gde je, takođe, podvučena alarmantna pojava neželjene pošte, kao i potreba za zakonskom regulativom iz ove oblasti. Sve ovo je uticalo de se izglasa *CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act* – Zakon o kontrolisanju agesivnog i neželjenog reklamiranja i pornografije) *Act*[204] 2003. godine. Iako se ovim zakonom daje na značaju borbi protiv neželjene pošte, kritičari kažu da se njime ne postiže mnogo, recimo, ne traži se od pošiljalaca pošte da imaju dozvolu od lica koja primaju poštu, zabranjeno je privatnim licima koja primaju neželjenu poštu da tuže pošiljaoce, zatim se uvodi obaveza kompanijama koje šalju veliki broj elektronskih poruka u svrhe marketinga da obezbede informacije o svojoj kompaniji. Pri tom, kritičari kažu da se ova obaveza uspostavlja na strani legalno prijavljenih kompanija, koje su samo u malom broju slučajeva i pošiljaoci neželjene pošte, dok je mnogo veći broj onih kompanija, izvan zakona, koje, u stvari, šalju ovakvu elektronsku poštu.[205]

Iz priloženog se vidi da napredak informacionih tehnologija mora da prati i odgovarajuća reakcija zakonodavaca, koja bi na adekvatan način i u što kraćem roku predupredila zloupotrebu ovog razvoja.

[203] Izvor: *http://www.legi-internet.ro/spamsen.htm*, 1. 5. 2009.
[204] Izvor: *http://www.spamlaws.com/federal/108s877.shtml*, 1. 5. 2009.
[205] Izvor: *http://www.spamlaws.com/federal/index.shtml,* 1. 5. 2009.

3. UPOREDNI PREGLED ZAKONODAVSTAVA ODABRANIH ZEMALJA

Usaglašenost nacionalnih zakonodavstava sa najznačajnijim članovima EKVTK (u zagradama su datumi stupanja na snagu Konvencije u državama, ukoliko su je ratifikovale).

Albanija i Austrija

	Albanija (1.7.2004.)	**Austrija (-)**
član 2 – nezakonit pristup		član 118a. Krivičnog zakonika
član 3 – nezakonito presretanje	članovi 123. i 255. Krivičnog zakonika	članovi 119. i 199a. Krivičnog zakonika
član 4 – ometanje podataka	član 192b. Krivičnog zakonika	član 126a. Krivičnog zakonika
član 5 – ometanje sistema	član 255. Krivičnog zakonika	član 126b Krivičnog zakonika
član 6 – zloupotreba uređaja	član 286. Krivičnog zakonika	član 126c Krivičnog zakonika
član 7 – falsifikovanje upotrebom računara	članovi 186, 187. i 189. Krivičnog zakonika	član 225a. Krivičnog zakonika
član 8 – prevara upotrebom računara		član 148a. Krivičnog zakonika
član 9 – dečja pornografija	član 117. Krivičnog zakonika	član 207a. Krivičnog zakonika
član 10 – kršenje autorskih prava	članovi 148. i 149. Krivičnog zakonika; članovi 14. i 50. Zakona o autorskim pravima	član 91. Federalnog zakona o autorskim pravima u literaturi i umetnosti i povezanim pravima
član 11 – pokušaj, pomaganje ili podstrekavanje	članovi 23. i 27. Krivičnog zakonika	članovi 12. i 15. Krivičnog zakonika

član 12 – odgovornost pravnih lica		član 3. Federalnog statuta o krivičnoj odgovornosti pravnih lica
član 13 – sankcije i mere	članovi 117, 122, 123, 165, 186-192, 255, 286a. Krivičnog zakonika; član 50. Zakona o autorskim pravima	članovi 118a, 119, 119a, 126, 126b, 126c, 148a, 207a i 225a. Krivičnog zakonika; član 91. Federalnog zakona o autorskim pravima u literaturi i umetnosti i povezanim pravima; član 4. Federalnog statuta o krivičnoj odgovornosti pravnih lica
član 16 – čuvanje računarskih podataka (u rač. saobraćaju)	član 299(2) Zakonika o krivičnom postupku	članovi 109. i 134(2-2) Zakonika o krivičnom postupku; član 103(4) Zakona o telekomunikacijama
član 17 – otkrivanje računarskih podataka (u rač. saobraćaju)		
član 18 – nalog za predaju rač.podataka	članovi 191. i 211. Zakonika o krivičnom postupku	članovi 111(2), 134 (2-2), 138. Zakonika o krivičnom postupku; članovi 92(3-3 i 6) i 103(4) Zakona o telekomunikacijama
član 19 – pretraga i zaplena računarskih podataka	članovi 202, 203. i 209. Zakonika o krivičnom postupku	članovi 109, 119. i 122. Zakonika o krivičnom postupku
član 20 – *real-time* sakupljanje podataka		članovi 134. i 137. Zakonika o krivičnom postupku
član 21 – presretanje podataka	članovi 221-223. Zakonika o krivičnom postupku	
član 22 – nadležnost organa		članovi 64. i 65. Krivičnog zakonika

Tabela 4.1.

Belgija i Bugarska

	Belgija (-)	Bugarska (7.4.2005.)
član 2 – nezakonit pristup	član 550bis. Krivičnog zakonika	članovi 216(3,5 i 6). i 319a. Krivičnog zakonika
član 3 – nezakonito presretanje	članovi 259bis. i 314bis. Krivičnog zakonika	članovi 171 (1 i 3). Krivičnog zakonika
član 4 – ometanje podataka	član 550ter.(1-2) Krivičnog zakonika	članovi 319b, 319c. i 319e. Krivičnog zakonika
član 5 – ometanje sistema	član 550ter.(1 i 3) Krivičnog zakonika	članovi 319b, 319c. i 319d. Krivičnog zakonika
član 6 – zloupotreba uređaja	članovi 259bis(2bis), 314bis(2bis), 550bis(5), 550ter(4). Krivičnog zakonika	član 319e. Krivičnog zakonika
član 7 – falsifikovanje upotrebom računara	član 504quater. Krivičnog zakonika	članovi 319b. i 319c. Krivičnog zakonika
član 8 – prevara upotrebom računara	član 210bis. Krivičnog zakonika	članovi 212a. i 319b(2) Krivičnog zakonika
član 9 – dečja pornografija	član 383bis. Krivičnog zakonika	član 159(2-5). Krivičnog zakonika
član 10 – kršenje autorskih prava	članovi 79bis. do 81. Zakona o autorskim i srodnim pravima	član 172a. Krivičnog zakonika
član 11 – pokušaj, pomaganje ili podstrekavanje	član 67. Krivičnog zakonika	članovi 18. i 20-22. Krivičnog zakonika
član 12 – odgovornost pravnih lica	član 5. Krivičnog zakonika	član 83a. Zakona o administrativnim prekršajima i sankcijama
član 13 – sankcije i mere	članovi 210bis, 259bis, 314bis, 504quater, 550bis. i 550ter. Krivičnog zakonika	članovi 171(1 i 3), 159, 172a, 212a, 216(3), 319a-319e. Krivičnog zakonika
član 16 – čuvanje računarskih podataka (u rač.saobraćaju)		članovi 125, 159, 162(6), 163. i 172(3). Zakonika o krivičnom postupku; članovi 55, 56. i 148. Zakona o unutrašnjim poslovima

član 17 – otkrivanje računarskih podataka (u rač.saobraćaju)		član 159. Zakonika o krivičnom postupku; članovi 55, 56. i 148. Zakona o unutrašnjim poslovima
član 18 – nalog za predaju rač.podataka	članovi 46bis. i 88bis. Zakonika o krivičnoj istrazi	članovi 159. i 172(3) Zakonika o krivičnom postupku; članovi 55, 56. i 148(1). Zakona o unutrašnjim poslovima
član 19 – pretraga i zaplena računarskih podataka	članovi 39bis, 88ter. i 88quater Zakonika o krivičnoj istrazi	
član 20 – *real-time* sakupljanje podataka	član 88bis. Zakonika o krivičnoj istrazi	rezerva na Konvenciju
član 21 – presretanje podataka	član 90.ter. Zakonika o krivičnoj istrazi	član 172. Zakona o krivičnom postupku
član 22 – nadležnost organa	članovi 6-14. Zakonika o krivičnom postupku	članovi 3-6. Krivičnog zakonika

Tabela 4.2.

Češka republika i Dominikanska republika

	Češka republika (-)	Dominikanska republika (-)
član 2 – nezakonit pristup	član 257a. Krivičnog zakonika	član 6. Zakona protiv VTK
član 3 – nezakonito presretanje	član 239. Krivičnog zakonika	član 9. Zakona protiv VTK
član 4 – ometanje podataka	član 257a. Krivičnog zakonika	član 10. Zakona protiv VTK
član 5 – ometanje sistema	član 257a. Krivičnog zakonika	član 11. Zakona protiv VTK
član 6 – zloupotreba uređaja		član 8. Zakona protiv VTK
član 7 – falsifikovanje upotrebom računara		član 18. Zakona protiv VTK
član 8 – prevara upotrebom računara	članovi 89. i 250. Krivičnog zakonika	članovi 13, 14, 15. i 16. Zakona protiv VTK
član 9 – dečja pornografija	član 205. Krivičnog zakonika	član 24. Zakona protiv VTK
član 10 – kršenje autorskih prava	član 152. Krivičnog zakonika	član 25. Zakona protiv VTK
član 11 – pokušaj, pomaganje ili podstrekavanje		
član 12 – odgovornost pravnih lica		član 60. Zakona protiv VTK
član 13 – sankcije i mere		
član 16 – čuvanje računarskih podataka (u rač.saobraćaju)	član 84(7) Zakona o telekomunikacijama; članovi 90. i 97. Zakona o elektronskim komunikacijama; član 88a. Zakonika o krivičnom postupku	član 53. Zakonika o krivičnom postupku
član 17 – otkrivanje računarskih podataka (u rač.saobraćaju)		član 56. Zakonika o krivičnom postupku
član 18 – nalog za predaju rač.podataka	članovi 78, 79, 88. i 158d. Zakonika o krivičnom postupku; član 47. Zakona o policiji	član 54. Zakonika o krivičnom postupku

član 19 – pretraga i zaplena računarskih podataka	članovi 82-85b. Zakonika o krivičnom postupku	
član 20 – *real-time* sakupljanje podataka	član 88. Zakonika o krivičnom postupku	
član 21 – presretanje podataka		
član 22 – nadležnost organa	članovi 16-20a. Krivičnog zakonika	član 65. Zakonika o krivičnom postupku

Tabela 4.3.

Finska i Francuska

	Finska (24.5.2007.)	Francuska (10.1.2006.)
član 2 – nezakonit pristup	poglavlje 38, član 8. Krivičnog zakona	član 323-1. Krivičnog zakona
član 3 – nezakonito presretanje	poglavlje 38, članovi 3, 4. i 8(2). Krivičnog zakona	član 226-15(2). Krivičnog zakona
član 4 – ometanje podataka	poglavlje 35, član 1. Krivičnog zakona	član 323-1. Krivičnog zakona
član 5 – ometanje sistema	poglavlje 38, članovi 5, 7a i 7b. Krivičnog zakona	
član 6 – zloupotreba uređaja	poglavlje 34, član 9a i 9b Krivičnog zakona; članovi 6. i 42. Zakona o zaštiti privatnosti u elektronskim komunikacijama	član 323-3-1. Krivičnog zakona
član 7 – falsifikovanje upotrebom računara	poglavlje 33, članovi 1. i 6. Krivičnog zakona	član 323-4. Krivičnog zakona
član 8 – prevara upotrebom računara	poglavlje 36, član 1(2) i poglavlje 37, član 8. Krivičnog zakona	član 323-3-1. Krivičnog zakona
član 9 – dečja pornografija	poglavlje 17, članovi 18, 18a i 19. Krivičnog zakona	član 227-23. i 227-24. Krivičnog zakona
član 10 – kršenje autorskih prava	poglavlje 49, član 1. Krivičnog zakona	članovi L112-1. i L112-2. Zakona o intelektualnoj svojini
član 11 – pokušaj, pomaganje ili podstrekavanje	poglavlje 5, članovi 5. i 6. Krivičnog zakona	član 323-7. Krivičnog zakona
član 12 – odgovornost pravnih lica	poglavlje 9 Krivičnog zakona	član 323-6. Krivičnog zakona
član 13 – sankcije i mere		
član 16 – čuvanje računarskih podataka (u rač.saobraćaju)	poglavlje 4, članovi 4b i 4c Zakona o merama prinude	članovi 16(1). i 56. Zakona o krivičnom postupku
član 17 – otkrivanje računarskih podataka (u rač.saobraćaju)		član 60-2. Zakona o krivičnom postupku

član 18 – nalog za predaju rač.podataka	članovi 27. i 28. Zakona o krivičnoj istrazi	članovi 56-11, 60-1, 60-2. i 99-3. Zakona o krivičnom postupku
član 19 – pretraga i zaplena računarskih podataka	poglavlja 4 i 5 Zakona o merama prinude; član 27. Zakona o krivičnoj istrazi	članovi 56. i 99(3-4). Zakona o krivičnom postupku
član 20 – *real-time* sakupljanje podataka	poglavlje 5a Zakona o merama prinude	član 60-2. Zakona o krivičnom postupku
član 21 – presretanje podataka	poglavlje 5a Zakona o merama prinude; član 95 Zakona o tržištu komunikacija	članovi 100 do 100-3, 100-6. i 706-95(1). Zakona o krivičnom postupku
član 22 – nadležnost organa	poglavlje 1 Krivičnog zakona	

Tabela 4.4.

Hrvatska i Indonezija

	Hrvatska (3.7.2002.)	**Indonezija (-)**
član 2 – nezakonit pristup	član 223(1). Krivičnog zakona	član 30(1). Zakona o informacijama i elektronskim transakcijama
član 3 – nezakonito presretanje	član 223(4). Krivičnog zakona	član 31(1). Zakona o informacijama i elektronskim transakcijama
član 4 – ometanje podataka	član 223(3). Krivičnog zakona	član 32(1). Zakona o informacijama i elektronskim transakcijama
član 5 – ometanje sistema		član 33. Zakona o informacijama i elektronskim transakcijama
član 6 – zloupotreba uređaja	član 223(6 i 7). Krivičnog zakona	član 34(1). Zakona o informacijama i elektronskim transakcijama
član 7 – falsifikovanje upotrebom računara	član 223a. Krivičnog zakona	član 35. Zakona o informacijama i elektronskim transakcijama
član 8 – prevara upotrebom računara	član 224a. Krivičnog zakona	član 36. Zakona o informacijama i elektronskim transakcijama
član 9 – dečja pornografija	član 197a. Krivičnog zakona	član 27(1). Zakona o informacijama i elektronskim transakcijama
član 10 – kršenje autorskih prava	članovi 230. i 231. Krivičnog zakona	
član 11 – pokušaj, pomaganje ili podstrekavanje	članovi 33, 37. i 38. Krivičnog zakona	važe odredbe Krivičnog zakona
član 12 – odgovornost pravnih lica	Zakon o odgovornosti pravnih lica	član 52(4). Zakona o informacijama i elektronskim transakcijama
član 13 – sankcije i mere	članovi 174(4), 197a, 223, 223a, 224a, 230. i 231. Krivičnog zakona	u članovima vezanim za relevantna krivična dela
član 16 – čuvanje računarskih podataka (u rač.saobraćaju)		član 43(3). Zakona o informacijama i elektronskim transakcijama

član 17 – otkrivanje računarskih podataka (u rač.saobraćaju)		član 43(4). Zakona o informacijama i elektronskim transakcijama
član 18 – nalog za predaju rač.podataka		član 43(3). Zakona o informacijama i elektronskim transakcijama
član 19 – pretraga i zaplena računarskih podataka	članovi 211b(2) i 215. Zakona o krivičnom postupku	
član 20 – *real-time* sakupljanje podataka		
član 21 – presretanje podataka		važe odredbe Krivičnog zakona
član 22 – nadležnost organa	članovi 13-16. Krivičnog zakona	

Tabela 4.5.

Italija i Jermenija

	Italija (5.4.2008.)	Jermenija (12.10.2006.)
član 2 – nezakonit pristup	član 615ter. Krivičnog zakonika	član 251. Krivičnog zakona
član 3 – nezakonito presretanje	članovi 617quater, quinquies, sexies i 623bis Krivičnog zakonika	član 254. Krivičnog zakona
član 4 – ometanje podataka	član 635bis. Krivičnog zakonika	član 253. Krivičnog zakona
član 5 – ometanje sistema	član 635quater. Krivičnog zakonika; član 167. Zakona o zaštiti podataka	
član 6 – zloupotreba uređaja	član 615quater, quinquies. Krivičnog zakonika	član 255. Krivičnog zakona
član 7 – falsifikovanje upotrebom računara	član 491bis. Krivičnog zakonika	član 252. Krivičnog zakona
član 8 – prevara upotrebom računara	član 640ter. Krivičnog zakonika	
član 9 – dečja pornografija	članovi 600ter, quarter, quarter 1, quinquies, sexies, septies. Krivičnog zakonika	član 263. Krivičnog zakona
član 10 – kršenje autorskih prava	članovi 171-a bis, 171bis, 171ter, 171octies i 174ter Zakona o autorskom pravu	član 158. Krivičnog zakona
član 11 – pokušaj, pomaganje ili podstrekavanje	članovi 56. i 110. Krivičnog zakonika	članovi 33. i 39. Krivičnog zakona
član 12 – odgovornost pravnih lica	članovi 24, 24bis i 25quiquies Zakona o administrativnoj odgovornosti pravnih lica	
član 13 – sankcije i mere	u članovima vezanim za relevantna krivična dela	u članovima vezanim za relevantna krivična dela
član 16 – čuvanje računarskih podataka (u rač.saobraćaju)	član 132 (4, 4ter, quater) Zakona o zaštiti podataka	član 16. Zakona o slobodnom pristupu informacijama

član 17 – otkrivanje računarskih podataka (u rač.saobraćaju)	član 244(2). Zakona o krivičnom postupku	članovi 235, 239-241. Zakonika o krivičnom postupku
član 18 – nalog za predaju rač.podataka	član 256(1). Zakona o krivičnom postupku	
član 19 – pretraga i zaplena računarskih podataka	članovi 247(1bis), 250, 254bis i 260(2). Zakona o krivičnom postupku	
član 20 – *real-time* sakupljanje podataka	član 132(4ter, quarter) Zakona o zaštiti podataka	
član 21 – presretanje podataka	član 266bis Zakona o krivičnom postupku	
član 22 – nadležnost organa	članovi 6, 7, 9. i 10. Krivičnog zakona	članovi 14-16. Krivičnog zakona

Tabela 4.6.

Kina i Kipar

	Kina (-)	**Kipar (30.4.2004.)**
član 2 – nezakonit pristup	član 285. Krivičnog zakona	član 4. Zakona 22(III)04
član 3 – nezakonito presretanje	član 252. Krivičnog zakona	član 5. Zakona 22(III)04
član 4 – ometanje podataka	član 286. Krivičnog zakona	član 6. Zakona 22(III)04
član 5 – ometanje sistema		član 7. Zakona 22(III)04
član 6 – zloupotreba uređaja		
član 7 – falsifikovanje upotrebom računara	član 287. Krivičnog zakona	član 9. Zakona 22(III)04
član 8 – prevara upotrebom računara		član 10. Zakona 22(III)04
član 9 – dečja pornografija	članovi 363, 364, 366. i 367. Krivičnog zakona	član 11. Zakona 22(III)04
član 10 – kršenje autorskih prava	članovi 217, 218. i 220. Krivičnog zakona; članovi 1, 3, 9, 10(2, 5, 6, 11, 12, 15), 11, 12, 20. i 24(2) Zakona o autorskim pravima	član 12. Zakona 22(III)04
član 11 – pokušaj, pomaganje ili podstrekavanje	članovi 22-24, 27. i 29. Krivičnog zakona	član 13. Zakona 22(III)04
član 12 – odgovornost pravnih lica	članovi 30. i 31. Krivičnog zakona	član 14. Zakona 22(III)04
član 13 – sankcije i mere	članovi 32-34. Krivičnog zakona	
član 16 – čuvanje računarskih podataka (u rač.saobraćaju)		
član 17 – otkrivanje računarskih podataka (u rač.saobraćaju)	regulisano podzakonskim aktima	

član 18 – nalog za predaju rač.podataka		
član 19 – pretraga i zaplena računarskih podataka	član 116. Zakona o krivičnom postupku i podzakonski akti	
član 20 – *real-time* sakupljanje podataka	član 10. Zakona o državnoj bezbednosti: član 16. Zakona o narodnoj policiji	
član 21 – presretanje podataka		
član 22 – nadležnost organa	članovi 6-12. Krivičnog zakona	član 16. Zakona 22(III)04

Tabela 4.7.

Mađarska i Makedonija

	Mađarska (1.7.2004.)	**Makedonija (15.9.2004.)**
član 2 – nezakonit pristup	članovi 300c i 300e Krivičnog zakonika	
član 3 – nezakonito presretanje		
član 4 – ometanje podataka		član 251(1). Krivičnog zakona
član 5 – ometanje sistema		
član 6 – zloupotreba uređaja		član 251(6). Krivičnog zakona
član 7 – falsifikovanje upotrebom računara		član 379-a(1). Krivičnog zakona
član 8 – prevara upotrebom računara		član 251(4-5). Krivičnog zakona
član 9 – dečja pornografija	član 204. Krivičnog zakonika	član 193. Krivičnog zakona
član 10 – kršenje autorskih prava	članovi 329a-329c Krivičnog zakonika	član 286. Krivičnog zakona; članovi 1, 3, 9, 13, 14, 18, 19, 156, 159. i 168. Zakona o autorskim i srodnim pravima
član 11 – pokušaj, pomaganje ili podstrekavanje	član 18. Zakonika o krivičnom postupku	članovi 19, 24(1). i 251(7). Krivičnog zakona
član 12 – odgovornost pravnih lica	član 7. Zakona o elektronskom poslovanju i IT-u	
član 13 – sankcije i mere	članovi 204, 309c, 309e, 329a-329c Krivičnog zakonika	
član 16 – čuvanje računarskih podataka (u rač.saobraćaju)	član 151. Zakona o prenošenju informacija	
član 17 – otkrivanje računarskih podataka (u rač.saobraćaju)	član 151. Zakona o prenošenju informacija; član 151. Zakonika o krivičnom postupku	

član 18 – nalog za predaju rač.podataka	član 151. Zakona o prenošenju informacija	
član 19 – pretraga i zaplena računarskih podataka	član 151. Zakona o prenošenju informacija; član 151. Zakonika o krivičnom postupku	član 251(8) Krivičnog zakona
član 20 – *real-time* sakupljanje podataka	član 151. Zakona o prenošenju informacija	
član 21 – presretanje podataka		
član 22 – nadležnost organa	članovi 3-5. Krivičnog zakonika	

Tabela 4.8.

Maroko i Meksiko

	Maroko (-)	**Meksiko (-)**
član 2 – nezakonit pristup	član 607-3(1). Krivičnog zakona	članovi 211 bis 1, 2 i 4. Krivičnog zakona
član 3 – nezakonito presretanje		
član 4 – ometanje podataka	članovi 607-3(3). i 607-6. Krivičnog zakona	članovi 211 bis 2, 3, 4 i 5. Krivičnog zakona
član 5 – ometanje sistema	članovi 607-3, 607-4. i 607-5. Krivičnog zakona	
član 6 – zloupotreba uređaja	član 607-10. Krivičnog zakona	
član 7 – falsifikovanje upotrebom računara	član 607-7. Krivičnog zakona	ne postoje posebne odredbe – odgovara se kao za «obično» krivično delo
član 8 – prevara upotrebom računara		
član 9 – dečja pornografija		
član 10 – kršenje autorskih prava		
član 11 – pokušaj, pomaganje ili podstrekavanje	članovi 607-8. i 607-9. Krivičnog zakona	
član 12 – odgovornost pravnih lica		
član 13 – sankcije i mere		članovi 211 bis 1-7. Krivičnog zakona
član 16 – čuvanje računarskih podataka (u rač.saobraćaju)		
član 17 – otkrivanje računarskih podataka (u rač.saobraćaju)		
član 18 – nalog za predaju rač.podataka		

član 19 – pretraga i zaplena računarskih podataka	član 607-11. Krivičnog zakona	ne postoje posebne odredbe – primenjuje se opšta procedura za obezbeđenje dokaza
član 20 – *real-time* sakupljanje podataka		
član 21 – presretanje podataka		
član 22 – nadležnost organa		

Tabela 4.9.

Nemačka i Portugal

	Nemačka (09.03.2009)	**Portugal (-)**
član 2 – nezakonit pristup	član 202a(1). Krivičnog zakonika	član 7. Zakona o računarskom kriminalu
član 3 – nezakonito presretanje	članovi 148. i 201. Krivičnog zakonika; član 89. Zakona o telekomunikacijama	član 8. Zakona o računarskom kriminalu
član 4 – ometanje podataka	član 303a. Krivičnog zakonika	član 5. Zakona o računarskom kriminalu
član 5 – ometanje sistema	član 303b. Krivičnog zakonika	član 6. Zakona o računarskom kriminalu
član 6 – zloupotreba uređaja	član 202c. Krivičnog zakonika	
član 7 – falsifikovanje upotrebom računara	član 269. Krivičnog zakonika	član 4. Zakona o računarskom kriminalu
član 8 – prevara upotrebom računara	član 263a. Krivičnog zakonika	član 221. Krivičnog zakona
član 9 – dečja pornografija	član 184b. Krivičnog zakonika	član 172. Krivičnog zakona
član 10 – kršenje autorskih prava	član 106ff. Zakona o autorskim pravima	član 9. Zakona o računarskom kriminalu
član 11 – pokušaj, pomaganje ili podstrekavanje	članovi 22-24, 26. i 27. Krivičnog zakonika	članovi 22, 23. i 27. Krivičnog zakona
član 12 – odgovornost pravnih lica	članovi 30. i 130. Zakona o prekršajima	član 10. Zakona o računarskom kriminalu
član 13 – sankcije i mere	u članovima vezanim za relevantna krivična dela	u članovima vezanim za relevantna krivična dela
član 16 – čuvanje računarskih podataka (u rač.saobraćaju)	članovi 94, 95, 98, 100g i 100h. Zakona o krivičnom postupku	član 6. Zakona 69/98
član 17 – otkrivanje računarskih podataka (u rač.saobraćaju)	članovi 100g i 100h Zakona o krivičnom postupku	
član 18 – nalog za predaju rač.podataka	član 95. Zakona o krivičnom postupku; članovi 112. i 113. Zakona o telekomunikacijama	

član 19 – pretraga i zaplena računarskih podataka	članovi 94, 95, 102, 103, 105, 161. i 163. Zakona o krivičnom postupku	članovi 176-178. Zakona o krivičnom postupku
član 20 – *real-time* sakupljanje podataka	član 100g Zakona o krivičnom postupku	član 190. Zakona o krivičnom postupku
član 21 – presretanje podataka	članovi 100a i 100b Zakona o krivičnom postupku	
član 22 – nadležnost organa	članovi 3-9 Krivičnog zakona	članovi 5. i 6. Krivičnog zakona

Tabela 4.10.

Rumunija i Rusija

	Rumunija (12.5.2004.)	**Rusija (-)**
član 2 – nezakonit pristup	član 42. Zakona 161/2003	član 272. Krivičnog zakona
član 3 – nezakonito presretanje	član 43. Zakona 161/2003	
član 4 – ometanje podataka	član 44. Zakona 161/2003	član 273. Krivičnog zakona
član 5 – ometanje sistema	član 45. Zakona 161/2003	
član 6 – zloupotreba uređaja	član 46. Zakona 161/2003	
član 7 – falsifikovanje upotrebom računara	član 48. Zakona 161/2003	član 274. Krivičnog zakona
član 8 – prevara upotrebom računara	član 49. Zakona 161/2003	
član 9 – dečja pornografija	član 51(1). Zakona 161/2003	članovi 242. i 242.1 Krivičnog zakona
član 10 – kršenje autorskih prava	članovi 139(8-9) i 143. Zakona o autorskom pravu	član 146. i 147. Krivičnog zakona
član 11 – pokušaj, pomaganje ili podstrekavanje	članovi 23, 26. i 27. Krivičnog zakona; članovi 47, 50. i 51(2) Zakona 161/2003	članovi 15. i 32-36. Krivičnog zakona
član 12 – odgovornost pravnih lica	član 19(1). Krivičnog zakona	
član 13 – sankcije i mere	članovi 42-46, 48-49. i 51. Zakona 161/2003; član 53. Krivičnog zakona	članovi 146, 147, 272. i 274. Krivičnog zakona
član 16 – čuvanje računarskih podataka (u rač.saobraćaju)	član 54. Zakona 161/2003	
član 17 – otkrivanje računarskih podataka (u rač.saobraćaju)		

član 18 – nalog za predaju rač.podataka	član 16. Zakona o osnivanju, organizovanju i funkcionisanju Direktorata za istraživanje krivičnih dela organizovanog kriminala i terorizma	
član 19 – pretraga i zaplena računarskih podataka	članovi 55. i 56(1-3) Zakona 161/2003; članovi 96. i 99. Zakona o krivičnom postupku	članovi 182. i 183. Zakona o krivičnom postupku
član 20 – *real-time* sakupljanje podataka		
član 21 – presretanje podataka	član 57. Zakona 161/2003; član 91. Zakona o krivičnom postupku	
član 22 – nadležnost organa	članovi 3-4. i 142-143. Krivičnog zakona	članovi 11. i 12. Krivičnog zakona; član 2. Zakona o krivičnom postupku

Tabela 4.11.

Slovačka i Turska

	Slovačka (-)	Turska (-)
član 2 – nezakonit pristup	član 247(1). Krivičnog zakonika	član 243(1).. Krivičnog zakona
član 3 – nezakonito presretanje	član 247(2). Krivičnog zakonika	
član 4 – ometanje podataka	član 247(1). Krivičnog zakonika	član 244(2). Krivičnog zakona
član 5 – ometanje sistema		član 244(1). Krivičnog zakona
član 6 – zloupotreba uređaja		
član 7 – falsifikovanje upotrebom računara		član 244(2). Krivičnog zakona
član 8 – prevara upotrebom računara	član 226. Krivičnog zakonika	član 158(1). Krivičnog zakona
član 9 – dečja pornografija	članovi 368-370. Krivičnog zakonika	član 226(3-5). Krivičnog zakona
član 10 – kršenje autorskih prava	član 283. Krivičnog zakonika	članovi 1b, 2. i 71-75. Zakona o intelektualnoj i umetničkoj svojini
član 11 – pokušaj, pomaganje ili podstrekavanje	članovi 14(1), 20 i 21(1). Krivičnog zakonika	članovi 35, 37-40. Krivičnog zakona
član 12 – odgovornost pravnih lica		član 60. Krivičnog zakona
član 13 – sankcije i mere	članovi 196, 247, 283. i 369. Krivičnog zakonika	u članovima vezanim za relevantna krivična dela
član 16 – čuvanje računarskih podataka (u rač.saobraćaju)	član 90(1). Zakonika o krivičnom postupku	član 6(1). Zakona 5651/2007
član 17 – otkrivanje računarskih podataka (u rač.saobraćaju)		
član 18 – nalog za predaju rač.podataka		

član 19 – pretraga i zaplena računarskih podataka	član 91. Zakonika o krivičnom postupku	član 134. Zakona o krivičnom postupku
član 20 – *real-time* sakupljanje podataka	član 90(1). Zakonika o krivičnom postupku	
član 21 – presretanje podataka	član 90. Zakonika o krivičnom postupku	član 135. Zakona o krivičnom postupku
član 22 – nadležnost organa	član 3. Zakonika o krivičnom postupku	članovi 8-13. Krivičnog zakona

Tabela 4.12.

VI

ODNOS VISOKOTEHNOLOŠKOG KRIMINALA SA TERORIZMOM I ORGANIZOVANIM KRIMINALOM

1. VISOKOTEHNOLOŠKI I ORGANIZOVANI KRIMINAL – SAVEZNIŠTVO U RAZVOJU

„Teško je reći kako će organizovani kriminal izgledati u budućnosti, ali realnost nije daleko od radnje nekog filma naučne fantastike.“[206]

Visokotehnološki i organizovani kriminal nemaju na prvi pogled gotovo ništa zajedničko. VT kriminal je nastao poslednjih godina, dok organizovani kriminal ima korene u nešto daljoj prošlosti. Iako može biti unosan, VT kriminal nije u fokusu kriminalnih grupa. Pored toga, bavljenje VT kriminalom zahteva znatno poznavanje računarskih i ostalih novih tehnologija. Osobe koje su uglavnom vezuju u široj javnosti za izvođenje različitih ilegalnih radnji posredstvom računara, tzv. hakeri (engl. *hackers*) posmatraju se kao usamljeni pojedinci koji deluju isključivo individualno i napadaju pojedinačne računare ili računarske sisteme, bez šireg plana i organizacije. Dakle, bez dublje analize, mogli bismo zaključiti da između ova dva nema dodirnih tačaka. Realnost je ipak drugačija – vođene uglavnom finansijskim interesima, kriminalne grupe se sve više okreću korišćenju različitih aspekata visokih tehnologija, pre svega u cilju lakšeg obavljanja kriminalnih delatnosti, ali i radi stvaranja novih vrsta nelegalnih delatnosti koje predstavljaju simbiozu „klasičnog“ organizovanog kriminala i VT kriminala. Kako Suzan Brener (*Susan Brenner*) primećuje, udruživanje kriminalaca u kriminalne organizacije u realnom svetu je način multipliciranja, višestrukog uvećanja njihove snage. Da li je sajber kriminalcima takvo uvećanje potrebno? Po Brenerovoj, u virtuelnom svetu snaga ne igra nikakvu ulogu i pojedinac koji raspolaže određenim znanjem i tehnologijom može sam da učini istu štetu koju bi učinilo više ljudi koji rade zajedno kao organizovana grupa. Međutim, kada ciljevi razbojnika VT kriminala postanu kompleksniji, kada je potrebno izvršiti simultane upade, napade ili druge radnje prema više pojedinaca ili kompanija, udruživanje snage – shvaćene u tom virtuelnom smislu – opet postaje aktuelno.[207]

---

[206] Bojan Dobovšek, *Organised Crime – Can We Unify the Definition?*, u: Policing in Central and Eastern Europe: Comparing Firsthand Knowledge with Experience from the West, *http://www.ncjrs.org/policing/org323.htm*, 1. 5. 2009.

[207] Susan W. Brenner, *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships*, North Carolina Journal of Law & Technology 4/2002, str. 27–29.

Odnos visokotehnološkog i organizovanog kriminala može se, dakle, posmatrati iz dva aspekta: kao organizovanje sajber kriminalaca, i kao korišćenje savremenih tehnologija u aktivnostima „klasičnog" organizovanog kriminala. U drugom slučaju, reč je o elektronskim transakcijama, tokovima novca koji se teško prate ako se pripadnici organizovanog kriminala služe novim pogodnostima za transfer ili „pranje" novca stečenog nelegalnim aktivnostima. Do sada najveća i najpoznatija afera u vezi sa pranjem novca korišćenjem savremenih tehnologija dogodila se 2000. godine, kada je ogranak sicilijanske mafije pokušao da „opere" oko 400 miliona dolara preko Banke Sicilije, uz posredovanje čitavog niza banaka u Portugalu, Švajcarskoj i Banke Vatikana. Prevara je otkrivena samo zato što je jedan od učesnika u pranju novca odao policiji ceo plan.[208]

Prva aktivnost je, međutim, daleko zanimljivija kada se izučava visokotehnološki kriminal. Da li je moguće kriminalno udruživanje pojedinaca ili grupa u virtuelnom prostoru? Da, ali ne onako kako bi to pojedinci verovatno sebi predstavili. Najjednostavnije rečeno, kada neki pojedinac ima „kvalitetnu" ideju o tome kako izvesti određenu prevaru, a nema dovoljno finansijskih sredstava ili opreme, ili jednostavno želi da smanji rizik od hapšenja za 50 odsto, udružiće se sa drugim pojedincem.[209] Ono što je u ovakvoj „organizaciji" poseban kuriozitet jeste da se njeni članovi nikada ne moraju videti, niti znati identitet, izgled, ili bilo koji privatni podatak drugih osoba sa kojima su na ovaj način povezane. U konačnom hapšenju u okviru operacije *Firewall*, koja je trajala preko godinu dana, a koju su oktobra 2004. godine izvele policijske jedinice SAD i Kanade, otkrivena je grupa od 26 ljudi koji su organizovano pribavljali i prodavali brojeve i druge podatke ukradenih kreditnih kartica. U trenutku kada su uhvaćeni, oni su preprodali oko 1,7 miliona kreditnih kartica i ostvarili dobit od oko 4,3 miliona dolara. Po-

[208] Više o ovom i sličnim primerima: Phil Wiliams, *Organized Crime and Cybercrime: Synergies, Trends, and Responses*, *http://www.crime-research.org/library/Cybercrime.htm*, 1. 3. 2009. Stručnjaci širom sveta već godinama upozoravaju da veza između organizovanog kriminala i VT kriminala postaje sve očiglednija. Videti, npr. različite tekstove u kojima se ove dve kriminalne pojave poistovećuju ili se ukazuje na jasnu vezu između organizovanja kriminalnih grupa i organizovanja grupa koje vrše prevare na internetu: *Fighting the Agents of Organized Cybercrime*, *http://www.cnn.com/2008/TECH/05/08/digitalbiz.cybercrime/index.html*; *Repost Warns of Organized Cybercrime*, *http://www.itworldcanada.com/a/IT-Focus/39c78aa4-df47-4231-a083-ddd1ab8985fb.html*, 1. 5. 2009.

[209] Zanimljiv primer o ovakvom udruživanju: Robert Vamosi, *Cybercrime does pay; here's how*, *http://reviews.cnet.com/4520-3513_7-6427016-1.html*, 1. 5. 2009.

jedinci koji su bili članovi ove grupe nisu se lično poznavali, već samo preko njihovih internet nadimaka.[210]

Drugi način ovakve organizacije predstavlja „organizovano" organizovanje sajber kriminalca, najčešće pod okriljem neke grupe organizovanog kriminala, koja želi da proširi svoje delovanje i na internet prevare. Takve grupe se prepoznaju pre svega po masovnosti prevara koje obavljaju, ali njihovi metodi se ne razlikuju mnogo od onih koje koriste pojedinci. Takođe, ovakve grupe obavljaju isključivo lukrativne prevare, dok se ne bave onima koje su pojedini hakeri radili „za slavu", odnosno da bi preneli neku političku ili sličnu poruku.[211] Alan Paller, direktor Instituta SANS, kaže da je u pitanju industrija vredna nekoliko milijardi dolara, kao i da dobro finansirani hakeri širom planete bez prestanka istražuju mogućnosti za vršenje prevara i krađu identiteta.[212] Takođe, mogućnosti koje se otvaraju do sada su neviđene, jer ceo organizovani kriminal može da se preseli u virtuelni svet. Najbolji primer predstavljaju tzv. onlajn iznude, koje se svode na plaćanje „reketa" od strane onlajn servisa organizovanim kriminalnim grupama, u zamenu za njihovu (onlajn) zaštitu. Po pravilu, ovakve „ponude" najpre dobijaju internet sajtovi koji se bave klađenjem na sportske i druge događaje, a veoma često napadači dolaze iz zemalja istočne Evrope, koja je donedavno bila idealno mesto za njihovo skrivanje.[213] Međutim, postoje slučajevi onlajn iznude i u Srbiji. Tužilaštvu za visokotehnološki kriminal prosleđen je imejl upućen Radio-televiziji Srbije sa pretnjom identičnom u primerima onlajn iznude. Dakle, sve je isto kao i u klasičnoj kriminalnoj operaciji, samo se aktivnosti odigravaju u sajber svetu. I druga krivična dela mogu naći svoje mesto na internetu, pre svega zato što se komunikacija obavlja anonimno i sa daleko manjim rizikom nego, npr. na ulici. Tako se mogu naći različite agencije koje nude usluge prostitucije, čak i u zemljama u kojima je to strogo zabranjeno. Ono što, ipak, najviše zabrinjava jeste on-

[210] Videti izveštaj Tajne službe SAD (US Secret Service) o ovom događaju od 28. oktobra 2004. godine: *http://www.secretservice.gov/press/pub2304.pdf* (1. 5. 2009); kao i druge detalje u izveštajima različitih organizacija koje se bave sigurnošću na internetu: *http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1146949,00.html*, 1. 5. 2009; *http://antivirus.about.com/b/2004/11/02/operation-firewall-nabs-28.htm*, 1. 5. 2009.

[211] Izvor: *http://www.wired.com/techbiz/media/news/2006/09/71793*, 1. 5. 2009.

[212] Izvor: *McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet*, *http://www.mcafee.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf*, 1. 5. 2009, str. 7. Institut SANS je najpoznatija ustanova koja se bavi edukacijom u vezi sa zaštitom elektronskih informacija u bazama podataka, kao i informacija na internetu. Više informacija na internet adresi Instituta: *http://www.sans.org/*, 1. 5. 2009.

[213] Izvor: *McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet*, *loc. cit.*, str. 14.

lajn prodaja narkotika, koja sve više uzima maha i koja se ne može tako lako uočiti, posebno kada je manjih razmera i kada ne uključuje međudržavne pošiljke. Sa druge strane, kada je reč o organizovanim grupama koje deluju koordinirano u različitim delovima sveta, situacija je drugačija. U operaciji *Cyber Chace*, koju su izvele policije SAD, Kanade i Indije u aprilu 2005. godine, uhapšene su 23 osobe u 11 gradova u tri države, koje su organizovale mrežu prenošenja lekova koji izazivaju zavisnost i čija je distribucija inače strogo kontrolisana. Lekovi su proizvedeni i Indiji, a zatim transportovani i SAD, gde su prepakovani i prodavani onlajn kupcima. Za kupovinu se nije tražio recept lekara, samo uplata preko kreditne kartice, a ukupan profit koji je ova grupa ostvarila procenjen je na oko sedam miliona dolara, dok su u samoj akciji zaplenjeni lekovi u istoj vrednosti. Cena lekova bila je viša od uobičajene, a indijski proizvođač ih je distribuirao na preko 200 različitih internet sajtova u SAD i Kanadi.[214]

Udruživanje radi vršenja krivičnih dela pomoću visokih tehnologija može imati i drugačiju dimenziju. Poznat je slučaj vlasnika kompanije koji je „iznajmio“ šesnaestogodišnjeg hakera da „obara“ internet prezentacije konkurentskih firmi. Posledica njegovog delovanja bila je blokada različitih internet sajtova, ali i blokada rada nekoliko internet provajdera u trajanju od pet meseci, sa ukupnom štetom od oko dva miliona dolara. Iako su obojica na kraju otkrivena i uhapšena, ovaj jednostavan primer pokazuje koliko opasno može da bude pravo udruživanje i organizovanje u kriminalnu grupu radi vršenja napada iz ekonomskih interesa.[215]

Kad se posmatra odnos VT kriminala i organizovanog kriminala, posebno je važno istaći problem prikupljanja dokaza u odnosu na izvršioce krivičnih dela organizovanog kriminala. Naime, preovlađujući vid prikupljanja dokaza jesu mere prisluškivanja telefonskih razgovora, predviđene članom 232 ZKP. Međutim, komunikacija se preselila u virtuelni prostor upravo zbog nepostojanja procesnih odredaba za monitoring takve vrste saobraćaja. Sad možete da koristite programe (*skype, messenger*...) za obavljanje telefonskih razgovora. Tehnička karakteristika ovih programa je da ne reaguju na adminstratorske zabrane u odnosu na *firewall*, te da je protok informacija potpuno slobodan. Kako ostvariti monitoring nad ovom vrstom saobraćaja? Čini nam se da u ovom momentu ne postoji svest o značaju ovog problema, iako se određene državne agencije njime bave, ali to ne može da bude učinjeno bez izmena procesnih zakona, o čemu će još biti reči.

[214] Izvor: *ibidem*, str. 9.
[215] Izvor: *ibidem*, str. 11.

2. VISOKOTEHNOLOŠKI KRIMINAL I TERORIZAM – NEVIDLJIVI NEPRIJATELJI

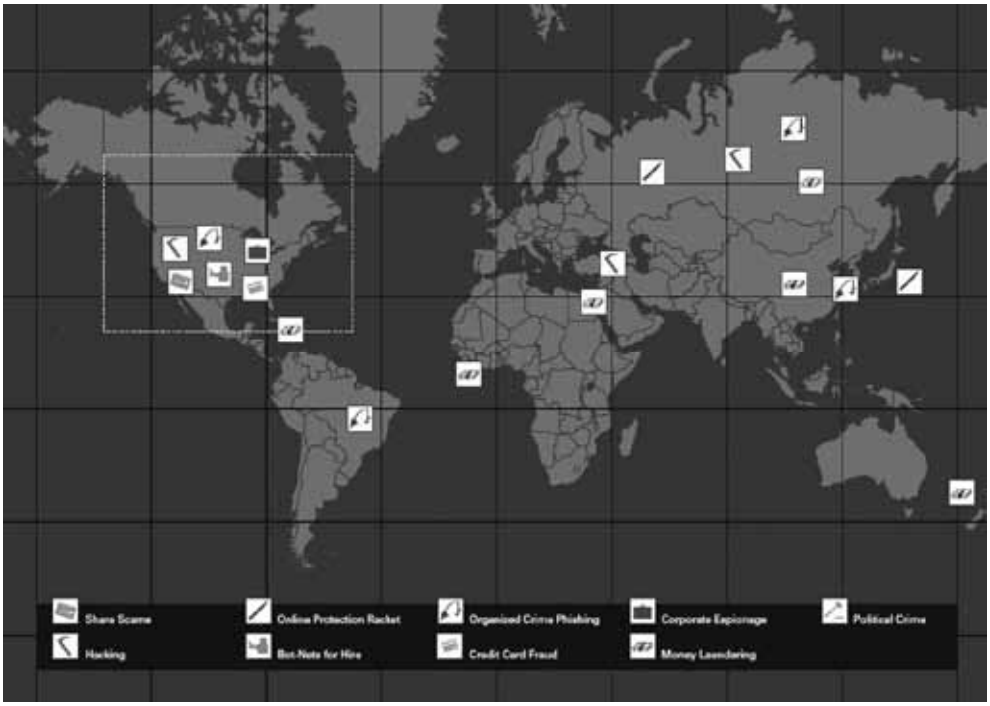
Kada je reč o odnosu sajber kriminala i terorizma, mora se reći da savremene tehnologije, računarske i druge, nude obilje mogućnosti za teroriste da svojim nelegalnim aktivnostima sabotiraju svakodnevni način života i bezbednost građana. Ono što je zajedničko obema pojavama jeste da se savremeni terorizam, upravo kao i VT kriminal, odvijaju uz anonimnost izvršilaca, pa se može i u jednom i u drugom slučaju govoriti o „nevidljivim neprijateljima". Npr. obaranjem računarske mreže nekog aerodroma, mogu se izazvati znatni zastoji u avionskom saobraćaju i takođe veliki finansijski gubici; isto tako se može neautorizovano uticati na bilo koji računarski sistem državnih institucija, berze i sl. Još konkretnije, mada više u domenu telekomunikacione nego računarske zloupotrebe savremenih tehnologija, dokazano je da su u različitim terorističkim napadima širom sveta mobilni telefoni korišćeni kao okidač – inicijator eksplozija. Kako se tehnologije razvijaju, mogućnosti postaju sve šire i drastičnije.[216]

Drugi aspekt povezanosti visokotehnološkog kriminala i terorizma je u komunikaciji i transferu podataka, novca, logistike putem interneta i drugih računarskih mreža. Jednostavno, internet je komunikaciju između različitih delova sveta učinio ne samo jednostavnijom i jeftinijom već i mnogo težom za prisluškivanje i praćenje. Milijarde elektronskih poruka koje svakodnevno kruže računarskim mrežama ne mogu se u potpunosti ispratiti, dok je presretanje ovakvih vrsta komunikacije zakonski zaštićeno i ne može da se obavlja bez osnova i odgovarajuće procedure. Zato nije nerealno reći da postoji veza između savremenih tehnologija i terorizma, kao i da dobro obučeni teroristi mogu ponekad na sebe preuzeti ulogu sajber kriminalaca radi ostvarivanja nekog zadatka. Previše bi, međutim, bilo izvesti ovakav zaključak van okvira realnosti: ljudi koji se bave visokotehnološkim kriminalom rade to pre svega iz finansijskih pobuda; daleko je manji broj onih koji to čine iz političkih, religijskih i drugih ubeđenja. Ovakvo mišljenje ne dele svi stručnjaci, pa se mogu naći različita tumačenja koliko je pretnja sajber terorizmom realna i aktuelna. Centar za zaštitu nacionalne infrastrukture Ujedinjenog Kraljevstva[217] je u toku 2007. godine ponovio mišljenje

[216] Poznato je, npr. da sve savremene fabrike vode koriste računare za njenu preradu – i na ovaj proces se može uticati (pre svega u smislu njegove destrukcije, odnosno zastoja u proizvodnji) neovlašćenim pristupom takvim računarskim mrežama.

[217] *Centre for the Protection of National Infrastructure* (CPNI) jeste vladino telo koje se bavi povećanjem bezbednosti i bezbednosnim savetima preduzećima i organizacijama koje se bave poslovima vezanim za infrastrukturu. Internet prezentacija na adresi: *http://www.cpni.gov.uk*, 1. 5. 2009.

koje preovlađuje – da je pretnja niska ali da se posmatranje elektronskih komunikacija nastavlja u skladu sa ciljem da se spreči narušavanje bezbednosti pojedinaca i organizacija.[218]



Slika 5: Vrste kriminalnih aktivnosti u svetu koje se vezuju za korišćenje računara i računarskih tehnologija[219]

Očigledan podatak koji demantuje ovakvo mišljenje, nažalost, jeste posledica napada na SAD, 11. septembra 2001. godine, gde je dokazano da je većina komunikacije išla preko steganografije (u slici, video ili audio-klipu bila je skrivena poruka).

Treći aspekt je lakoća širenja ideja koje su motiv za činjenje terorističkih napada. Kroz praksu u poslednje dve godine, pogotovu u SAD i Velikoj Britaniji, procesuirani su postupci protiv lica koja su preko foruma na internetu širila razne ideje, kao i savete za pravljenje oružja.

[218] Opet, različito mišljenje i pogled iz drugog aspekta mogu se naći u tekstu Louise I. Shelley, *Organized Crime, Terrorism and Cybercrime* u: Alan Bryden/Philipp Fluri (ur.), *Security Sector Reform: Institutions, Society and Good Governance*, Baden-Baden, 2003, str. 303–312. Ovaj članak se može pronaći i na internet adresi: *http://www.crime-research.org/articles/Terrorism_Cybercrime*, 1. 5. 2009.

[219] Izvor: *McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet*, *loc. cit*, str. 2.

VII

GRANIČNI SLUČAJEVI VISOKOTEHNOLOŠKOG KRIMINALA

1. SPAMMING, COOKIES, ADWARE/SPYWARE

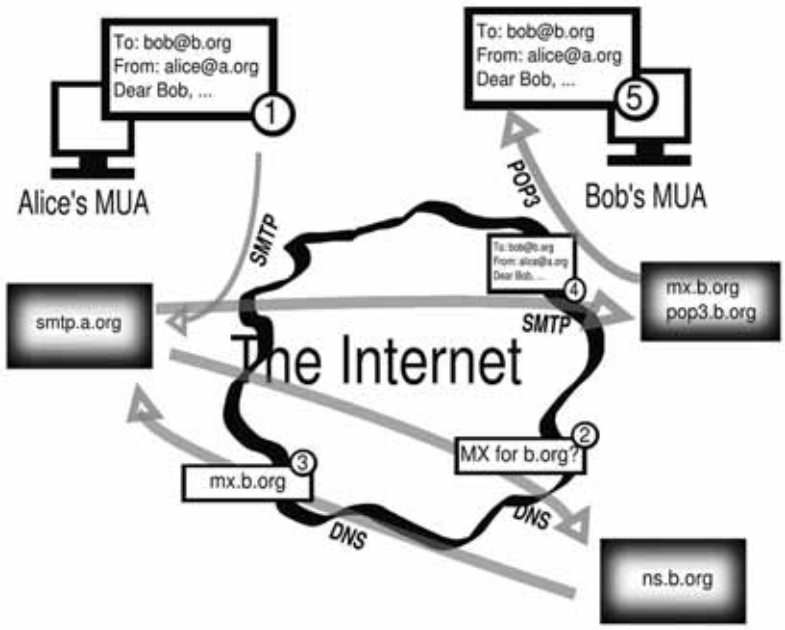
Za razliku od hakerskih napada i zlonamernih programa/virusa (*malware*), granični slučajevi visokotehnološkog kriminala (*spam, cookies, adware/spyware, pop-up*) u najvećem broju slučaja predstavljaju upotrebu računarskih tehnologija u svrhe agresivnog marketinga, koji najčešće nemaju direktnih posledica na korisnika ili računarski sistem. Ipak, ove pojave mogu da izazovu i teže posledice, pogotovu ako su u pitanju prevare preko neželjene elektronske pošte (*spam*), ili zagušenja i otkazi sistema (*denial of service*) usled preopterećenosti, kao i *spyware* programi, koji narušavaju privatnost, a nekad se koriste i za hakerske napade.

Da bismo se u potpunosti posvetili *spam* porukama, moramo se osvrnuti na elektronsku poštu i ukratko objasniti kako ona funkcioniše. Počeci elektronske pošte (*e-mail*) svakako su vezani za osamdesete godine prošlog veka i komercijalizaciju interneta. SMTP (*Simple Mail Transfer Protocol*) definisan je RFC-om 821. *Request For Comment*, skr. RFC, jesu tekstovi kojima se uspostavljaju standardi vezani za funkcionisanje interneta. IETF (*International Engineering Task Force*) jeste organizacija odgovorna za objavljivanje RFC-a. Inače, IETF je „velika međunarodna zajednica dizajnera računarskih mreža, operatera, prodavaca, i istraživača čija je briga evolucija arhitekture interneta i njegov nesmetan rad".[220] IETF je organizovan u grupe koje se bave transportom i bezbednošću podataka preko interneta. Nema formalno članstvo, nije propisana ni članarina, ali je obično finansijski podupiru neke organizacije američke vlade ili iz sveta IT-a [trenutno su to NSA (*National Security Agency*) i *VeriSign*].[221]

Elektronska pošta danas najčešće funkcioniše po *store-and-forward* (zadrži i prosledi) principu. U pitanju je server/klijent orijentisana arhitektura. Elektronska pošta se, u formi podataka, šalje sa klijentskih aplikacija MUA (*Mail User Agent*) kao što su *Outlook, Outlook Express, IncrediMail, Thunderbird* itd., do servera na internetu ili u LAN-u (aplikacije tipa: *Microsoft Exchange, IBM Lotus*...). Komunikacija dalje teče do sledećeg servera, koji razrešava imena, a na kraju i do željenog računara/korisnika, odnosno imejl aplikacije MUA na njegovom računaru. Ova aplikacija koristi protokole POP3 (*Post Office Protocol* – protokol koji je na računaru zadužen da elektronsku poštu preuzme sa odgovarajućeg servera) ili IMAP (*Internet Message*

[220] Izvor: *http://www.ietf.org/overview.html*, 1. 5. 2009.
[221] Izvor: *http://en.wikipedia.org/wiki/Internet_Engineering_Task_Force*, 1. 5. 2009.

Access protocol, sa istim zaduženjem), koji omogućavaju da pošta dospe do krajnjeg korisnika. Pojmove IP, SMTP, POP3 ili IMAP nalazimo kao protokole koji su deo i funkcionišu po TCP/IP modelu komunikacije. Svakako, za razumevanje celog toka komunikacije neophodno je i razjasniti pojam DNS (*Domain Name System*), koji je zadužen da pretvara ljudima razumljiva imena u internet adrese. U vezi sa elektronskom poštom, DNS služi da se tačno locira računar/korisnik na osnovu imejl adrese; ako ona glasi, na primer, *petar.petrovic@internetprovajder.com* bitno je naglasiti da sve posle grčkog slova @ predstavlja ime domena, kome pripada korisnički nalog, odnosno sve što piše pre @ (imena) domena, sa kojima radi DNS, predstavljaju reči obično odvojene tačkama koje pomažu u komunikaciji i lociranju tražene adrese (*google.com, yahoo.com, ietf.org*). „Cilj imena domena (*domain name*) jeste da pruže mehanizam za imenovanje resursa na taj način da se imena mogu koristiti na različitim vrstama računara, mreža i protokola…"[222] Na kraju, treba zaključiti da preko SMTP-a, POP3, IMAP-a i DNS-a i tehnologija koje se nalaze ispod, funkcioniše razmena imejl poruka. U suštini, retko kada se poruke direktno razmenjuju između povezanih računara. Gore pomenutim RFC 821 utaban je put za elektronsku poštu sa kakvom se danas srećemo.

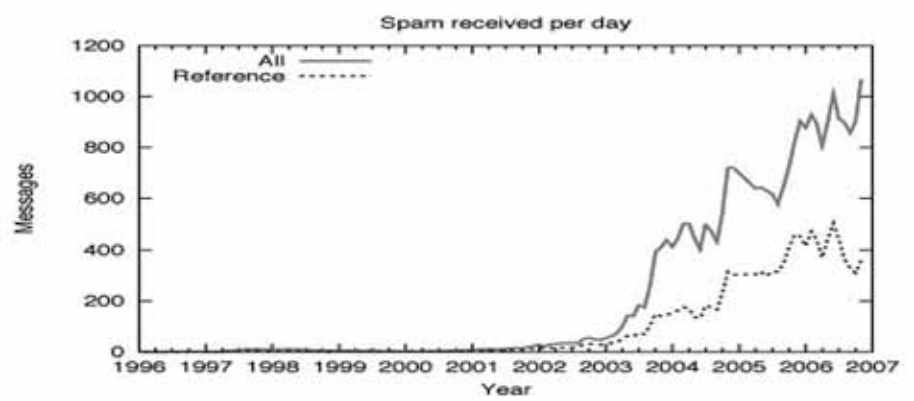


Slika 6: Ilustrovana imejl komunikacija [223]

[222] Izvor: *https://tools.ietf.org/html/rfc1035*, 1. 5. 2009.
[223] Izvor: *http://commons.wikimedia.org/wiki/File:How_e-mail_works.svg*, 1. 5. 2009.

Da je imejl zaista postao najčešći vid komunikacije u elektronskoj formi govore i sledeći podaci preuzeti sa internet sajta *http://email.about.com*. Naime, dnevno se, tvrde na ovom sajtu, pošalju 183 milijarde imejl poruka, odnosno dva miliona po sekundi. [224] Veliki broj imejlova u odnosu na ove cifre predstavlja neželjenu elektronsku poštu (*spam*), koja je danas veliki problem na internetu.

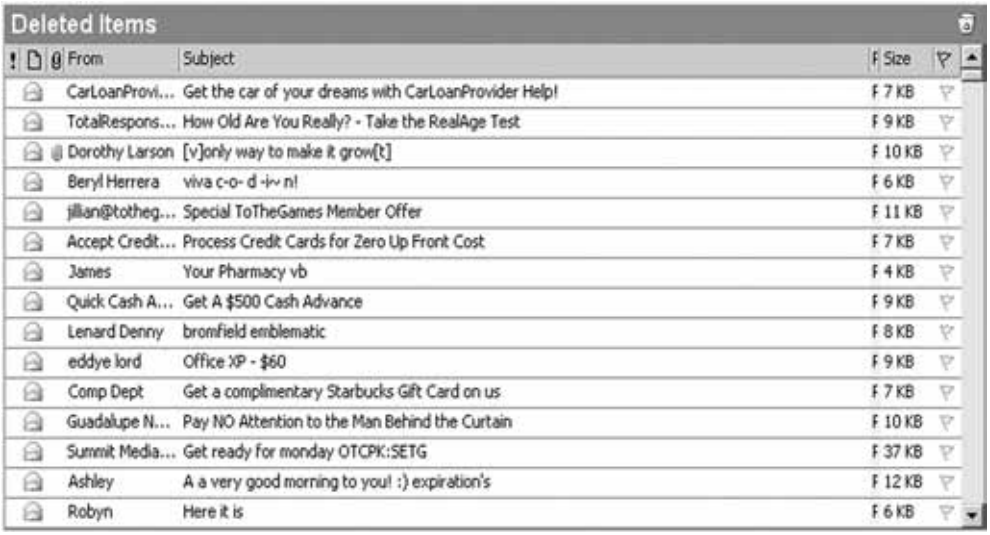
Spam je, jednostavno rečeno, neželjena elektronska pošta, koja ima komercijalnu prirodu. Termin *spam* se najčešće vezuje za skeč poznate engleske pozorišne trupe Monty Python.[225] Sledeći dijagram ilustruje koliko *spam* poruka prima jedan korisnik dnevno (crvena linija – korisnik sa više imejl adresa; plava, isprekidana linija – dnevna količina *spam* poruka koje dospevaju na jednu imejl adresu).



Slika 7: Spam statistika [226]

Slanje neželjene elektronske pošte najčešće funkcioniše tako što oni koji je šalju nabavljaju na ilegalnom tržištu liste sa velikim brojem imejl adresa ili ih sami pribavljaju korišćenjem programskih alata, koji se popularno zovu *spambots*.[227] 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. Evo primera poštanskog sandučeta (*inbox*) pretrpanog *spam* porukama:

[224] Izvor: *http://email.about.com/od/emailtrivia/f/emails_per_day.htm*, 1. 5. 2009.
[225] Izvor: *http://www.cybernothing.org/faqs/net-abuse-faq.html#2.1*, 1. 5. 2009.
[226] Izvor: *http://spamnation.info/stats/*, 1. 5. 2009.
[227] Izvor: *http://en.wikipedia.org/wiki/Spambot*, 1. 5. 2009.



Slika 8: Spam poruke u poštanskom sandučetu računara [228]

Kao što se može videti, neželjene 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 neželjenu poruku, u prilogu imejla (*attachment*), pošalje i neki virus (*malware)*, te 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.

Slika 9: Primer spam poruke sa virusom „crvićem" u prilogu (*attachment*) [229]

[228] Izvor: *http://commons.wikimedia.org/wiki/File:Email-spam-sample.png*, 1. 5. 2009.
[229] Izvor: *http://www.nortylemon.com/SPAM%20MAIL.htm*, 1. 5. 2009.

Neželjena pošta može da posluži i za *phishing* i razne druge prevare, gde se izgled tela imejl poruke preobražava/maskira, tako da upućuje na legitiman i pouzdan izvor (memorandum neke finansijske institucije), a, u stvari, služi za krađu identiteta ili otkrivanje poverljivih podataka kao što su računi u banci, korisnička imena i šifre itd.


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Slika 10: Izgled phisihing imejla
(obratiti pažnju da je nepravilno napisana reč recieved, a treba received) [230]

Moguće je i da se na računarima korisnika instaliraju razne neželjene aplikacije, koje koriste imejl nalog korisnika tog računara za slanje neželjene pošte bez njegovog znanja (u žargonu ti računari se zovu „zombi" računari). Najbolja zaštita u ovom slučaju je ažurirana antivirusna zaštita. U borbi protiv *spam* poruka prvi filter predstavljaju ISP (*Internet Service Provider* – firme koje pružaju internet usluge). Jasno je da neželjena pošta, u količinama sa kojima se danas susrećemo, predstavlja opterećenje za njihove resurse. Većina ISP-ova pruža svojim korisnicima usluge filtriranja elektronske pošte, preko veb portal aplikacija, koje koriste ili metodu prepoznavanja teksta u *Subject* polju poruke ili prate broj poslatih imejl poruka sa iste IP adrese. Od korisnika se očekuje da sam podesi ove filtere zato što postoji opasnost da se tokom ovog postupka blokira i legitimna pošta. U prvo vreme *spam* poruke su bile čist tekst u telu imejl poruke, a kada je metoda prepoznavanja teksta počela da daje rezultate, oni koji ih šalju dosetili su se da, umesto teksta, u telo poruke ubace sliku sa tekstom, koju zaštitni programi ne bi prepoznali kao *spam*. Ovo samo ilustruje večitu igru mačke i miša između ljudi koji su za-

[230] Izvor: *http://en.wikipedia.org/wiki/File:PhishingTrustedBank.png*, 1. 5. 2009.

duženi za bezbednost računara i onih koji bi da je kompromituju. U suštini, najbolja praksa je da se za registrovanje na razne veb portale ili internet prezentacije formira poseban imejl nalog (preko, recimo *google* ili *yahoo mail*-a), koji će služiti isključivo u te svrhe, a na internetu postoje i besplatne aplikacije koje vam mogu pomoći u odbrani od *spam* poruka (primer – *magic mail monitor*[231]), dajući vam uvid u poruke koje se nalaze na serveru (čime vam omogućavaju da, pre nego što preuzmete svoju elektronsku poštu, obrišete neželjene poruke direktno sa servera).

Cookies (kolačići) svoj naziv duguju kolačićima sudbine (*fortune cookies*),[232] 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 nalazi se aplikacija koja prepoznaje ove brojeve) i 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 u trajni, kada se nalaze na hard disku računara.[233]

Slika 11: Lokacija[234] *gde su smešteni „kolačići" na računaru pod Windows operativnim sistemom*[235]

[231] Izvor: *http://mmm3.sourceforge.net/*, 1 . 5. 2009.
[232] Izvor: *http://www.wisegeek.com/what-are-computer-cookies.htm*, 1. 5. 2009.
[233] Izvor: *http://www.wisegeek.com/what-are-computer-cookies.htm*, 1. 5. 2009.
[234] Obratiti pažnju na to da posle *C:\Documents and settings* ide ime korisnika računara (na primeru je to *Admin*).
[235] Izvor: *http://online-privacy.org/where-are-cookies-file-located-on-my-pc.html*, 1. 5. 2009.

Treba napomenuti da se mogu javiti slučajevi kada neke „kolačiće“ može koristiti 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 se „kolačići“ restriktivno prihvataju, ili čak i isključe, uz napomenu da neke internet prezentacije u ovom slučaju neće raditi.

Slika 12: Podešavanja vezana za „kolačiće“ na internet pretraživaču Mozilla Firefox 2.0.0.20

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“.[236] *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 korisnika 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

[236] Izvor: *http://en.wikipedia.org/wiki/Adware*, 1. 5. 2009.

da se njihovi programi zovu *spyware*, pa je iz *McAfee*-a (proizvođači bezbednosnih aplikacija) proizašao termin PUP (*Potentially Unwanted Program*),[237] 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*“,[238] 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 informacije koje su im korisne 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.]. Kao primere za ove programe navodimo razne *key logger* programe (koji pamte šta se kuca na tastaturi), zatim *dialer* programe (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 možete koristiti i neke besplatne programe, koji mogu da se pronađu na internetu, na primer *Spybot Search & Destroy*.[239]

[237] Izvor: *http://searchsecurity.techtarget.com/loginMembersOnly/1,289498,sid14_gci1066761,00.html*, 1. 5. 2009.

[238] Izvor: *http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214518,00.html#*, 1. 5. 2009.

[239] Izvor: *http://www.safer-networking.org/index2.html*, 1. 5. 2009.

VIII

ODNOS PRAVA NA PRIVATNOST I POTREBE ZA NADZOROM SAJBER PROSTORA

1. UVOD

Pravo na privatnost ličnog i porodičnog života je složeno ljudsko pravo, koje obuhvata nekoliko aspekata: privatnost doma, prepiske, komunikacije, intimnog i porodičnog života. Različite su posledice postojanja i praktikovanja ovog prava: privatni život svakog pojedinca, posebno onaj deo koji se odvija u njegovom domu, zaštićen je od bilo kakvog (neodobrenog) uvida javnosti; čak i kada je reč o javnim ličnostima koje su uvek pod budnim okom javnosti i medija, granice su jasno povučene i ne mogu se prelaziti. Na tome se zasnivaju presude kako nacionalnih, tako i međunarodnih sudova. Dom kao takav je zaštićen od neovlašćenog upada drugih lica, kao i predstavnika državnih vlasti i organa, osim u slučajevima koji su detaljno i jasno uređeni zakonom. Isti slučaj je i sa prepiskom, odnosno u novije vreme aktuelnom komunikacijom putem telefonskih i elektronskih uređaja. Zabranjeno je prisluškivati, ometati i presretati komunikaciju pojedinca ili grupe sa drugim pojedincima ili grupama – to je ustavni princip koji se mora poštovati i koji trpi mali broj zakonskih izuzetaka, povezanih za vršenje istražnih radnji povodom krivičnih dela.

Sa druge strane, postoji i zaštita pojedinca i grupa od uvida drugih pojedinaca u njihov privatni i porodični život. Država je, dakle, u specifičnom položaju – ona se uzdržava od narušavanja prava na privatnost, ali istovremeno i štiti građane od takvog ugrožavanja prava od strane nedržavnih subjekata, pojedinaca i organizacija.

Pravo na privatnost garantovano je kako domaćim propisima, tako i međunarodnim instrumentima.

„U cilju… povećanja sloboda izražavanja informacija i ideja, države članice treba da poštuju volju korisnika (interneta, *prim. aut.*) da ne otkriju svoj identitet.“[240]

Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda (EKLJP),[241] predviđa članom 8, stav 1 zaštitu privatnog i porodičnog života: „Svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske.“

[240] Deklaracija Komiteta ministara Saveta Evrope o slobodi komunikacije na internetu od 18. maja 2003. godine.

[241] Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda, Savet Evrope (1950); „Službeni list SCG – Međunarodni ugovori“, br. 9/2003.

U obimnoj praksi koja se tiče navodnih kršenja člana 8 od strane država potpisnica EKLJP,[242] nije mnogo prostora posvećeno prikupljanju podataka o ličnosti putem računara i drugih savremenih uređaja i tehnologija. Ipak, neke paralele se mogu izvesti kada je reč o postojećoj praksi, kada su pojedinci tvrdili da im je povređeno pravo na privatnost prepiske. Recimo, država koja prisluškuje telefonske razgovore pojedinca mimo načina koji je određen zakonom, ne može se braniti argumentom da su prisluškivani razgovori sadržali detalje o počinjenim krivičnim delima,[243] dok se za bilo kakvo presretanje komunikacije traži ispunjenje strogih kriterijuma: mora da postoji pravna kontrola u presretanju i na taj način mora da se štiti nacionalna bezbednost ili da se vrši prevencija nereda ili izvršenja krivičnog dela, a presretanje se može sprovesti samo ako postoje činjenice koje bi, *prema rezonu objektivnog posmatrača*, mogle da ukažu na zloupotrebu kanala komunikacije za nedozvoljene radnje.[244] Takođe, Sud je u svakom pojedinačnom postupku ocenjivao da li nacionalni zakoni zemalja u pitanju daju dovoljne garantije da se prisluškivanje neće zloupotrebiti, kao i da li se ono primenjuje samo kada je nužno neophodno.[245] Konačno, na osnovu prakse Suda, mora da postoji zaštita prikupljenih podataka o ličnosti, kao i njihova upotreba isključivo u svrhu za koju su prikupljeni.

Ukratko sažeti, uslovi za prisluškivanje komunikacija (presretanje podataka), prema dosadašnjoj praksi Suda, jesu sledeći:

– standardi za presretanje podataka moraju se jasno odrediti zakonom, dovoljno precizno kako bi se sprečila svaka njihova arbitrarna primena;

– dozvola (odobrenje) za presretanje mora da bude izdata od strane nezavisnog organa (najbolje od strane sudije);

– presretanje podataka može da se vrši samo u okviru istražnih radnji o teškim krivičnim delima;

– presretanje podataka može da se vrši samo ako postoje čvrsti dokazi da je prisluškivano lice umešano u kriminalne aktivnosti;

---

[242] Detaljnija analiza prakse Komisije i Evropskog suda za ljudska prava povodom člana 8 EKLJP u: Ivana Krstić, *Pravo na poštovanje privatnog i porodičnog života – član 8 Evropske konvencije o ljudskim pravima*, Beograd, 2006.

[243] *A. protiv Francuske*, predstavka broj 14838/89. Citirano prema: *ibidem*, str. 61.

[244] *Rinzivillo protiv Italije,* predstavka broj 31543/96; *Fox, Campbell i Hartley protiv Ujedinjenog Kraljevstva*, predstavke broj 12244/86, 12245/86, 12383/86. Kao i u prethodnom primeru, odluka Suda se odnosila na pismenu komunikaciju, ali smatramo da se može primeniti i na ostale vrste komunikacije, uključujući i one svojstvene upotrebi savremenih visokih tehnologija (tekstualne poruke preko mobilnih telefona, imejl poruke i sl.). Citirano prema: *ibidem*, str. 63.

[245] Videti, npr. *Klass protiv Nemačke*, predstavka broj 5029/71 ili *Malone protiv Ujedinjenog Kraljevstva*, predstavka broj 8691/79. Citirano prema: *ibidem*, str. 64–65.

– presretanje podataka može da se vrši samo kada ostale tehnike koje manje ugrožavaju privatnost ličnosti nisu dovoljne;

– svako odobrenje za prisluškivanje mora da se odnosi samo na određenu osobu ili događaj;

– pravila o prisluškivanju moraju da se odnose podjednako na sve komunikacije između dva lica, bez obzira na to da li uključuju glas, faks, slike ili podatke, žičnu ili bežičnu, digitalnu ili analognu komunikaciju;

– domašaj i vremensko trajanje prisluškivanja moraju da budu ograničeni;

– prisluškivanje mora da se vrši na način koji najmanje urušava privatnost lica, a da se pri tome mogu prikupiti potrebni dokazi;

– informacije koje su prikupljene ili presretnute na ovaj način mogu da se koriste samo u svrhe za koje se prisluškivanje vršilo, ili u svrhu nacionalne bezbednosti;

– sudija koji je odobrio prisluškivanje mora da dobije povratne informacije o njegovom sprovođenju;

– sva prisluškivana lica u okviru istražnih radnji o krivičnom delu moraju se nakon završetka prisluškivanja obavestiti o tome, bez obzira na to da li je protiv njih podignuta optužnica;

– moraju se omogućiti mehanizmi za naknadu štete ukoliko dođe do kršenja standarda o poštovanju privatnosti lica.[246]

Zaštita privatnosti lica je takođe jedan od ključnih ciljeva politike Evropske unije. Članovi 7 i 8 Povelje o osnovnim ljudskim pravima Evropske unije proklamuju pravo na poštovanje porodičnog i privatnog života, doma, komunikacije i privatnih podataka.

Kada je reč o pravnom sistemu Srbije, Ustav Republike Srbije[247] u čl. 40–42 predviđa nepovredivost stana, tajnost pisama i drugih sredstava opštenja,[248] kao i zaštitu podataka o ličnosti, dok Zakonik o krivičnom postupku[249] sadrži u članu 85 propisanu proceduru za privremeno oduzimanje pisama, telegrama i drugih pošiljki, na osnovu koga se ne može zaključiti da je zakonodavac imao u vidu bilo kakvu elektronsku komunikaciju, a čl. 14 i 147 re-

[246] Jim Dempsey, *Protecting Privacy and Freedom of Communication in the Fight against Cybercrime*, Southeast Europe Cybersecurity Conference, Sofija, Bugarska, 8–9. septembar 2003. Jim Dempsey je politički direktor organizacije *Global Internet Policy Initiative* (GIPI). Više o ovoj organizaciji na internet adresi: *http://www.internetpolicy.net/*, 1. 5. 2009.

[247] „Službeni glasnik RS“, br. 98/2006.

[248] Član 41 Ustava Republike Srbije: „Tajnost pisama i drugih sredstava komuniciranja je nepovrediva. Odstupanja su dozvoljena samo na određeno vreme i na osnovu odluke suda, ako su neophodna radi vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom.“

[249] „Službeni glasnik RS“, br. 46/2006, 49/2007.

guliše se tajni zvučni i optički nadzor osumnjičenog – opet nema odredaba o elektronskoj komunikaciji, a među delima za koja sud može izreći ovakvu istražnu meru nema dela visokotehnološkog kriminala. Konačno, Zakon o zaštiti podataka o ličnosti[250] sadrži čitav niz odredaba koje imaju cilj ostvarivanje prava na privatnost svakog pojedinca prilikom obrade podataka koji su vezani za njega.[251]

Kada je reč o samom ugrožavanju, odnosno kršenju ovog prava u savremenom okruženju, mogućnosti su raznovrsne i gotovo neiscrpne. Mnogi postupci koje pojedinci ili organizacije čine, a koji bi se mogli podvesti kao kršenje prava na privatnost, ne spadaju u dela visokotehnološkog kriminala; zapravo, ona i dalje ne spadaju u kažnjive ili zabranjene vrste ponašanja. Pravo na privatnost se, dakle, može kršiti na dva načina, kada je reč o upotrebi savremenih tehnologija: od strane pojedinaca, grupa ili organizacija, kao i državnih organa i institucija; od strane policije i drugih nadležnih organa u istraživanju dela visokotehnološkog kriminala.

[250] „Službeni glasnik RS“, br. 97/08.

[251] Ovaj Zakon je naročito relevantan kada je reč o prikupljanju i obradi podataka koji se vezuju za korišćenje interneta.

2. KORIŠĆENJE RAČUNARA I DRUGIH VISOKOTEHNOLOŠKIH UREĐAJA I PRAVO NA PRIVATNOST LIČNOSTI

Kada je reč o upotrebi računara i računarskih mreža i sistema a naročito interneta kao sredstva komunikacije, najdrastičniji oblik narušavanja privatnosti je sasvim sigurno krađa identiteta osobe u cilju sticanja materijalne ili druge koristi. Postoje, međutim, i drugi oblici invazije na privatnost lica, koji u većini slučajeva nisu inkriminisani kao kažnjiva dela: korišćenje tuđih podataka ili lika bez namere da se preuzme identitet lica; korišćenje podataka koje osoba ostavi na internetu, u reklamne svrhe;[252] prodaja imejl adresa firmama radi slanja *spam* poruka. Svi ovi postupci spadaju u narušavanje prava na privatnost lica, kao i drugih ličnih prava. Treba primetiti da se oni, ipak, znatno razlikuju u načinu izvršenja i ostvarenoj koristi, kao i društvenoj opasnosti koju nose. Kako, npr. okarakterisati predstavljanje pod tuđim likom? Ovo je zanimljivo pitanje koje do danas nije rešeno u zakonodavstvima, kako u Srbiji, tako i u drugim državama. Očigledno je da krađa tuđeg lika u ovom slučaju ne povlači posledice koje bi bile društveno opasne – osim ukoliko se neko lice ne služi tuđim likom da bi izvršilo neko drugo krivično delo (npr. često se pedofili na internetu predstavljaju kao deca kako bi zadobili poverenje svojih potencijalnih žrtava). Ipak, licu čije se slike – koje se mogu naći na internetu, na tzv. socijalnim sajtovima koji služe za upoznavanje i povezivanje ljudi – koriste od strane drugih, nepoznatih lica u svakom slučaju ne može biti prijatna sama ta činjenica i njegovo pravo na privatnost mora se smatrati povređenim.[253] Koliko mogu da budu jednostavni slučajevi „upada“ u tuđe privatne informacije, govori i česta pojava prilikom deljenja jednog računara

[252] Poznat je skorašnji primer popularnog internet sajta *Facebook*, koji je odlučio da ne briše profile (naloge) svojih korisnika koji odluče da prestanu da ih koriste. Profili, koji često sadrže razne privatne podatke – po pravilu imejl adresu korisnika i njegove fotografije, pa čak i takve kao što su brojevi telefona i kućna adresa, čuvani su kao neaktivni i nakon što bi ih korisnik „obrisao“. Iako je *ratio* za ovakvu odluku bio lakši povratak na *Facebook* korisnika koji su prethodno imali profile pa su ih deaktivirali, ovakav potez nije naišao na odobravanje korisnika, i pre nego što je cela stvar uopšte mogla da dobije neki pravni – sudski epilog, pravilo o trajnom čuvanju profila je ukinuto i deaktivirani profili su obrisani.

[253] Ovde postoji još jedan problem, a to je autorstvo na tzv. javnim slikama, koje se mogu slobodno preuzimati, i za čije korišćenje ne postoje nikakve prepreke, niti upozorenja na sajtovima na kojima se nalaze.

između više lica – slučajni ulazak u imejl nalog drugog korisnika, kada se ovaj prilikom prethodne upotrebe na „izloguje“.[254]

Nezavisno od korišćenja računara, nove tehnologije, nastale pre svega u cilju da nam olakšaju svakodnevni život, mogu često da se koriste kao sredstvo za ugrožavanje privatnosti. Postoje, npr. ozbiljne diskusije na temu kamera za nadzor na javnim mestima. Ove kamere su uobičajeni deo elektronskog obezbeđenja u državnim institucijama i privatnim firmama, stambenim i poslovnim zgradama. One mogu da budu postavljene i na nekim javnim mestima isključivo iz razloga bezbednosti – npr. kamere na semaforima i autoputevima, koje snimaju nesavesne i neoprezne vozače. Svako lice može da postavi kamere ispred svog objekta, ili unutar njega. Šta se dešava kada se kamere postave na javnim mestima, tako da lica koja prolaze ulicom nisu ni svesna da su predmet snimanja i nadzora? Ove kamere su sve češće u upotrebi, često se koriste i u direktnim televizijskim prenosima (npr. u izveštajima o stanju saobraćaja u pojedinim delovima grada), a mogu se naći i u prenosima uživo na internetu, neretko uz mogućnost zumiranja kadrova. Ovaj sindrom „velikog brata“ koji sve posmatra ne može se smatrati kršenjem prava na privatnost u pravom smislu, jer pravo na lik nije zaštićeno na javnim lokacijama – npr. televizije često snimaju određene sekvence na ulicama koje se potom emituju na televiziji, uvek uz određenu vrstu novinarskog priloga. Međutim, za razliku od novinarskih priloga, u ovom slučaju nema selekcije materijala koji je dostupan širokom krugu lica – najčešće svakome sa kvalitetnom internet konekcijom, bez ograničenja ili uz minimalna ograničenja koja zavise od tehničkih mogućnosti postavljenih uređaja za snimanje. Tako, može se desiti da materijal koji nije prikladan za svačije oči bude dostupan svakom uzrastu – npr. dete može da „prisustvuje“ saobraćajnoj nesreći sa fatalnim ishodom.

Poseban vid ovog problema je i kontroverzni program koji je lansirala kompanija *Google – Google Street View*, koji može da pokaže slike iz različitih ulica većih gradova širom sveta (videti sliku 13). Ovaj program se zasniva na realnim slikama ulica uživo, na kojima se nalaze ljudi, automobili i sl. Koliko se duboko na ovaj način zadire u pravo na privatnost? Možda ne najpreciziji, ali u svakom slučaju zanimljiv odgovor može da ponudi gospođa iz Velike Britanije, koja je pokrenula brakorazvodnu parnicu nakon što je slučajno na snimku jedne od ulica videla parkiran automobil svog muža ispred

[254] Veliko je pitanje, na koje i dalje ne postoji nedvosmislen odgovor, da li su podaci koje zaposleni ostavi na računaru prilikom njegovog korišćenja na poslu privatni podaci tog lica, ili pripadaju poslodavcu? Ova dilema je nastala prethodnih godina, kada su zaposleni masovno koristili internet konekciju i računar na radnom mestu da bi završavali različite obaveze, ali i igrali onlajn igrice, posećivali socijalne sajtove i sl.

nepoznate kuće, u vreme kada je on navodno bio na službenom putu.[255] Ovo nije prvi primer ovakvog procesa, a optuženi se uglavnom brane zahtevima za odbacivanje ovakvih dokaza prikupljenih narušavanjem privatnosti. Ostaje da se vidi kako će sudovi reagovati na ovaj novi vid dokazivanja i da li će se dokazi prikupljeni na ovaj način oceniti kao validni za sudske postupke. Ukoliko odgovor bude pozitivan, nesumnjivo je da će to otvoriti vrata za mnoge nove programe sličnog tipa, koji će sve dublje zadirati u sferu privatnosti ličnosti.

Slika 13: Screenshot programa Google Street View

Kao što je napomenuto, internet može da se koristi i za prikupljanje različitih podataka o ličnosti, koji potom mogu da se upotrebe u reklamne svrhe. Iako u Srbiji kultura kupovine i plaćanja raznih računa putem interneta i elektronskog bankarstva još nije sasvim zaživela, u mnogim državama to je uobičajeni način kupovine. Na osnovu podataka koje neko lice na taj način ostavi, može se rekonstruisati čitav njegov privatni život, navike, bračni status, da li ima kućnog ljubimca i sl. Slično može da se dogodi i osobama koje plaćaju kreditnom karticom u prodavnicama – poznati su primeri iz Nemačke gde su osobe koje su u supermarketima kupovale, npr. hranu za pse, posle izvesnog vremena počele da dobijaju kataloge opreme za kućne ljubimce na kućnu adresu. Iako ovakav način „prodaje“ ličnih podataka od strane prodavnica ili banaka koje izdaju kreditne kartice ne može biti legalan, jer se kosi sa propisima o zaštiti podataka o ličnosti, realno je očekivati da se ovakve zloupotre-

[255] Izvor: Blic online, *Preko Gugla otkrila preljubu*, *http://www.blic.rs/zanimljivosti.php?id=86407*, 1. 5. 2009.

be poverenja potrošača mogu nastaviti i u budućnosti, jer je gotovo nemoguće identifikovati (neformalne) kanale prenosa ovih informacija. Sa druge strane, korišćenje ovakvih podataka može ne samo da zadire u privatni život pojedinaca nego i da predstavlja i potencijalnu uvertiru u činjenje drugih krivičnih dela – recimo, prodajom turističkih aranžmana mogu da se odrede datumi kada određena osoba (porodica) neće biti u svom domu[256] i sl. Ostaje da se vidi kako će se zakonodavac, ali i nadležni državni organi, izboriti sa ovim problemima koji nastaju zloupotrebom različitih savremenih tehnologija.

[256] Ovakav slučaj je poznat iz prakse, ali posredi su bili turistički aranžmani koji su prodavani onlajn, putem interneta.

3. ISTRAŽNE RADNJE DRŽAVNIH ORGANA KOJE MOGU DA UGROZE PRAVO NA PRIVATNOST LIČNOSTI

Kada su države u osvit XXI veka počele ozbiljno da se bave istraživanjem dela visokotehnološkog kriminala, postavilo se pitanje koliko istražni organi mogu (smeju) da zadiru u privatnost građana? Pravo na privatnost nije apsolutno i ono trpi znatna ograničenja kada je reč o istraživanju krivičnih dela. Kako se, međutim, klasične mere i istražne radnje, klasični standardi invazije privatnosti pojedinca mogu upotrebiti kada je reč o virtuelnom svetu? Veoma brzo je postalo očigledno da dela počinjena putem računara i na računarskim mrežama uopšte nije lako ni percipirati, a da se tragovi o njihovom postojanju lako i efikasno uklanjaju od strane počinilaca, ali i drugih faktora. Samim tim, bilo je potrebno razviti specifična ovlašćenja istražnih organa, a pre svega policije, prilikom sprovođenja istražnih radnji za neko od dela visokotehnološkog kriminala. Preovladavalo je stanovište da je obim ovih ovlašćenja i dalje neodređen i da će tek praksa pokazati kako će se ona dalje razvijati.[257] Od tada je prošlo nekoliko godina, a uporedo sa razvojem visokotehnološkog kriminala, iskristalisale su se mere kako se on može sprečiti i istraživati. Istovremeno, rasla je i zabrinutost da li te mere zadiru suviše u pravo na privatnost komunikacije pojedinca na računarskim mrežama, kao i pravo na privatnost podataka koje pojedinac čuva u svom računaru.

Evropska konvencija o visokotehnološkom kriminalu navodi određene procesne (istražne) radnje koje mogu da se izvršavaju prilikom istraživanja dela visokotehnološkog kriminala. U ove radnje, između ostalih, spadaju: hitna zaštita sačuvanih računarskih podataka, hitna zaštita i delimično otkrivanje podataka u saobraćaju, izdavanje naredbe o predaji, kao i zaplena i pretraživanje sačuvanih računarskih podataka, prikupljanje podataka o saobraćaju u realnom vremenu, presretanje poruka. Očigledno je da su dela povezana sa upotrebom računara i drugih savremenih tehnologija specifična, i da policija i tužilaštvo moraju da imaju na raspolaganju široku paletu različitih sredstava i mehanizama kako bi obezbedili dokaze o počinjenom delu i počiniocu. Međutim, nabrojana sredstva koja će im po Konvenciji u budućnosti biti dostup-

[257] Ekatarina A. Drozdova, *Civil Liberties and Security in Cyberspace*, u: Abraham D. Sofaer, Seymour E. Goodman (ur.), *The Transnational Dimension of Cyber Crime and Terrorism*, Hoover Press, 2001, str. 204.

na otvaraju veliku dilemu: koliko se njima zadire u privatnost ličnosti, odnosno – da li je pojavom osnova sumnje da se neko lice bavi nedozvoljenim radnjama koristeći računar, njegova privatnost u pogledu informacija koje se nalaze kako na računaru, tako na računarskim mrežama koje koristi (posebno na internetu) znatno ograničena procesnim pravilima istrage? Očigledno je da su i tvorci Konvencije imali na umu ovu dilemu kada su u članu 15 Konvencije, na početku procesnopravnog dela teksta, naglasili: „Svaka strana ugovornica treba da obezbedi da uspostavljanje, sprovođenje i primena ovlašćenja i postupaka navedenih u ovom odeljku, podleže uslovima i ograničenjima predviđenim domaćim pravom, koje mora da omogući odgovarajuću zaštitu ljudskih prava i sloboda, uključujući i prava koja proizlaze iz obaveza koje je strana ugovornica preuzela na osnovu Konvencije Saveta Evrope o zaštiti ljudskih prava i osnovnih sloboda iz 1950. godine, Međunarodnog pakta Ujedinjenih nacija o građanskim i političkim pravima iz 1966. godine i ostalih važećih međunarodnih dokumenata o ljudskim pravima, i koje će da sadrži načelo proporcionalnosti. Ti uslovi i ograničenja mogu, u zavisnosti od vrste ovlašćenja ili postupaka o kojima je reč, između ostalog, da obuhvate sudsku ili drugu vrstu nezavisne kontrole, na osnovu kojih se opravdava primena i ograničenje obima i trajanja tih ovlašćenja ili postupaka. U meri u kojoj je to u skladu sa javnim interesom, a naročito sa pravilnom primenom prava, svaka strana ugovornica treba da razmotri posledice ovlašćenja i postupaka iz ovog odeljka na prava, odgovornosti i opravdane interese trećih strana.“[258]

Koliko su ova ograničenja dovoljna da se privatnost korišćenja računara i računarskih mreža sačuva? Smernice za saradnju između organa za sprovođenje zakona i internet provajdera u borbi protiv visokotehnološkog kriminala, koje je objavio Savet Evrope 2008. godine,[259] smatraju da su internet provajderi (*Internet Service Provider*, ISP) i policijsko-tužilački istražni organi

[258] Iako se u poslednje vreme situacija menja, treba napomenuti da je većina tehnološki razvijenih zemalja koje nisu potpisale Konvenciju kao jedan od glavnih razloga takvog postupanja navela da bi na taj način bile obavezne da u svoja nacionalna zakonodavstva unesu odredbe koje bi značile znatno zadiranje u prava građana, odnosno u pravo na privatni život ličnosti.

[259] *Guidelines for the cooperation between law inforcement and internet service providers against cybercrime*; dokument je usvojen na Globalnoj konferenciji o saradnji protiv visokotehnološkog kriminala u organizaciji Generalnog direktorata za ljudska prava i pravne poslove Saveta Evrope, 1. i 2. aprila 2008. godine. Smernice ne predstavljaju obavezujući dokument i cilj njihovog stvaranja je pre svega edukacija pripadnika policije i tužilaštva kada je reč o istraživanju dela visokotehnološkog kriminala. Mogu se, između ostalog, pronaći i na internet adresama *http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_activity_Interface 2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf* i *http://www.ifap.ru/library/book294.pdf,* 1. 5. 2009.

osnova na kojoj počiva sistem za otkrivanje i istraživanje ove vrste krivičnih dela. Otuda je za svaku državu važno da njihov odnos reguliše na način koji bi omogućio nadzor nad saobraćajem na internetu, ali istovremeno garantovao zaštitu svih prava korisnika računara, odnosno svetske mreže. Čak se zaštita privatnosti podataka u saobraćaju posebno pominje kao jedan od ciljeva kojima efikasna saradnja mora da teži.[260] Od drugih načina sprečavanja zloupotreba ovakvih postupaka, Smernice izričito preporučuju da se svaki nalog koji potiče od tužilaštva ili policije može dostaviti isključivo u dokumentovanom obliku (napismeno), a u ekstremno hitnim slučajevima kada je moguć samo usmeni dogovor, dokumentacija mora da bude naknadno dostavljena, bez odlaganja. Zahtevi moraju da budu jasni i nedvosmisleni, odnosno precizni i usmereni samo na one podatke koji su nužno neophodni radi sprovođenja istražnih radnji. Takođe, svi podaci koje ISP dostave istražnim organima moraju da budu poverljivi i da se upotrebljavaju samo u svrhe zbog kojih su prikupljeni.[261]

Uporednopravno gledano,[262] standardi koji su uspostavljeni kada je reč o zapleni računara ili bilo kom drugom načinu korišćenja privatnih podataka u istrazi, veoma su visoki i odgovaraju uspostavljenom nivou poštovanja ljudskih prava.[263] Takođe, uspostavljen je princip proporcionalnosti mera koje će se preduzeti i težine krivičnog dela u pitanju, tako da se invazione mere ne primenjuju na lakše oblike dela, kao ni u slučajevima kada ne mogu imati racionalnu svrhu. U slučajevima kada se mogu preduzeti sa realnim očekivanjima da će dovesti do otkrivanja krivičnog dela ili omogućiti njegovo procesuiranje, primenjuju se različita ograničenja.

Tako, npr. u Belgiji i Mađarskoj vlasnik podataka ili administrator sistema mora da bude obavešten o tome koji su podaci kopirani u toku istrage;

[260] *Guidelines for the cooperation between law inforcement and internet service providers against cybercrime*, tačke 14 i 15.

[261] *Ibidem*, tačke 25–28 i 32.

[262] Pri istraživanju nacionalnih zakonodavstava o procesnim odredbama koje mogu ugroziti ili ograničiti pravo na privatnost ličnosti, korišćeni su podaci objavljeni u analizi za Evropsku komisiju: Lorenzo Valeri, *et alia*, *Handbook of Legal Procedures of Computer and Network Misuse in EU Countries* (2006), kao i u nacionalnim izveštajima država upućenim Savetu Evrope, koji se mogu naći na internet adresi: *http://www.coe.int/cybercrime*, 1. 5. 2009.

[263] Treba napomenuti da je u posmatranim zemljama deo uobičajene sudske prakse izvođenje elektronskih dokaza, koji se smatraju validnim kao i svi drugi dokumenti – ako podnosilac može da dokaže njihovu autentičnost. Otuda su forenzičke istrage fokusirane na kopiranje postojećih podataka pre nego njihove fizičke zaplene, naravno, osim u slučajevima kada je to neophodno (postoji opasnost od širenja računarskog virusa, nemoguće je napraviti kopiju podataka i sl.).

podaci koji se nalaze na računarskim mrežama kopiraće se samo ako postoji realna opasnost da će u protivnom biti trajno izbrisani; u svakom slučaju, kopiraće se samo podaci koji su nužni za sprovođenje krivičnog postupka – ovaj standard „minimuma uzurpiranja privatnosti" nalazimo i u drugim zemljama, npr. u Estoniji, Španiji, kao i u austrijskom Zakoniku o krivičnom postupku. Takođe, u Belgiji, Austriji i Finskoj postoji standard tajnosti preuzetih podataka i njihove upotrebe samo u svrhe sprovođenja istrage i krivičnog postupka. Postoje i druga specifična ograničenja – npr. nemački Zakonik o krivičnom postupku predviđa da ove podatke mogu pregledati samo tužioci, ali ne i policijski organi.[264]

Dalje, dokazi koji se nalaze na računaru mogu se prihvatiti u postupku protiv određenog lica ukoliko tužilac može da dokaže da je računar radio normalno u vreme njegove zaplene, odnosno da se to lice zaista koristilo nedozvoljenim sadržajem sa računara (audio i video-zapisi, dokumenti, štetni programi i sl.), kao i da se sadržina hard diska i ostalih nosača informacija na računaru nije promenila od trenutka njegove zaplene do trenutka izvođenja dokaza. U suprotnom, vršenje alternacija na računaru smatra se kontaminacijom dokaza. Ovakvo rešenje postoji, npr. u kiparskom zakonodavstvu (Zakon o dokazima i Zakon o krivičnom postupku), kao i u Ujedinjenom Kraljevstvu (Zakon o policiji i dokazima u krivičnom postupku i policijski Vodič kroz dobru praksu pri sakupljanju računarskih dokaza).

Za pretraživanje prostorija (stana, poslovnog prostora) uglavnom se traže isti uslovi kao kod bilo kog drugog krivičnog dela – policija može da pristupi pretraživanju (pretresu) sa sudskim nalogom, a bez njega, samo u slučaju da postoje osnove sumnje da je u tim prostorijama neko krivično delo izvršeno u bliskoj prošlosti, trenutno je u izvršenju ili će se izvršiti u bliskoj budućnosti.[265] Krivično delo u pitanju mora da bude teže prirode, s tim što različita zakonodavstva postavljaju različite uslove kada će se ono tako posmatrati.

Kada je reč o prisluškivanju komunikacija i presretanju podataka, takođe može da se povuče paralela sa „klasičnim" istražnim metodama – obavezno je odobrenje suda (u Finskoj je, npr. u pitanju viši sud) i ove radnje mogu da traju ograničeno vreme. U Estoniji je, npr. izričito naglašeno da tzv. „internet monitoring" nije svakodnevna policijska aktivnost i da se može vršiti samo u slučajevima kada postoje osnovi sumnje da se određene komunikacije koriste za vršenje dela visokotehnološkog kriminala. Francuski Zakon o krivičnom postupku (član 100) postavlja i dodatni uslov za presretanje podataka – in-

[264] Član 110 Zakonika o krivičnom postupku Nemačke.

[265] U Nemačkoj i u tom slučaju policija mora da pribavi nalog, ali ne od suda, nego od tužioca (član 105 Zakonika o krivičnom postupku).

formacije koje će se na ovaj način prikupiti moraju da budu od posebnog značaja za istraživanje krivičnog dela. Nemački Ustav (Osnovni zakon) štiti prava građana na privatnost u komunikaciji – otud, presretanje može da se vrši samo za krivična dela od naročitog značaja (ugrožavanje nacionalne bezbednosti, terorizam i sl.) dok se za sva ostala dela mora pribaviti nalog suda, ili tužioca u hitnim slučajevima. U Poljskoj je presretanje podataka i osluškivanje elektronskih komunikacija moguće samo za dela koja su izričito navedena u Zakonu o policiji i Zakonu o krivičnom postupku, a dela visokotehnološkog kriminala mogu da budu predmet ovakvih mera samo ako se dokaže da su ona bila jedna od faza izvršenja nekog složenijeg, težeg krivičnog dela.

U nizu zemalja ne postoje posebne odredbe za istraživanje dela visokotehnološkog kriminala: Italija (sa nekoliko izuzetaka), Belgija, Portugal, Estonija, Holandija, Letonija, Litvanija, Slovenija, Luksemburg, Poljska itd. U ovim državama se krivična dela povezana sa upotrebom računara istražuju i procesuiraju na osnovu ekstenzivnog tumačenja postojećih odredaba o istražnim i drugim radnjama. U svakom pojedinačnom slučaju, tužioci ili sudije su ti koji određuju šta može da se sprovede kao istražna radnja, kao i koji dokazi mogu da budu prihvaćeni u toku postupka. Ipak, osnovni zaključak koji se nameće jeste da su sudovi prihvatili sve specifičnosti u postupku dokazivanja dela visokotehnološkog kriminala kao nužno potrebne, kao i da su elektronski dokazi uobičajena pojava u ovakvim postupcima. To istovremeno znači da se oni moraju prikupljati sa posebnom pažnjom i da i za njihovo pribavljanje moraju da važe isti standardi poštovanja ljudskih prava, naročito prava na privatnost, kao i ostala materijalna i procesna ograničenja zapisana u nacionalnim zakonima.

IX

TEHNIČKE MOGUĆNOSTI POLICIJE I TUŽILAŠTVA ZA SUZBIJANJE VISOKOTEHNOLOŠKOG KRIMINALA

TEHNIČKE MOGUĆNOSTI POLICIJE I TUŽILAŠTVA ZA SUZBIJANJE VISOKOTEHNOLOŠKOG KRIMINALA

Savremeni pojavni oblici kriminala zahtevaju novu metodiku otkrivanja krivičnih dela, koja podrazumeva i pribavljanje dokaza u elektronskoj formi, odnosno elektronskih, softverskih ili kompjuterskih dokaza, kako ih nazivaju u teoriji i u još nedovoljno izgrađenoj praksi. S obzirom na to da se kriminal koji se vrši putem visokih tehnologija odvija na raznim poljima, kompjuter i drugi uređaji i sredstva visoke tehnologije mogu se u odnosu na ovaj kriminal pojaviti bilo kao predmet krivičnog dela, odnosno objekat napada, bilo kao sredstvo izvršenja krivičnog dela. Ovo je prisutno ne samo u oblasti kompjuterskog već i u oblasti opšteg, ali i finansijskog i ekonomskog kriminala, to jest u svim kriminalnim slučajevima gde se kao sredstvo izvršenja, ili kao sredstvo za prikrivanje krivičnog dela ili učinioca, pojavljuje bilo koji uređaj čije je funkcionisanje zasnovano na visokoj informatičkoj tehnologiji, odnosno elektronskoj tehnologiji.

Kriminalno ponašanje u ovoj oblasti odvija se u vrlo specifičnoj – elektronskoj sredini. Stoga, uspešno suprotstavljanje ovoj vrsti kriminala podrazumeva poznavanje funkcionisanja uređaja koji rade na principima visoke tehnologije, poznavanje kompjuterskih sistema i mreža i modernih telekomunikacionih tehnologija. Osnovna funkcija kompjuterskog sistema je obrada i distribucija podataka u elektronsku sredinu. Podatke koji se nalaze u formi pogodnoj za ljudsko opažanje i razumevanje, operater korišćenjem računara prebacuje u formu pogodnu za automatsko obrađivanje, dakle, oni se kroz interaktivni odnos čoveka i uređaja pretvaraju u podatke u elektronskoj formi. Elektronski podaci sami po sebi sada predstavljaju niz magnetskih tačkica na stalnoj ili privremenoj memoriji računara i oni mogu da budu primarni dokaz. U takvom obliku ne mogu se čulno opaziti, ali se mogu koristiti kao dokaz. Moguće ih je presnimiti na drugi oblik elektronske memorije: tvrdi ili meki disk (flopi disketu), optički kompakt disk, eksternu memoriju (izmenljivi disk) i tako obezbediti u neizmenjenom obliku, a da bi se čulno opazili, pretvaramo ih pomoću uređaja i programa u tekst, fotografiju, video- zapis, zvuk ili drugi oblik koji je pogodan za ljudsko opažanje i razumevanje.

Kada operater može da identifikuje i kontroliše podatak, može se smatrati da je takav podatak materijalni objekat, kao što je, na primer, podatak zabeležen na tvrdom (*hard*) disku, izmenljivom disku – popularnoj fleš memoriji

(USB *flash disc*), disketi (*flopy disc*), na kompakt disku (CD), magnetnoj traci i dr. Takav podatak je moguće i čulno opaziti u vidu slike na monitoru, zvuka, pisanog teksta ili slika odštampanih pomoću kompjuterskih štampača, ili kombinacije svega navedenog. Ovo je veoma važno sa aspekta pribavljanja, obezbeđivanja i korišćenja dokaza koje na uređaju pronađemo u elektronskoj formi, jer podatak koji je obrađivan u kompjuterskom sistemu ne može se više identifikovati i kontrolisati od strane operatera bez poznavanja i poštovanja određenih postupaka i korišćenja specifičnih tehničkih sredstava. Informacioni sistem automatski prebacuje podatke od jednog mesta na memoriji do drugog. U kompjuterskim mrežama za osobu koja kontroliše podatke nemoguće je da fizički locira obrađene podatke, bilo u celini ili delimično, bez posebnih procedura i tehničkih sredstava. Budući da takvi podaci mogu da budu kontrolisani samo uz pomoć „logičkih" operacija, a ne uz pomoć fizičkih, bilo bi teško tretirati ih kao definisanje objekta.

Preporuke Saveta Evrope iz 1989. i 1995. godine ističu potrebu nacionalnih izvršnih vlasti da osnuju i prošire broj specijalizovanih jedinica za kompjuterski kriminalitet. Ove jedinice treba da budu adekvatno obučene i da raspolažu neophodnom tehničkom opremom i softverskim sistemom. Mnoge države su već formirale takve jedinice za kompjuterski kriminalitet. Veliki broj njih je stvorio profesionalce koji poseduju tehnička znanja i sposobnosti i raspolažu proceduralnim instrukcijama kako istrage treba da se sprovedu, a da se istovremeno smanji rizik od gubitka dokaza, kao i da se obezbedi njihova prihvatljivost na sudu.

Jedan od najvećih problema u vezi sa otkrivanjem i krivičnim gonjenjem kompjuterskog kriminala predstavljaju elektronski dokazi. Razvoj visokih informacionih i telekomunikacionih tehnologija brži je nego što možemo da zamislimo. S druge strane, neki zakoni su doneti pre više decenija, tako da oni ne odgovaraju današnjem tehnološkom i ekonomskom razvoju društva.

Problem je da li elektronski dokaz i pod kojim uslovima može da se smatra kao materijalni, u istom smislu kao dokument, knjiga, spis, magnetofonska i video-traka, fotografija i nesporni potpis. Na primer, da bi se dokazalo krivično delo iz oblasti ekonomskog i finansijskog kriminala, potrebno je pribaviti određenu poslovnu dokumentaciju (fakture, otpremnice, izvode promena na žiro računu kod poslovne banke i dr.). Moderno poslovanje podrazumeva vođenje kompjuterskog knjigovodstva, koje omogućava brzinu i tačnost formiranja knjigovodstvenih dokumenata, neuporedivo veću brzinu računskih operacija koje se vrše pri knjiženju, daje mogućnosti za brže i efikasnije pretraživanje poslovne dokumentacije, ali, s druge strane, stvara i mogućnost zloupotreba u smislu formiranja lažne dokumentacije, koja ima sve karakteristike intelektualnog falsifikata. Dakle, dokazi za osnovno krivično delo koji

se prikrivaju tim falsifikatima moraju se pronaći u kompjuteru ili kompjuterskoj mreži pravnog lica prilikom vršenja uvida u određenu poslovnu dokumentaciju. Ovaj uvid se umesto na klasičan način, listanjem i pregledanjem dokumenata, sada vrši izlistavanjem kompjuterski formiranih dokumenata, koje treba pronaći u memoriji uređaja na kojem se knjigovodstvo vodi. Dakle, otkrivanje i pronalaženje ovakve dokumentacije, kao i utvrđivanje da li je ona autentična ili naknadno menjana, zahteva poznavanje procedura i načina rada kompjuterskog knjigovodstva, ali i posebna informatička znanja koja, uz upotrebu specijalnih softvera za pronalaženje podataka i ponovno izazivanje brisanih podataka, odnosno utvrđivanje izmena podataka u memoriji uređaja ili na dokumentima, kao i komunikacije koja je vršena kroz mrežu, treba da obezbede pribavljanje i fiksiranje kvalitetnih dokaza.

Postavlja se pitanje da li radi obezbeđivanja dokaza treba izvršiti privremeno oduzimanje uređaja na kojem se vodi knjigovodstvo, odnosno hard diska na kojem se relevantni podaci čuvaju, ili se dokazom može smatrati kopija tih podataka napravljena na licu mesta po određenoj proceduri. U dosadašnjoj praksi, privremeno je oduzimana samo dokumentacija koja se odštampa na papiru, a zatim je potpisom i pečatom overi odgovorno lice. U određenim slučajevima to je možda dovoljno, ali je to metodološki pogrešan pristup. U memoriji uređaja, osim dokumenta u obliku koji je dostupan, nalaze se i drugi relevantni podaci, na primer, skriveno, „crno“ knjigovodstvo ili brisani podaci, koji se određenim postupcima i uz korišćenje posebnih softverskih alata mogu restituisati.

Problem primarnog i sekundarnog dokaza izražen je ovoj oblasti. Naime, u zakonodavstvima nekih zemalja sekundarni dokazi mogu da se prihvate samo u slučaju da se ne raspolaže primarnim dokazima. Proceduru dolaženja do dokaza u elektronskoj formi neophodno je materijalizovati sačinjavanjem zapisnika, u kojima se detaljno opisuju primenjene procedure, fotografisanjem, audio-video dokumentovanjem, prisustvom svedoka i stručnih lica u postupku. Sve ovo se radi u cilju da se otkloni sumnja da su dokazi pribavljeni na zakonit način i da se potvrdi da su u potpunosti fiksirani u obliku u kojem su i zatečeni na licu mesta. Organi otkrivanja i krivičnog gonjenja moraju da poštuju ovu metodiku i procedure kako u kasnijoj fazi postupka dokazi ne bi bili osporeni.

Ukoliko ne postoji mogućnost da se dokazi pribave odmah i direktno na licu mesta, neophodno je kompjutersku opremu ili druge uređaje bezbedno isključiti, zapečatiti i privremeno oduzeti na način koji obezbeđuje da ne dođe do uništenja, brisanja ili izmene dokaza koji se u elektronskoj formi nalaze na tim uređajima. Ovi dokazi se mogu fiksirati kasnije u laboratorijskim ili drugim pogodnim uslovima, uz obavezno prisustvo osumnjičenog ili lica od

kojeg su ovi uređaji oduzeti ili, pak, odgovornog lica u pravnom licu ili državnom organu. Ukoliko je fizički nemoguće oduzeti uređaje i opremu, ili delove uređaja, treba obezbediti i zapečatiti prostoriju u kojoj se oni nalaze, a prethodno onemogućiti ne samo fizički već i pristup uređaju sa daljine žičnim ili bežičnim putem, odnosno isključiti ga iz mreže, kako bi se dokazi sačuvali u neizmenjenom obliku.

U oblasti suzbijanja kompjuterskog kriminala potrebno je primenjivati i specijalne istražne tehnike kao što su elektronsko praćenje, presretanje elektronskih komunikacija ili druge oblike nadzora. To mogu da budu i tajne operacije za potrebe borbe protiv organizovanog kriminala. Za primenu ovih tehnika neophodno je najpre stvoriti zakonski i institucionalni okvir, kao i izvršiti edukaciju i osposobljavanje pripadnika policije za elektronsko praćenje, što bi posebno predstavljalo utvrđivanje lokacije lica preko IP adresa, bez čega neće biti moguće ostvariti efikasno gonjenje učinilaca koji se prilikom izvršenja krivičnog dela koriste kompjuterskom tehnologijom.

To navodi na činjenicu da je neophodno u što kraćem roku izvršiti dopunu pozitivnih zakonskih propisa koji se odnose na mogućnost da kao dokaze u postupku treba prihvatiti i elektronske dokaze izvedene na magnetskim medijima, optičkim diskovima i drugim vrstama elektronskih memorija, kao i ostalim medijima iz kojih mogu da se, posredno i neposredno, izvedu elektronski dokazi.

Takođe, neophodno je primenjivati zakon o digitalnom potpisu. *Digitalni potpis* je skup podataka u elektronskom obliku, koji su dati ili logički pridruženi elektronskim porukama ili dokumentima i služe kao metod za identifikaciju potpisnika. Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja poruke (dokaz da poruka nije promenjena na putu od pošiljaoca do primaoca), kao i da obezbedi garantovanje (neporecivost) identiteta pošiljaoca poruke. Prvi standard digitalnog potpisa usvojen je 1991. godine i bazirao se na RSA asimetričnom algoritmu. Vlada SAD usvojila je Digital Signature Standard (DSS), koji se bazira na El Gamal šemi asimetričnog algoritma. Osnovu digitalnog potpisa čini sadržaj same poruke. Pošiljalac primenom kriptografskih algoritama prvo od svoje poruke koja je proizvoljne dužine stvara zapis fiksne dužine (npr. 512 ili 1024 bita) koji u potpunosti odslikava sadržaj poruke. To, u stvari, znači da svaka promena u sadržaju poruke dovodi do promene potpisa. Dakle, pošiljalac kreira digitalni potpis na osnovu poruke koju želi da pošalje. Šifruje ga svojim tajnim ključem i šalje zajedno sa porukom. Primalac po prijemu poruke dešifruje potpis pošiljaoca njegovim javnim ključem. Zatim kreira potpis na osnovu poruke koju je primio i upoređuje ga sa primljenim potpisom. Ako su potpisi identični, može biti siguran da je poruku zaista poslao pravi pošiljalac (jer je njegovim javnim ključem uspe-

šno dešifrovao potpis) i da je ona stigla nepromenjena (jer je utvrđeno da su potpisi identični). I pored velike sigurnosti koju pruža ovaj metod zaštite, i dalje postoji mogućnost prevare. Neko je mogao poslati svoj javni ključ tvrdeći da je od pravog pošiljaoca, a zatim slati poruke za koje bi primalac mogao da bude u zabludi da ih šalje pravi pošiljalac.

Ovaj problem rešava se upotrebom *digitalnih sertifikata*, koje možemo nazvati i digitalnom ličnom kartom. Digitalni sertifikat je uverenje kojim se potvrđuje veza između podataka za verifikaciju elektronskog potpisa i identiteta potpisnika, koji je izdat od strane akreditovanog sertifikacionog tela.

Važnost digitalnih potpisa i digitalnih sertifikata za dokazivanje u oblasti kompjuterskog kriminala je očigledna. U nedostatku običnog potpisa ili rukopisa, koji bi se mogli veštačiti, kao i nedostatka tragova koji se koriste kao dokazi za klasična krivična dela (otisci prstiju i dlanova, biološki tragovi, mikrotragovi, tragovi oruđa i alata itd.), ipak, treba rasvetliti krivično delo i otkriti izvršioca, između ostalog i tako što će se nesporno utvrditi ko je obavio određenu operaciju na kompjuteru koja zbog svoje posledice predstavlja radnju izvršenja krivičnog dela. Ako je sam pristup računaru ili mreži uslovljen identifikacijom korisnika putem digitalnog potpisa ili digitalnog sertifikata, moguće je suziti krug osumnjičenih na lica koja koriste ovakav potpis ili sertifikat ili koja su bila u prilici da ih zloupotrebe.

Elektronski dokazi zavise od načina izvršenja konkretnog krivičnog dela koje je direktno ili posredno povezano sa kompjuterom i kompjuterskim mrežama. Kao relevantni dokazi mogu da posluže sve vrste memorija na kojima se skladište elektronske informacije (hard diskovi, fleš memorije, optički kompakt diskovi i dr.), tekuće i neko prethodno (*back-up*) stanje podataka, svi elektronski dnevnici, štampani izveštaji izvedeni sa svih vrsta elektronskih memorija, izvorna (*Source*) i izvršna (*exe, com*) verzija programa, hardverska i telekomunikaciona oprema.

Zbog specifičnosti krivičnih dela kompjuterskog kriminala, svi dokazi moraju da budu prikupljeni i obezbeđeni tokom pretkrivičnog postupka i istrage, u kojoj će često biti potrebna i ekspertiza od strane stručnog lica – sudskog veštaka odgovarajuće struke. Zakon o uslovima za obavljanje poslova veštačenja[266] u članu 19 određuje posebne uslove koje treba da ispunjava lice koje može vršiti veštačenje kao stalni veštak. U oblasti informacionih tehnologija neophodna su specifična znanja i iskustva, a posebno je važno stalno praćenje novih tehnologija, kako bi se u uslovima stalnog razvoja i ekspanzije održao nivo znanja potreban da se uspešno obavi postavljeni zadatak. Posebno znanje i iskustvo u ovoj oblasti često poseduju lica koja nemaju visoko

[266] „Službeni glasnik RS“, br. 16/87, 17/87.

obrazovanje ni veliko životno iskustvo, ali su fanatični entuzijasti, koji prate sve inovacije i za koje takoreći nema tajni u oblasti visokih informacionih tehnologija.

Važeći Zakonik o krivičnom postupku donekle omogućava uspešno vođenje krivičnog postupka za izvršena dela kompjuterskog kriminala. Presudan značaj za vođenje krivičnog postupka ima pribavljanje i obezbeđenje dokaza. Ono se u pretkrivičnom postupku ostvaruje radnjom dokazivanja – privremenim oduzimanjem predmeta regulisano je čl. 82–86 ZKP-a (što konkretno znači oduzimanje hardvera, softvera ili drugih računarskih komponenata). Odredbe Zakonika o krivičnom postupku, koje su od posebnog značaja za borbu protiv kompjuterskog kriminala, sadržane su u članu 232 kojim se daje mogućnost da istražni sudija, na pismeni i obrazloženi predlog državnog tužioca, može da naredi nadzor i snimanje telefonskih i drugih razgovora ili komunikacija drugim tehničkim sredstvima lica za koja postoji osnovana sumnja da su sama ili sa drugim licima izvršila krivična dela sa elementima organizovanog kriminala (između ostalog, falsifikovanje i pranje novca). Mere mogu da traju najduže tri meseca, a zbog važnih razloga mogu da budu produžene za još tri meseca. Poštanska, telegrafska i druga preduzeća, društva i lica registrovana za prenošenje informacija dužna su da organima unutrašnjih poslova omoguće izvršenje navedenih mera. Ovakva ovlašćenja omogućavaju prikupljanje komunikacionih podataka u skladu sa odredbama Konvencije o kompjuterskom kriminalu.

Predlažemo da se dopune odredbe člana 225, stav 2 Zakonika o krivičnom postupku, koje se odnose na ovlašćenje organa unutrašnjih poslova, da u pretkrivičnom postupku preduzimaju potrebne mere i radnje, tj. potražne radnje. Ove odredbe treba dopuniti ovlašćenjem organa unutrašnjih poslova da mogu izvršiti pregled računarskih podataka na kompjuteru ili kompjuterskoj mreži, odnosno drugom uređaju ili predmetu koji sadrži takve podatke.

Prave probleme pribavljanja, obezbeđivanja i korišćenja elektronskih, odnosno dokaza u elektronskoj formi ili, kako ih neki nazivaju, digitalnih dokaza, definisaće praksa otkrivanja i gonjenja krivičnih dela za čije su dokazivanje potrebni takvi dokazi. Praktične probleme potom treba iz života preneti u zakonsku regulativu i nova zakonska rešenja efikasno primenjivati od strane dobro obučenih specijalista u ovoj oblasti.

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala,[267] koji je stupio na snagu 25. jula 2005. godine, predvideo je osnivanje posebnih organizacionih jedinica državnih organa radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela određena članom 3

[267] „Službeni glasnik RS“, br. 61/05.

Zakona. Za razliku od brzine usvajanja zakona, proces konstituisanja zakonom predviđenih organa trajao je skoro tri godine. Najveći problem u radu ovih organa uslovljen je neodgovarajućom zakonskom regulativom. Međutim, osposobljenost i broj angažovanih kadrova, kao i odgovarajuća tehnička opremljenost – uslov su bez kojeg i najbolju zakonsku regulativu nije moguće sprovesti.

Dinamika razvoja IT zahteva kontinuiranu, neprekidnu obuku svih učesnika u borbi protiv VT kriminala, a odgovarajuća tehnička opremljenost samo je preduslov primene tako stečenih znanja i veština.[268]

Iako je članom 12 Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala propisano, da „...ministarstvo nadležno za poslove pravosuđa obezbeđuje *odgovarajuće* prostorije i sve druge *tehničke uslove* potrebne za efikasan rad Posebnog tužilaštva i Veća“, nakon skoro četiri godine od stupanja ove odredbe na pravnu snagu, sa žaljenjem možemo da konstatujemo da Posebnom tužilaštvu još nisu obezbeđeni uslovi propisani navedenim članom.

Ukoliko bi se nemogućnost rešavanja navedenih problema, u sadašnjem trenutku, mogla opravdati aktuelnom ekonomskom situacijom, nerešavanje ovih problema u prethodnom periodu svakako je rezultat drugih faktora. Jedan od značajnijih jeste i odsustvo vizije razvoja društva, pa tako i pravne nauke, trenutno etablirane u pojedincima nespremnim na nove izazove. Njihovo nerazumevanje logike razvoja informacionih tehnologija i njenih „proizvoda“, tako razumljivih *teenage* generaciji, nosi sa sobom nerazumevanje i onih aspekata IT-a koji mogu ugroziti društvo i njegov pravni poredak.

Takvo nerazumevanje, s jedne strane, i potreba da se „dokažemo“ u procesu pridruživanja EU, s druge strane, ima za posledicu politički motivisano donošenje zakona, čije sprovođenje i obezbeđivanje instrumenata za njihovo sprovođenje, kao na našem primeru, može potrajati tri, i više godina.

Činjenica da se VT kriminal ne odvija na trgovima i ulicama otežava njegovo percipiranje, ali ga zbog toga ne čini i manje opasnim.

Naprotiv, uvereni smo da je reč o kriminalu *sui generis*, koji će svojom vitalnošću i sposobnošću mutacije vrlo brzo postati ozbiljan problem države, zadirući ne samo u njenu ekonomsku moć već i u samu bezbednost, o čemu nam govore iskustva drugih država koje su u informatičku eru kročile znatno pre nas.[269]

[268] Poslednja kontinuirana obuka iz oblasti VT kriminala sprovedena je u okviru projekta Saveta Evrope PACO–Srbija, koji je okončan sredinom 2008. godine.

[269] Npr. veliki sajber napad na Estoniju 2007. godine, koji je onesposobio sajtove vlade, političkih partija, medijskih kuća, banaka i kompanija, i tako napravio totalni kolaps u funkcionisanju države.

Da bismo imali spreman odgovor i na takav scenario – neophodno je unaprediti tehničke i druge uslove rada posebnih organizacionih jedinica državnih organa koje se bore protiv VT kriminala.

Kada je u pitanju unapređenje tehničkih mogućnosti državnih organa koji se bore protiv VT kriminala, svakako je najznačajnije unapređenje tehničkih mogućnosti policije, posebno njihovog specijalizovanog odeljenja.

Fiksiranje, prikupljanje, čuvanje i obrada digitalnih dokaza nalažu visoku tehničku opremljenost Posebnog odeljenja MUP-a, pri čemu potreba za hitnim i neodložnim veštačenjima nalaže potrebu posedovanja najsavremenijih hardverskih i softverskih alata kojima je moguće „ući u trag" izvršiocima ovih krivičnih dela, koji se neretko regrutuju iz reda veoma promućurnih ljudi, sa multidisciplinarnim znanjima iz IT-a, često stečenim na samom vebu.

Posebno tužilaštvo svakako nema takve potrebe, međutim, s obzirom na činjenicu da je u svakodnevnom poslu upućeno na često prisustvo u globalnoj računarskoj mreži, njena tehnička opremljenost mora da bude na nešto višem nivou u odnosu na ona tužilaštva koja se isključivo bave tzv. „opštim kriminalom".

Postojanje kontakt tačke u okviru „mreže 24/7",[270] predviđene Konvencijom o visokotehnološkom kriminalu,[271] nezamislivo je bez sigurnog onlajn pristupa svim vrstama telekomunikacionih mreža.

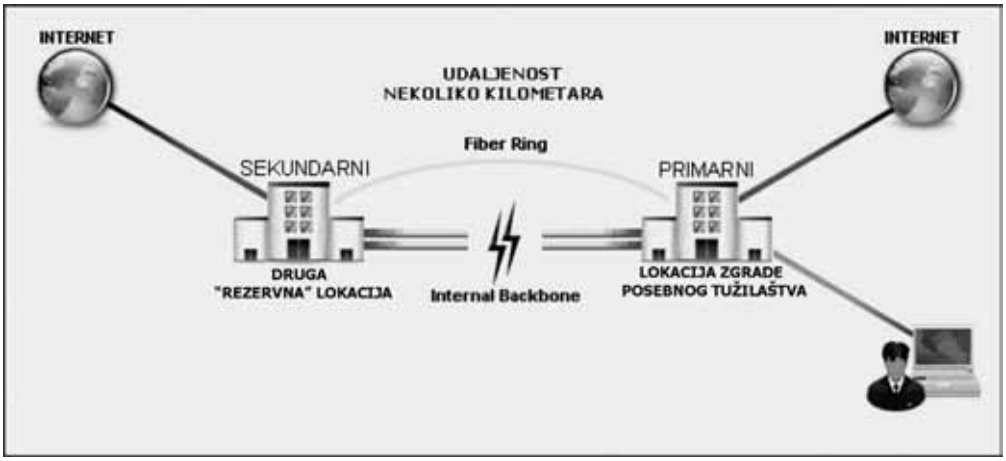
Sve to podrazumeva postojanje redundantnog računarskog sistema[272] implementiranog na heterogenim platformama (Windows/Linux), sa visokom propusnom moći mreže, koja bi celokupnim performansama obezbedila sigurnost i brzinu u obavljanju redovnih poslova Posebnog tužilaštva.

Zamišljeni redundantni računarski sistem, koji bi u velikoj meri garantovao nesmetano funkcionisanje mreže Posebnog tužilaštva, izgledao bi kao na *slici 14*.

[270] „ Da bi rad mreže bio olakšan, svaka strana ugovornica treba da obezbedi obučeno i opremljeno osoblje" – član 35 Konvencije.

[271] Svaka strana ugovornica treba da odredi mesto za kontakt, koje je dostupno 24 sata, sedam dana u nedelji, da bi omogućila pružanje trenutne pomoći istragama ili postupcima u vezi sa krivičnim delima koja se odnose na računarske sisteme i podatke, ili radi prikupljanja dokaza u elektronskom obliku o krivičnom delu (član 35 Konvencije).

[272] Redundantan sistem – u kojem za sve segmente sistema postoje alternativni, koji se u slučaju otkazivanja primarnog automatski aktivira, omogućujući tako neprekidan rad.



Slika 14

U ovom trenutku, tehničke mogućnosti Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala nisu na zadovoljavajućem nivou.

Rad se i dalje odvija u okviru postojećeg prostora Okružnog javnog tužilaštva, na VI spratu Palate pravde, u ul. Savskoj 17a u Beogradu, uz korišćenje zajedničkih tehničkih resursa koji svojim osobinama ne odgovaraju potrebama Posebnog tužilaštva.

Korišćenje zajedničkih tehničkih resursa podrazumeva *nepostojanje samostalne računarske mreže* Posebnog tužilaštva koja bi, po našem viđenju, trebalo da se sastoji od *pet* servera:

– WIN 2003/Linux server na kojem bi se nalazili AD – aktivni direktorijumi sa DHCP, DNS i drugim uobičajenim servisima,

– SQL server sa odgovarajućom bazom podataka,

– File server, na kojem bi se nalazili podaci svakog korisnika ponaosob, kao i deljeni podaci,

– Firewall – koji može biti ISA server, ili neko drugo hardversko rešenje (CISCO PIX...),

– Exchange server – za elektronsku poštu.

Svaki od ovih redundantnih servera trebalo bi da ima zaseban UPS, kao alternativno i nezavisno napajanje.

Tehničke mogućnosti Posebnog tužilaštva svakako bi bile unapređene i posedovanjem dovoljne količine odgovarajućeg softvera neophodnog za vršenje svakodnevnog posla, što podrazumeva i posedovanje softvera[273] koji bi

[273] Posebno tužilaštvo ne raspolaže programima kao što su Nero, Corel, Adobe Photoshop i sl.

omogućio postupajućim zamenicima razgledanje digitalnih dokaza i rezultata obavljenih veštačenja.

S obzirom na dinamiku razvoja IT-a, u pogledu vrste softvera neophodnog za rad nije moguće definisati godišnje potrebe tužilaštva, što, imajući u vidu njegovu cenu, nameće potrebu rezervisanja novčanih sredstava u budžetu iz kojeg se tužilaštvo finansira.

Budući da suzbijanje VT kriminala podrazumeva i preventivnu stranu delovanja, smatramo da je od posebnog značaja izrada kvalitetne veb prezentacije[274] tužilaštva, koja bi svojim sadržajima edukovala njene posetioce ne samo u pogledu potencijalnih opasnosti koje ih vrebaju na mreži već i u pogledu mera koje mogu preduzeti u cilju sigurnosti i zaštite sopstvenog integriteta. Takođe, iznoseći primere iz tužilačke i sudske prakse, uvereni smo da bi takvi sadržaji mogli da odvrate izvestan broj lica od izvršenja krivičnih dela, koja su planirali ili nameravali da izvrše.

Najzad, interaktivnost veb prezentacije omogućila bi ne samo uslugu pružanja konkretnih saveta ili pomoći već i mogućnost podnošenja krivičnih prijava[275] – što je od posebnog značaja za pravovremeno reagovanje, od čije brzine često zavisi da li će se pribaviti validan digitalni dokaz, i to u onom stanju kakvo je bilo u trenutku izvršenja dela. Zakonik o krivičnom postupku, čija je primena odložena do 31. decembra 2010. godine, predviđa takvu mogućnost.[276] Podnošenje prijave obavljalo bi se kroz proceduru *step by step*[277] tokom koje bi podnosilac u ponuđenom obrascu unosio onlajn, na predviđenim mestima, potrebne identifikacione i druge podatke na osnovu čije validnosti bi ih sistem prihvatao ili odbacivao, onemogućavajući na taj način „lažno prijavljivanje" i zagušenje servera nepotrebnom poštom (*slika 15*).

[274] *www.beograd.vtk.jt.rs*

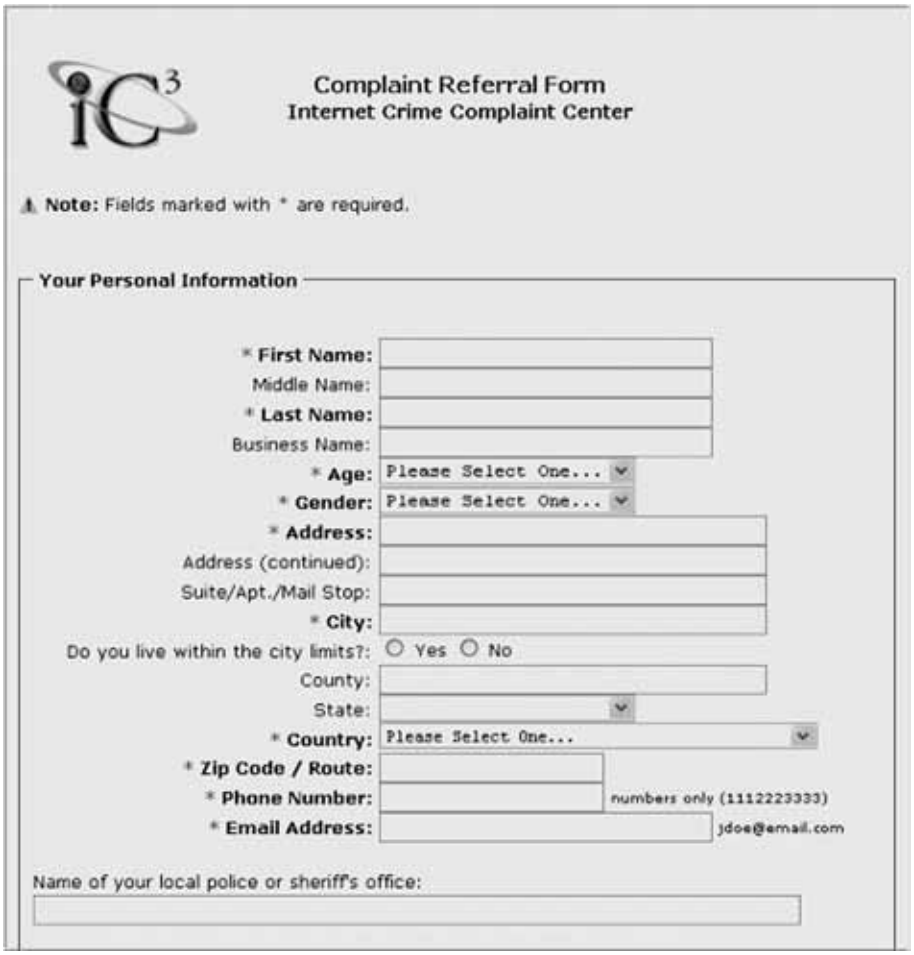
[275] Po uzoru na The Internet Crime Complaint Center (IC3) – www.ic3.gov

[276] Član 254 ZKP.

(1) Krivična prijava se podnosi nadležnom javnom tužiocu, pismeno ili usmeno, telefonom, elektronskom poštom ili upotrebom drugih tehničkih sredstava i načina.

(2) Ako se krivična prijava podnosi usmeno, prijavilac će se upozoriti na posledice lažnog prijavljivanja, a prijava i upozorenje se unose u zapisnik. Ako je prijava saopštena telefonom ili upotrebom drugih tehničkih sredstava i načina, sačiniće se službena beleška, a ako je prijava podnesena elektronskom poštom, ona će se sačuvati na odgovarajućem nosiocu podataka i odštampati.

[277] „Korak po korak".



Slika 15

Omogućavanje navedenih usluga putem veb prezentacije mora da bude maksimalno pojednostavljeno i razumljivo u čemu državnim organima, pa tako i Posebnom tužilaštvu za borbu protiv VT kriminala, neprocenjivu pomoć može da pruži Republički zavod za informatiku i internet[278] svojim *Preporukama za izradu Web prezentacija organa državne uprave*, koje predstavljaju odgovor na brze promene u oblasti tehnologija, prioritete u oblasti elektronske uprave, kao i strateške dokumente koji su prihvaćeni od strane Vlade RS, kao što su „eSEE Agenda + Za razvoj informacionog društva u jugoistočnoj Evropi 2007–2012“, potpisana u oktobru 2007. godine, „Konvencija UN o pravima osoba sa invaliditetom“ i „Opcioni protokol na

[278] *www.rzii.sr.gov.yu*

međunarodnu konvenciju o pravima osoba sa invaliditetom“, potpisani 17. decembra 2007. godine.

I da zaključimo.

S obzirom na toliko puta pominjani karakter visokotehnološkog kriminala koji ne priznaje nacionalne boje i obeležja, nameće se logičan zaključak da su tehnička sredstva neophodna za njegovo otkrivanje i suzbijanje jedinstvena, ta stoga i univerzalna, za sve države i pravne sisteme.

Da li će i u kom obimu takva tehnička sredstva biti i upotrebljena, u velikoj meri zavisi od ekonomske moći države, te je u tom smislu izlišno davati poređenja i uporedne analize u odnosu na tehničku opremljenost tužilaštava iz regiona, pa i šire.

Ono što je nesumnjivo jeste činjenica da je reč o znatnim finansijskim izdacima koje mnoge države iz svojih skromnih budžeta nisu u stanju da izdvoje, u čemu s pravom očekuju pomoć ekonomski razvijenijih – koje bi u suzbijanju takve globalne pojave kao što je visokotehnološki kriminal morale da prepoznaju i sopstveni interes.

X

PRAKSA SPECIJALIZOVANIH ORGANA ZA SUZBIJANJE VISOKOTEHNOLOŠKOG KRIMINALA U SRBIJI

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 s radom u aprilu 2008. godine. Početak njihovog rada obeležen je prvo rešavanjem problema broja ljudi i nedostatkom službenih prostorija, kao i snabdevanjem kompjuterskom opremom. Bez obzira na sve ove probleme, uspeli su u kratkom periodu da 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 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, imamo podnete 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,[279] dok se pod proizvodima u elektronskom obliku posebno podrazumevaju računarski programi i autorska dela koja se mogu upotrebiti 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 predlog 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 krivična dela protiv intelektualne svojine (Glava XX Krivičnog zakonika), imovine (Glava XXI Krivičnog zakoni-

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

ka) 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 nadležnost 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 leži u nedostatku službenih prostorija, sa čime 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, te stoga 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 jer 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 oduzetih 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 koji 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 je 184, dok su krivične prijave podnete protiv 166 lica, što predstavlja značajan 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.[280] Razlog tome leži u činjenici da izvršilac ovih krivičnih dela može biti 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[281] i pedofilije na internetu, odnosno krivično delo prikazivanje pornografskog materijala i iskorišćavanje dece za pornografiju,[282] koja po svojoj prirodi i načinu izvršenja svakako spadaju u stvarnu nadležnost Posebnog 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 se prepliće sa nadležnošću tužilaštava opšte nadležnosti imajući u vidu da ukoliko je reč o količini ispod 500 koma-

[280] Član 199 Krivičnog zakonika Republike Srbije.
[281] Član 225 Krivičnog zakonika Republike Srbije.
[282] Član 185 Krivičnog zakonika Republike Srbije.

da 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.

Jedna od glavnih odlika rada Posebnog tužilaštva jeste uspostavljanje saradnje sa javnim tužilaštvima i područnim upravama Ministarstva unutrašnjih poslova na teritoriji cele Republike Srbije. Naime, krivična dela visokotehnološkog kriminala predstavljaju novi oblik kriminaliteta, a prikupljanje i obezbeđenje dokaza koji mogu da služe u sudskom postupku umnogome se razlikuju od prikupljanja klasičnih dokaza. Pored postupanja u predmetima iz svoje nadležnosti, velika pažnja je posvećena i ujednačavanju prakse u postupanju svih javnih tužilaštava na teritoriji Republike Srbije. Osnovne smernice za postupanje u krivičnim delima visokotehnološkog kriminala dostavljene su javnim tužilaštvima na teritoriji Srbije, a naročito je podstaknut neposredni kontakt sa posebnim tužiocem i njegovim zamenicima kako bi se već na početku razjasnila sva pitanja i dileme u vezi sa izvršenjem krivičnih dela visokotehnološkog kriminala i prikupljanjem dokaza. Takođe, uspostavljena je saradnja i sa područnim upravama Ministarstva unutrašnjih poslova, kojima su dostavljeni telefoni za kontakt sa posebnim tužiocem i njegovim zamenicima, kao i uputstvo za sačinjavanje potvrde o privremeno oduzetim predmetima u elektronskom obliku, te na taj način posebni tužilac efikasnije vrši kontrolu rada u pretkrivičnom postupku. Imajući u vidu da krivična dela visokotehnološkog kriminala neretko imaju i međunarodni karakter, ostvarena je i efikasna saradnja sa Kancelarijom Interpola u Republici Srbiji tako što Posebno tužilaštvo redovno prima obaveštenja i podatke koji se odnose na visokotehnološki kriminal koji je izvršen ili za koji postoji sumnja da će biti izvršen na teritoriji Republike Srbije. Pored navedenog, Posebno tužilaštvo za visokotehnološki kriminal je u 2008. godini zaključilo Sporazum o saradnji u oblasti visokotehnološkog kriminala sa Nacionalnom žandarmerijom Republike Francuske.

Imajući u vidu prirodu dokaza koji se pojavljuju u vezi sa izvršenjem krivičnih dela visokotehnološkog kriminala i mogućnost njihovog relativno lakog uklanjanja ili uništavanja u postupku njihovog pribavljanja, tužilaštvo, kao rukovodilac pretkrivičnog postupka, ustanovilo je postupak preliminarnog planiranja i saradnje sa Odeljenjem za visokotehnološki kriminal i Službom za specijalne istražne metode i u njenom okviru Odeljenjem za obradu

elektronskih dokaza Ministarstva unutrašnjih poslova u sprovođenju svake konkretne radnje.

U radu Posebnog tužilaštva velika pažnja je posvećena stručnom usavršavanju, prisustvu na stručnim seminarima i drugim vidovima obuke koji su značajni za uspešnu borbu protiv visokotehnološkog kriminala. Veliki broj seminara i skupova na ovu temu uzrokovan je i sve većim interesom javnosti, kao i podizanjem svesti o značaju suzbijanja ove vrste kriminaliteta i formiranja koncepta visokotehnološke bezbednosti kroz aktivno učešće svih društvenih subjekata i uspostavljanjem čvršće saradnje sa organima otkrivanja i gonjenja kako na domaćem, tako i na međunarodnom planu. U navedenom smislu u toku 2008. godine postavljena je i internet prezentacija tužilaštva na adresi *www.beograd.vtk.jt.rs* čiji je cilj, između ostalog, i da se omogući javnosti da se bolje upozna sa radom tužilaštva i ostvarenim rezultatima.

3. DOSADAŠNJA SUDSKA PRAKSA

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.[283] U pogledu ostalih krivičnih dela iz oblasti visokotehnološkog kriminala koja su predmet sudskog postupka, najzastupljeniji oblici su prevara iz člana 208 KZ,[284] u kojoj se kao sredstvo izvršenja krivičnog dela pojavljuje računar, računarska prevara iz člana 301 KZ, računarska sabotaža iz člana 299 KZ i neovlašćeni 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 uličnе 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 torrent-a ili *rapdishare* mreže ili kupovinom legalnih kopija u za to ovlašćenim prodavnicama. Ovako neovlašćeno umnoženi primerci autorskih dela se naručiocima dostavljaju korišćenjem usluga JP PTT Srbije – plaćanje pouzećem, odnosno podizanje novca nakon

[283] „Službeni glasnik RS“, br. 85/05, 88/05, 107/05.
[284] Krivični zakonik.

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 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, i to 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.

Kao karakteristični primeri iz sudske prakse mogu se navesti:

Produženo krivično delo – Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199, stav 3 u vezi sa st. 1 i 2 Krivičnog zakonika u vezi sa članom 61. Krivičnog zakonika

Po optužnici Posebnog tužilaštva za visokotehnološki kriminal, presudom Okružnog suda u Beogradu od 10. 7. 2008. god., uz prethodno opozivanje uslovnih osuda, zbog tzv. „ulične piraterije“, osuđen je na jedinstvenu kaznu zatvora u trajanju od 11 (jedanaest) meseci M. J. (24) iz Beograda što je, u deset navrata, u periodu od 29. 6. 2006. godine do 14. 5. 2008. godine, u Beogradu, na istovetnim lokacijama u ulicama Bulevar kralja Aleksandra i Ustaničkoj, u nameri da za sebe pribavi protivpravnu imovinsku korist, na improvizovanim tezgama – u vidu ulične prodaje stavljao u promet neovlašćeno umnožene primerke autorskih dela u vidu CD-ova i DVD-ova koje je prethodno nabavljao od N. N. lica ispred ulaza u OTC „Novi Beograd“ u Novom

Beogradu, da bi ih zatim na navedenim mestima prodavao – prisvajajući za sebe gotov novac u vidu ostvarene razlike između njihove prodajne i nabavne cene, što je činio sve do intervencija ovlašćenih službenih lica policijskih stanica Zvezdara i Stari grad – koja su od njega tokom navedenog perioda, uz potvrdu, privremeno oduzela ukupno 4.949 (četiri hiljade devet stotina četrdeset devet) optičkih diskova sa nasnimljenim filmovima i računarskim igrama različitih nosilaca autorskih prava, kao i sa nasnimljenim muzičkim sadržajima u audio i MP3 formatu, većeg broja autora koji svoja autorska prava na teritoriji Republike Srbije kolektivno ostvaruju preko organizacije SOKOJ.

Krivično delo Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava u produženom trajanju iz člana 199, stav 3 u vezi sa st. 1 i 2 KZ u vezi sa članom 61 KZ

Po optužnici Posebnog tužilaštva za visokotehnološki kriminal, Okružni sud u Beogradu je na javnom ročištu oglasio krivim G. M. iz Beograda, izrekavši mu uslovnu osudu tako što mu je utvrdio kaznu zatvora u trajanju od šest meseci i istovremeno utvrdio da se ista neće izvršiti ukoliko okrivljeni u vremenu proveravanja od dve godine ne učini novo krivično delo, što je u periodu od decembra 2006. do 19. 5. 2008. godine, u svom stanu u Beogradu, u uračunljivom stanju svestan svog dela i njegove zabranjenosti čije je izvršenje hteo, u nameri pribavljanja imovinske koristi za sebe, neovlašćeno umnožavao primerke autorskih dela, stavljao ih u promet i držao u svom stanu na adresi prebivališta u nameri stavljanja u promet, na način što je primerke pojedinačnih autorskih dela nabavljao preko interneta, korišćenjem mreže *peer to peer* i bit torrent-a, kao i iznajmljivanjem iz DVD klubova tzv. „master" kopija autorskih dela, koje je potom smeštao na hard disk svog računara i na optičke nosače slike i zvuka u vidu CD-ova i DVD-ova, nakon čega je oglašavao prodaju kopija ovako pribavljenih autorskih dela preko interneta putem svojih prezentacija na sledećim domenima: *www.mp3zabava.cjb.net, www.geocities.com/dvdtrezor/, www.dvdtrexor.da.ru* ostavljajući kao kontakt adresu svoje elektronske pošte *mp3zabava@yahoo.com* i *dvdtrezor@yahoo.com,* kao i na *www.nostalgija.com, www.serbiancafe.com, www3.ptt.rs, www.zaradanovca.co.yu,* gde je kao kontakt ostavljao adresu elektronske pošte *mp3zabava@yahoo.com,* a koje su služile za dogovor oko narudžbina, a oglašavao se i u elektronskim oglasima *www.emarket365.com, www.megaoglasi.com* i *www.ba.emarket365.com* pod određenim imenom sa pretplatničkim brojem 064 41xxxx, na kojim prezentacijama je u okviru svojih ponuda postavljao cenovnik i katalog

autorskih dela koja nudi na prodaju, koji je sadržavao ukupno 13.433 naslova pojedinačnih autorskih dela, te je nakon pristizanja narudžbine od strane zainteresovanih lica na navedene adrese elektronske pošte i pretplatnički broj mobilnog telefona, preko svog računara na prazne optičke nosače slike i zvuka snimao naručena autorska dela, ovako neovlašćeno umnožene kopije autorskih dela putem poštanskih uputnica JP PTT Srbija pouzećem dostavljao naručiocima u zemlji i inostranstvu po ceni od 60 do 4.000 dinara po komadu, na koji način je ostvario imovinsku korist u iznosu od 400.000,00 dinara, što je činio sve do 19. 5. 2008. godine, kada su ovlašćena službe lica prilikom pretresa stana na adresi prebivališta pronašla i, uz potvrdu o privremeno oduzetim predmetima, oduzela kataloge u elektronskom obliku autorskih dela koja je stavljao u promet i 699 optičkih nosača slike i zvuka sa nasnimljenim primercima autorskih dela, a koji su se odnosili na autorska dela filmskog, muzičkog sadržaja, računarskih programa i igrica, različitih nosilaca autorskih prava.

Krivično delo Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199, stav 3 u vezi sa st. 1 i 2 Krivičnog zakonika u vezi sa članom 33 KZ

Po optužnici Posebnog tužilaštva, presudom Okružnog suda u Beogradu od 10. 10. 2008. god., zbog internet piraterije, oglašeni su krivim Ž. J. (36) i S. M. (35) iz Kraljeva, pa im je sud izrekao uslovnu osudu tako što im je utvrdio kaznu zatvora u trajanju od šest meseci i istovremeno utvrdio da se ista neće izvršiti ukoliko okrivljeni u vremenu proveravanja od dve godine ne učine novo krivično delo, što su, u periodu od 21. 6. 2005. godine, pa sve do dana 3. 6. 2008. godine, kada su lišeni slobode, na teritoriji Opštine Kraljevo, po prethodnom dogovoru, u nameri da sebi pribave imovinsku korist, putem bežične internet mreže *(wireless*), za novčanu nadoknadu neovlašćeno stavljali u promet preko 500 (pet stotina) primeraka raznovrsnih autorskih dela, različitih nosilaca autorskih prava na taj način što su tokom 2005. godine pa nadalje, na osnovu zajedničkih finansijskih ulaganja, izgradili i pustili u eksploataciju Wireless – bežičnu internet mrežu koja je funkcionisala neregistrovano pod neformalnim nazivom „eXcalibur Wireless“ (*Ekskalibur Vajrles*), što su činili u okviru poslovnog prostora svog privrednog društva tokom kog perioda su u navedenom prostoru primali novčane uplate korisnika interneta i FTP servisa, kojima je nakon izvršenih uplata bilo omogućeno da na svoje kućne računare preuzimaju neovlašćeno umnožene primerke raznovrsnih autorskih dela – u vidu fonograma, videograma, računarskih programa i drugih multimedijalnih sadržaja koje su okrivljeni, radi stavljanja u promet, neov-

lašćeno držali pohranjene na hard diskovima File Transfer Protocol servera, tj. servera sa protokolom za razmenu fajlova, koji se fizički nalazio u kući prvookrivljenog na adresi njegovog prebivališta, na koji je prvookrivljeni prethodno putem satelitskog interneta – iz etra *preuzimao* navedene sadržaje kojima su krajnji korisnici pristupali sa svojih računara, uz unošenje pristupnog imena i korisničke šifre – preko MAC *(mak)* adrese i pristupne tačke na kojoj su registrovani u pristupnoj bazi korisnika (*na mestu gde se nalazi antena koja prima najjači signal njihove bežične mreže*), a potom *preuzimali* ponuđene sadržaje – neovlašćeno stavljene u promet primerke autorskih dela u vidu filmova, računarskih igrica, muzike i drugih multimedijalnih sadržaja.

Produženo krivično delo Prevara iz člana 208, stav 1 u vezi sa čl. 33 i 61 Krivičnog zakonika

Po optužnom predlogu Posebnog tužilaštva KT VTK.br.55/07, presudom Okružnog suda u Beogradu, zbog prevare počinjene putem interneta, oglašeni su krivim J. Š. (30) i njegova devojka T. D. (29) iz Novog Sada, tako što im je sud izrekao uslovnu osudu utvrdivši im kaznu zatvora u trajanju od šest meseci i istovremeno utvrdio da se ista neće izvršiti ukoliko okrivljeni u vremenu proveravanja od dve godine ne učine novo krivično delo, što su, od januara 2007. godine do 15. jula 2007. godine u Novom Sadu, u nameri da sebi pribave protivpravnu imovinsku korist, zajednički – lažnim prikazivanjem činjenica da su predstavnici Agencije „Exit apartments“ koja pruža usluge smeštaja posetiocima internacionalnog muzičkog festivala „Exit 07“, sa mestom održavanja u Novom Sadu, u trajanju od 12. do 16. jula 2007.godine, koristeći računar, računarske mreže i računarske podatke, kao i njihove proizvode u materijalnom i elektronskom obliku, doveli u zabludu više britanskih državljana, ukupno njih 29 (dvadeset devet) i time ih naveli da im na štetu svoje imovine, a na ime plaćanja ugovorenih usluga smeštaja, uplate na naznačeni račun „Erste bank“ ukupno 3.937 evra, odnosno, u dinarskoj protivvrednosti 314.960,00 dinara, što su učinili na taj način što je okr. J. Š. prethodno, u Novom Sadu, zaključio sa „Erste bankom“ Ugovor o otvaranju deviznog tekućeg računa, kod internet servis provajdera „Neobee.net“ podneo Zahtev za registraciju internacionalnog poddomena www.exitapartments.com na kojem je potom njegov poznanik, koristeći usluge veb hostinga internet provajdera „Eunet“, izradio i postavio internet stranicu izrađenu po detaljnim uputstvima prvookrivljenog, a na kojoj su okrivljeni, njenim posetiocima, na engleskom jeziku, nudili usluge dnevnog smeštaja po ceni od 30 do 60 evra, u jednosobnim i trosobnim apartmanima hotela „Gymnas“ u Novom Sadu, sa kojim okrivljeni nikada

nisu imali poslovni odnos i saradnju te koje su usluge, prema datim uputstvima na internet stranici www.exitapartments.com, posetioci sajta mogli ne samo da rezervišu već avansno i da plate – polažući depozit u visini od 30 odsto od cene aranžmana na navedeni račun „Erste banke“, što su činili tzv. S.W.I.F.T.-om, kao jednim od najbržih načina obavljanja međunarodnih plaćanja, pri čemu su ošt. britanski i irski državljani, pre obavljenih plaćanja, odnosno pre polaganja depozita i dolaska na festival „Exit 07“ obavljali komunikaciju sa drugookrivljenom pozivanjem njenog broja mobilnog telefona +381964/668... objavljenog na stranici i putem naznačenih elektronskih adresa *info@exitapartments.com* i *exitapartments@neobee.net*, koja im se u tim prilikama lažno predstavljala kao menadžer za odnose sa javnošću agencije „Exit apartments“ iz Novog Sada, odgovarajući im na pitanja u vezi sa plaćanjem, kvalitetom apartmana, položajem apartmana u odnosu na mesto održavanja Festivala i sl., da bi im nakon izvršenih uplata saopštavala mesto susreta u Novom Sadu odakle bi trebalo da budu prevezeni do svojih apartmana – gde bi usledilo plaćanje do punog iznosa cene pruženog smeštaja, pa su tako, i pored postignutih dogovora, izbegavali bilo kakve kontakte sa oštećenima nakon njihovog dolaska u Novi Sad, zadržavajući na opisan način pribavljenu imovinsku korist u ukupnom iznosu od 3.937 evra, odnosno u dinarskoj protivvrednosti 314.960,00 dinara, s tim što su od nekoliko ošt. britanskih državljana, osim uplaćenog depozita, dobili u Novom Sadu i gotov novac u iznosu od 710 evra na taj način što su se po prethodnom dogovoru, dana 10. 7. 2007. godine u kafiću „Oliva“ u Bulevaru oslobođenja br. 133 u Novom Sadu, susreli sa ošt. britanskim državljanima, na kom mestu drugookrivljenoj, na ime navodne doplate za smeštaj, predaju gotov novac u navedenom iznosu, a ona njima pečatom overeni Ugovor i posetnicu sa natpisom „Agency for rent apartments“, da bi ih nakon toga, po instrukcijama okrivljenih, taksi vozilo prevezlo do hotela „Putnik“ u Novom Sadu gde bi shvatili da su prevareni.

Produženo krivično delo Računarska prevara iz člana 301, stav 3 u vezi sa stavom 1 KZ u vezi sa članom 61 KZ

Po zahtevu za sprovođenje istrage Posebnog tužilaštva za visokotehnološki kriminal, Okružni sud u Beogradu je doneo rešenje o sprovođenju istrage protiv B. V. što je u periodu od 31. 12. 2003. do 20. 11. 2007. godine, kao zaposleni u „Telekomu Srbija“, na radnom mestu tehničar za komutacione sisteme, u nameri da sebi i drugima pribavi protivpravnu imovinsku korist, lažno prikazivao podatke koji se odnose na tarifiranje telefonskog saobraćaja, odnosno utrošene telefonske impulse za određene telefonske priključke, čime

je uticao na rezultat elektronske obrade podataka o utrošenim telefonskim impulsima i naplatu ostvarenog telefonskog saobraćaja za ove priključke, na način što je preko računara-terminala koji je povezan sa centralom, preko koga se vrše sve aktivnosti vezane za rad centrale, koristeći zajedničko administratorsko korisničko ime „ROOT“ i lozinku „123456“, pristupao predmetnoj DKTS centrali, ulazio u meni „baza korisnici“ i u njemu za ukupno 18 telefonskih priključaka, od kojih su za 9 telefonskih priključaka korisnici fizička lica, a 6 telefonskih priključaka su službene linije „Telekoma Srbija“ na centrali neovlašćeno dodeljivao kategoriju „netarifiranje razgovora – poziva“ skidanjem čekiranja sa opcije „tarifira se kao pozivni“, dok je za 3 telefonska priključka čiji je on korisnik dodeljivao, pored kategorije „netarifiranje razgovora“ na navedeni način, i uslugu „konferencijske veze“, koje je na svim telefonskim priključcima u toku navedenog perioda nakon dodeljivanja povremeno skidao pa potom ponovo dodeljivao, te je postupajući po radnim nalozima Direkcije „Telekoma“ iz Beograda za proveru svih navedenih priključaka, tj. kontrolu stanja brojača, koji su dostavljani u centralu, bez provere, iako je znao da se radi o telefonskim priključcima kojima je dodelio opisane kategorije, vršio grupno čekiranje da je kontrola izvršena i da telefonski priključci ispravno funkcionišu, na koji način je svim opisanim radnjama pribavio sebi i drugima protivpravnu imovinsku korist u ukupnom iznosu od 10.680.770,52 dinara, koji iznos predstavlja štetu pričinjenu „Telekomu Srbija“, i to za sledeće telefonske priključke:

1. telefonske brojeve 014 41xxxx, 014 41xxxx, 014 41xxxx, čiji je on korisnik, na kojima je u navedenom periodu ostvaren i netarifiran telefonski saobraćaj u ukupnom iznosu od 2.673637,20 dinara, i to pojedinačno, na telefonskom broju 014 41xxxx u iznosu od 438.263,28 dinara, na telefonskom broju 014 41xxxx u iznosu od 2.134.168,20 dinara, na telefonskom broju 014 41xxxx u iznosu od 101.205,72 dinara;

2. telefonski broj 014 41xxxx, čiji je korisnik K. L., na kome je u navedenom periodu ostvaren i netarifiran telefonski saobraćaj u iznosu od 532.176,36 dinara;

3. telefonski broj 014 41xxxx, čiji je korisnik A. B., na kome je u navedenom periodu ostvaren i netarifiran telefonski saobraćaj u iznosu od 126.798,84 dinara;

4. telefonski broj 014 41xxxx, čiji je korisnik S. S., na kome je u navedenom periodu ostvaren i netarifiran telefonski saobraćaj u iznosu od 177.719,79 dinara;

5. telefonski broj 014 41xxxx, čiji je korisnik A. A., na kome je u navedenom periodu ostvaren i netarifiran telefonski saobraćaj u iznosu od 204.109,59 dinara;

6. telefonski broj 014 41xxxx, čiji je korisnik M. M., na kome je u navedenom periodu ostvaren i netarifiran telefonski saobraćaj u iznosu od 99.051,84 dinara;

7. telefonski broj 014 41xxxx, čiji je korisnik S. Č., na kome je u navedenom periodu ostvaren i netarifiran telefonski saobraćaj u iznosu od 378.544,68 dinara;

8. telefonski broj 014 41xxxx, čiji je korisnik M. N., na kome je u navedenom periodu ostvaren i netarifiran telefonski saobraćaj u iznosu od 134.499,60 dinara;

9. telefonski broj 014 41xxxx, čiji je korisnik O. O., na kome je u navedenom periodu ostvaren i netarifiran telefonski saobraćaj u iznosu od 46.498,32 dinara;

10. telefonski broj 014 41xxxx, čiji je korisnik J. J., na kome je u navedenom periodu ostvaren i netarifiran telefonski saobraćaj u iznosu od 374.028,48 dinara;

11. telefonske brojeve 014 41xxxx, 014 41xxxx, 014 41xxxx, 014 41xxxx i 014 141xxxx, koji su službene linije „Telekoma Srbija“, na kojima je u navedenom periodu ostvaren i netarifiran telefonski saobraćaj u ukupnom iznosu od 3.142.074,96 dinara, i to pojedinačno, na telefonskom broju 014 41xxxx u iznosu od 2.784.048,12 dinara, telefonskom broju 014 41xxxx u iznosu od 103.750,92 dinara, na telefonskom broju 014 41xxxx u iznosu od 77.105,52 dinara, na telefonskom broju 014 41xxxx u iznosu od 177.170,40 dinara, dok na telefonskom broju 014 41xxxx nije bilo telefonskog saobraćaja, a za telefonski broj 014 41xxxx formirao je telefonski liniju u centrali koja nije evidentirana u TIS-u centrale i telefonskom saobraćaju „Telekoma Srbija“ na kome je ostvaren i netarifiran telefonski saobraćaj u iznosu od 2.761.630,92 dinara.

U pogledu krivičnih sankcija koje se izriču učiniocima krivičnih dela visokotehnološkog kriminala, može se reći da su najzastupljenije uslovne osude. Razlog tome leži u činjenici što je zaprećenost kaznom za krivična dela visokotehnološkog kriminala u Krivičnom zakoniku Republike Srbije i inače mala. Tako, od svih krivičnih dela iz korpusa krivičnih dela visokotehnološkog kriminala samo za krivična dela neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199, stav 3 KZ, dakle ako je učinjeno u nameri pribavljanja protivpravne imovinske koristi, računarske sabotaže iz člana 299 KZ i računarske prevare iz člana 301, st. 2 i 3 KZ, ukoliko pribavljena imovinska korist prelazi iznos od 450.000,00, odnosno 1.500.000,00 dinara, zaprećenost kaznom je preko tri godine zatvora, dok je za sva ostala krivična dela ispod ove granice. U zavisnosti od opštih pravila o odmeravanju kazne u smislu člana 54 KZ i mogućnosti za ublažavanje kazne ispod granice

propisane zakonom sud – u zavisnosti od načina izvršenja krivičnog dela, vremena izvršenja, broja autorskih dela, držanja učinioca posle izvršenog krivičnog dela, pobuda iz kojih je krivično delo izvršeno, pribavljene imovinske koristi ili pričinjene štete i drugih zakonom određenih olakšavajućih i otežavajućih okolnosti – izriče krivične sankcije kojim bi se, po oceni suda, najbolje ostvarila svrha kažnjavanja. Kao što je rečeno, učiniocima krivičnih dela visokotehnološkog kriminala izriču se uslovne osude kojima se utvrđuje kazna zatvora u trajanju od nekoliko meseci, obično šest, do dve godine i istovremeno određuje da se neće izvršiti ukoliko učinilac u vremenu proveravanja, koje se određuje u odnosu na utvrđenu kaznu zatvora, u roku od jedne do pet godina ne učini novo krivično delo. Ovakve krivične sankcije se izriču licima koja se prvi put pojavljuju kao učinioci krivičnog dela i kada stepen ugrožavanja zakonom zaštićenih dobara po oceni suda nije velik, dok se u slučaju povrata ili višestrukog povrata ili težih krivičnih dela izriču kazne zatvora. Tako su u sudskoj praksi posebnog veća za borbu protiv visokotehnološkog kriminala u dva krivična predmeta izrečene efektivne kazne zatvora u trajanju od osam i jedanaest meseci, zbog krivičnog dela neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199, stav 3 u vezi sa st. 1 i 2. U svakoj osuđujućoj presudi, sud izriče mere bezbednosti oduzimanje predmeta iz člana 87 KZ i oduzimanje imovinske koristi iz čl. 91 i 92 KZ, dok se oštećeni, po pravilu, u pogledu svog imovinskopravnog zahteva upućuju na parnicu.

Ono što se pojavljuje kao specifičnost u sudskoj praksi u vezi sa izvršenjem krivičnih dela visokotehnološkog kriminala jeste, pored redovnog sudskog postupka, i primena postupka za kažnjavanje i izricanje uslovne osude od strane istražnog sudije. Odredbama čl. 455 do 458 Zakonika o krivičnom postupku[285] propisano je da, u slučaju potpunog priznanja okrivljenog, odnosno osumnjičenog, datog u prisustvu branioca istražnom sudiji, odnosno organu unutrašnjih poslova u smislu člana 226, stav 9 ovog zakonika, potkrepljenog i drugim dokazima prikupljenim u istrazi, javni tužilac može odmah nakon završene istrage, a najkasnije u roku od osam dana, u podignutoj optužnici predložiti da se, umesto glavnog pretresa, zakaže posebno javno ročište pred istražnim sudijom, na kome se, nakon saslušanja stranaka i uz izričiti pristanak okrivljenog, može doneti presuda. Ovakav postupak može da se primeni kod krivičnih dela za koja je propisana novčana kazna kao glavna kazna ili kazna zatvora do pet godina. Pod ovim uslovima istražni sudija može izreći novčanu kaznu, uslovnu osudu i kaznu zatvora do jedne godine, a uz njih jednu ili više sledećih mera: oduzimanje predmeta, zabranu upravljanja

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

motornim vozilom i oduzimanje imovinske koristi. Ono što je takođe specifično u vezi sa ovim postupkom jeste da troškovi postupka padaju na teret budžetskih sredstava suda. Razlog za primenu ovakvog postupka leži u njegovoj brzini i celishodnosti i samim tim efikasnijem ostvarivanju mera specijalne i generalne prevencije krivičnopravne zaštite. Naime, ono što je identifikovano kao problem u redovnom sudskom postupku u vezi sa izvršenjem ovih krivičnih dela, najčešće krivičnog dela neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199 KZ, u kome se dakle, po zahtevu ovlašćenog tužilaštva sprovodi istraga u kojoj se od strane istražnog sudije izvode svi potrebni dokazi – saslušanje okrivljenog, svedoka, oštećenih, sprovode potrebna veštačenja i sl, a zatim ponovo isti dokazi izvode i na glavnom pretresu koji se okončava presudom, jeste da traje suviše dugo, čime se ne ostvaruje potreban efekat krivičnopravne zaštite. Ovakav sudski postupak traje po dve ili tri godine i odaje utisak sporosti i nemoći države da se izbori sa izvršenjem ove vrste krivičnih dela, u kom periodu učinilac protiv koga se vodi postupak nastavlja sa izvršenjem krivičnih dela. S druge strane, primenom postupka izricanja krivične sankcije od strane istražnog sudije krivični postupak se od momenta podnošenja krivične prijave do izricanja presude na javnom ročištu, koja u većini slučajeva postaje pravnosnažna danom izricanja s obzirom na to da se stranke odriču prava na žalbu, završava za jedan do dva meseca. Na ovaj način postiže se brzina i efikasnost krivičnog postupka koji rezultira pravnosnažnom osuđujućom presudom vrlo brzo nakon izvršenja konkretnog krivičnog dela, čime se u punoj meri ostvaruje zaštitna funkcija krivičnog prava. Na ovaj način se znatno smanjuju i troškovi krivičnog postupka s obzirom na to da, iako troškovi padaju na teret budžetskih sredstava suda, oni su daleko manji nego u redovnom sudskom postupku jer obuhvataju samo troškove branioca, ukoliko je on postavljen po službenoj dužnosti, i to u vezi sa jednim saslušanjem okrivljenog pred istražnim sudijom i jednim javnim ročištem prilikom izricanja presude. U redovnom sudskom postupku troškovi obuhvataju troškove saslušanja svedoka i predstavnika oštećenih pred sudom, kako u istrazi, tako i na glavnom pretresu, troškove veštačenja, putne troškove službenih lica, troškove prevoza i dovođenja okrivljenog, sudski paušal i sl., koji, iako po pravilu padaju na teret okrivljenog koji je svojom radnjom i prouzrokovao krivični postupak, mogu pasti takođe na teret budžetskih sredstava suda, odnosno okrivljeni može da bude oslobođen plaćanja troškova krivičnog postupka u smislu člana 196, stav 4 ZKP[286] ukoliko bi njihovim plaćanjem bilo dovedeno u pitanje izdržavanje okrivljenog ili lica koje je dužan da izdržava.

[286] Zakonik o krivičnom postupku.

Iz svega iznetog može se zaključiti da sudska praksa Veća za borbu protiv visokotehnološkog kriminala Okružnog suda u Beogradu zavisi pre svega od ocene suda u pogledu opredeljivanja vrste krivičnih sankcija kojima bi se na najbolji način postigla svrha kažnjavanja, u čemu dominiraju uslovne osude, ali i zaprećenosti zakonom propisane kazne za krivična dela visokotehnološkog kriminala. Mala zaprećenost kaznama za krivična dela visokotehnološkog kriminala predstavlja izraz nerazumevanja opasnosti koje sa sobom nosi izvršenje ovih krivičnih dela, s obzirom na to da ugroženost zakonom zaštićenih dobara može da nastupi ne samo u ograničenom prostoru privatnog korišćenja već i u pogledu velikih sistema značajnih za celokupno društvo kao što su snabdevanje električnom energijom, vodosnabdevanje, nacionalni telekomunikacioni sistem i sl., koji se takođe oslanjaju na informacione tehnologije, u kom slučaju šteta može da bude nesagledliva. Takođe, način kako je formulisana stvarna nadležnost posebnih organa pomenutim članom 3 Zakona o organizaciji i nadležnosti državnih organa u borbi protiv visokotehnološkog kriminala, ne doprinosi ujednačavanju sudske prakse u ovoj oblasti krivičnog prava i navedena činjenica bi trebalo da bude što pre izmenjena, što je i predmet predloga izmena pomenutog zakona.

4. MEĐUNARODNA SARADNJA NA SUZBIJANJU VISOKOTEHNOLOŠKOG KRIMINALA

Ono što nesumnjivo proizlazi iz karakteristika ove vrste kriminala (bezgraničnost i transnacionalnost) jeste neophodnost međunarodnog povezivanja državnih organa u celom svetu koji se bave otkrivanjem i krivičnim progonom izvršilaca krivičnih dela visokotehnološkog kriminala.

U više navrata istican je značaj Konvencije o visokotehnološkom kriminalu Saveta Evrope, koja uspostavlja obavezu osnivanja kontakt tačke, 24/7, što znači da u svakoj od zemalja postoji tačka kojoj možete da se obratite i tražite dostavljanje određenih podataka, 24 sata u toku dana, sedam dana u nedelji.

Iako je Srbija ratifikovala Konvenciju tek u martu 2009. godine, to nije sprečavalo državne organe da intenzivno rade na unapređivanju međunarodne saradnje. Ovde pre svega mislimo na postupanje Posebnog tužilaštva za visokotehnološki kriminal.

Prvo na šta asocira pojam međunarodne pomoći jeste institut krivičnog procesnog prava a to je međunarodna pravna pomoć. Međutim, ovaj institut je spor i papirološki zahtevan tako da u većini slučajeva dovodi do odustanka od prikupljanja dokaza.

Stoga, potencira se neposredan kontakt između državnih agencija u cilju što brže razmene informacija. Osnovni cilj je fiksiranje dokaza, kako bi se pružila mogućnost, i ono što je najbitnije, vreme, kako bi se pokrenuo zvanični postupak međunarodne pravne pomoći.

Za dve godine aktivnog rada tužilaštvo je uspostavilo kontakt sa više međunarodnih subjekata u cilju što brže razmene informacija. Tužilaštvu na raspolaganju stoje i mehanizmi policijske razmene podataka, kao što su Interpol, Europol itd.

Jedan od najefikasnijih načina da se uspostavi kontakt sa predstavnicima drugih država jeste učestvovanje predstavnika tužilaštva na različitim konferencijama, kako u Srbiji, tako i u inostranstvu.

Beograd je u martu 2007. bio domaćin Regionalne konferencije o visokotehnološkom kriminalu, gde su prisustvovali predstavnici deset zemalja u okruženju.

Svake godine u Strazburu, pod pokroviteljstvom Saveta Evrope, održava se konferencija na kojoj se iz godine u godinu povećava broj učesnika iz različitih zemalja. Ove godine učestvovalo je 300 predstavnika državnih organa

iz 70 zemalja. Ovaj podatak je očigledan pokazatelj porasta svesti u velikom broju zemalja u cilju što efikasnije borbe protiv visokotehnološkog kriminala.

Iako broj potpisnika Konvencije nije veći od 45, postoji podatak da više od 100 država u svetu u okviru svojih zakona koristi rešenja implementirana u Konvenciji.

Na konferenciji posebna pažnja se posvećuje problemu kontakt tačke 24/7 i njenom funkcionisanju u različitim zemljama.

Učestvovanje na konferenciji je odlična prilika za razmenu i raspravljanje o problemima koji nastaju u toku krivičnog postupka.

Kad razmatramo pitanje međunarodne saradnje, ona može da se posmatra kroz odnos sa državnim institucijama stranih država ili kroz saradnju sa tzv. nevladinim sektorom, a tu pre svega mislimo na velike međunarodne kompanije kao što su Microsoft, Ebay, antivirusne kompanije...

Poslednjih nekoliko godina sve više se ističe značaj partnerstva između države i privrednih subjekata. Korist od uspešne saradnje ubiraju i država i privreda.

Tužilaštvo za visokotehnološki kriminal ostvarilo je saradnju i na nivou državnih organa, kao i na relaciji država–privreda.

U prvom delu istakli bismo odličnu saradnju sa predstavnicima ambasada SAD, Francuske i Velike Britanije u Beogradu.

Tužilaštvo ima ustanovljen partnerski odnos sa žandarmerijom Republike Francuske, koja je od januara 2009. godine u sastavu Francuskog ministarstva unutrašnjih poslova. Na tužilačkom nivou uspostavljena je saradnja sa Engleskim kraljevskim tužilaštvom.

Saradnja sa privredom odvija se preko Američke privredne komore, čija se kancelarija nalazi u Beogradu, kao i sa kancelarijom Microsoft-a.

Odlična saradnja uspostavljena je sa Savetom Evrope, kroz projekat PACO, čija je osnovna tema bila ekonomski kriminal, sa dve podgrupe pitanja: pranjem novca i visokotehnološkim kriminalom.

Imajući u vidu nameru Republike Srbije da Srbija postane deo EU, tužilaštvo je u kontaktima sa misijom OEBS u Republici Srbiji, kao i sa Evropskom komisijom.

Naravno, lista intenzivnih kontakata ne završava se samo pukim nabrajanjem institucija, već iskreno izraženom namerom da se saradnja u narednim godinama poboljša.

XI

PERSPEKTIVE RAZVOJA VISOKOTEHNOLOŠKOG KRIMINALA U SRBIJI

Prema podacima Internet svetske statistike (Internet World Stats), broj korisnika internet usluga u svetu 31. marta 2009. godine iznosio je *1.596.270.108* (*tabela 5*) od ukupne svetske populacije.[287] Penetracija internet korisnika u Republici Srbiji bez teritorije AP Kosovo i Metohija u odnosu na ukupno stanovništvo iznosi 32,4 odsto, odnosno *2.602.478* korisnika sa procentom rasta u odnosu na 2000. do 2009. godine od 550,6 odsto[288] (*tabela 6*). Na osnovu navedenih pokazatelja uočljivo je da je internet u Republici Srbiji postao jedan od najpopularnijih sistema masovne komunikacije.

REGIONI U SVETU	Broj stanovnika	Korisnici interneta na dan 31. 3. 2009.	. % populacije penetracija	Stopa porasta 2000-2009.
AFRIKA	975.330.899	**54.171.500**	5,6 %	1.100 %
AZIJA	3.780.819.792	**657.170.816**	17,4 %	474,9 %
EVROPA	803.903.540	**393.373.398**	48,9 %	274,3 %
SREDNJI ISTOK	196.767.614	**45.861.346**	23,3 %	1.296,2 %
SEVERNA AMERIKA	337.572.949	**251.290.489**	74,4 %	132,5 %
JUŽNA AMERIKA	581.249.892	**173.619.140**	29,9 %	860,9 %
AUSTRALIJA/OKEANIJA	34.384.384	**20.783.419**	60,4 %	172,7 %
UKUPNO	**6.710.029.070**	**1.596.270.108**	**23,8 %**	**342,2 %**

Tabela 5. Broj korisnika interneta u svetu

[287] *http://www.internetworldstats.com/stats.htm*
[288] *http://www.internetworldstats.com/stats4.htm#europe*

BIVŠA SFRJ	Broj stanovnika	Korisnici interneta na dan 31. 3. 2009.	. % populacije penetracija	Stopa porasta 2000-2009.
BOSNA I HERCEGOVINA	4.590.310	**1.441.000**	31,4 %	20.458,7 %..
CRNA GORA	678.177	**280,000**	41,3 %	n /a
HRVATSKA	4.491.543	**1.984.800**	44,2 %	892,4 %
MAKEDONIJA	2.061.315	**906.979**	44 %	2.923,3 %
SLOVENIJA	2.007.711	**1.300.000**	64,8 %	333,3 %
SRBIJA (bez KiM)	8.032.338	**2.602.478**	32,4 %	550,6 %
UKUPNO	**21.861.394**	**8.515.257**	**43,02 %**	5.031,66 %

Tabela 2. *Broj korisnika interneta u regionu (bivša SFRJ)*

Ovakav razvoj može društvu da pruži velike mogućnosti kao što su svi moderni procesi poslovanja poput elektronskog bankarstva (*online banking*), elektronske trgovine (*e-commerce*), internet telefoniranja (*Voice-over-Internet protocol* – VoIP), upravljanja energijom, saobraćajem, transportom, najsloženijim tehnološkim procesima itd.

Međutim, ovakav razvoj i prelazak društva iz industrijske u informacionu eru sa sobom nosi i veliku pretnju društvenom i ekonomskom životu, jer današnja moderna društva umnogome zavise od raspoloživosti informacionih tehnologija, naročito njene infrastrukture. Najvažniji primer je da je Rusija u sukobu protiv Gruzije u Južnoj Osetiji, pored konvencionalnog, vojnog, vodila paralelno i sajber rat. To je prvi put u istoriji čovečanstva da je jedna zemlja koristila modernu tehnologiju u ratovanju. Ruski hakeri su, naime, pre nego što je započeta vojna ofanziva, prvo srušili sve internet sajtove u Gruziji, onemogućivši joj komunikaciju sa svetom.

Prema analizama geopolitičkog Instituta „Stratfor“, ruska ofanziva protiv Gruzije nije počela tenkovima ili borbenim avionima, već u sajber prostoru. „Stratforovi“ stručnjaci saznali su da su sajtovi gruzijske vlade i medija bili srušeni u noći 7. avgusta 2008. godine, znači noć pre nego što su ruske trupe ušle u Južnu Osetiju.[289]

Takođe, kanadski istraživači otkrili su do sada najveću elektronsku špijunsku mrežu na svetu – „Mrežu duhova“ („Ghostnet“), sa sedištem u Kini. Izveštaj kanadske organizacije Monitor za informacijski rat (IWM) navodi da

[289] *http://www.pressonline.rs/page/stories/sr.html?id=44441&sectionId=40&view=story*

za nepoznate kineske hakere nije bilo granica – upadali su u kompjutere vlada širom sveta, njihovih ambasada, velikih firmi kao što je „Diloit i Tuš“ u Njujorku, kao i u lične računare najbližih saradnika premijera, novinara… Zasad postoje dokazi upada u 1.295 kompjutera u 103 zemlje, a među njima i u one koje je koristio NATO.[290]

Isto tako, kao posledica dnevnopolitičkih događaja koja se odražava u sajber kriminalu jeste i virtuelni rat između kosmetsko-albanskih i srpskih hakera, koji se predstavljaju kao Kosova Hackers Group[291] i United Jugoslavija Crew.[292] Svoje nezakonite „poduhvate“ ove dve grupe registruju na domenu *http://www.zone-h.org/index.php?option=com_attacks&Itemid=43&filter=1* iz kojeg se može uočiti da su do sada izvršili veliki broj *defacement*-a.[293]

Jedan od primera u kojima se internet koristi kao savršeno mesto za izvršenje krivičnog dela iznuda dolazi nam iz Bosne i Hercegovine, gde je jedan maloletni napadač iz Tuzle tražio od vlasnika domena *http://www.smokva.com* novčani iznos od 2.000 €, kako bi prestali sa DOS napadima na njihov server, i da bi svoju pretnju iskazao kao ozbiljnu, on je naveo da pod kontrolom ima oko 40.000 *botnetova*[294] i [295].

Kakve bi tek posledice bile kada bi učinioci krivičnih dela napali službe za snabdevanje vodom, električnom energijom, kontrolom leta, a koje u današnje vreme vrlo lako mogu da postanu meta sajber terorista. Stoga, na nedavnom kongresu u Londonu o sajber kriminalu, zvaničnici NATO-a skrenuli su pažnju da onlajn špijunaža i terorizam na internetu predstavljaju neke od najopasnijih pretnji globalnoj bezbednosti. Hakeri su u Americi već ušli u kompjuterski sistem Pentagona, u Indiji u ministarske fajlove, u Nemačkoj u kompjuter državnog kancelara, a Estonija je u aprilu prošle godine takođe bila žrtva sajber kriminala, kada je mnoštvo elektronskih pisama blokiralo elektronski sistem banaka i vlade.

Već sada sa sigurnošću može da se zaključi da je najveća svetska globalna mreža (internet) postala utočište organizovanog kriminala, te da je sajber kriminal profitabilna nezakonita aktivnost u kojoj učestvuju strukturirane or-

[290] *http://www.blic.rs/svet.php?id=85766*

[291] *http://www.khg-crew.ws/*

[292] *http://www.misterije.info/*

[293] Defacment je izmena stranice na serveru koji se napada, tačnije izmena prve stranice koja se dobija kada se ukuca internet adresa.

[294] Botnetovi su računari zaraženi zlonamernim programima koji omogućavaju njihovim autorima da preuzmu kontrolu nad napadnutim računarom bez znanja njegovog vlasnika, šaljući drugim računarima na internetu neželjene poruke elektronske pošte, viruse, kao i špijunske i druge zlonamerne programe, povećavajući na taj način broj zaraženih računara.

[295] *http://www.index.hr/vijesti/clanak.aspx?id=384531*

ganizovane grupe, čak i pojedinci koji se nikad nisu sreli uživo, ali koji sarađuju preko svetske globalne mreže.

Ono što je sigurno jeste da Srbija u korak prati svetske trendove u oblasti visokotehnološkog kriminala, te da ćemo u bliskoj budućnosti biti svedoci izvršenja krivičnih dela na isti način kao što smo opisivali u monografiji.

XII

PREPORUKE ZA IZMENU ZAKONODAVSTVA REPUBLIKE SRBIJE

UVOD

Jedan od najvažnijih preduslova za uspešan, stabilan i održiv razvoj društva svakako je i dobra pravna regulativa. Međutim, kvalitet pravnih normi ne zavisi, ili barem ne bi trebalo da zavisi, isključivo od pravnika. Prilikom formulisanja pravnih normi iz oblasti krivičnih dela koja generički možemo podvesti pod pojam visokotehnološkog kriminala neophodno je konsultovati i stručnjake i iz drugih, vanpravnih oblasti. Posebnu ulogu u tom procesu trebalo bi da imaju stručnjaci iz oblasti informacionih tehnologija, ali ne manje značajnu i ekonomisti – ukazivanjem na moguće ekonomske posledice različitih normativnih rešenja. Ovo stoga što se specifičnost visokotehnološkog kriminala ogleda i u posledicama koje prouzrokuje, prvenstveno u vidu ekonomske štete koja nije lako merljiva i najčešće prevazilazi imovinsku korist pribavljenu od strane pojedinca.

Takođe, s obzirom na vrstu predmeta kojima se vrše ova krivična dela *(računari, optički diskovi i sl.*), prilikom oblikovanja pravnih normi koje prate ovu oblast krivičnog prava bilo bi poželjno uključiti i stručnjake koji se bave različitim aspektima zaštite životne sredine, pre svega one koji se bave problemom uništavanja i reciklaže elektronskog otpada.

Primena neodgovarajuće metodologije u izradi zakona nesumnjivo predstavlja jedan od osnovnih razloga zbog kojih je dosadašnja pravna regulativa u ovoj oblasti bila manjkava. Razloge za takvo stanje svakako valja tražiti i u činjenici da je reč o kriminalu koji, svojom vitalnošću i mnoštvom pojavnih oblika, stavlja zakonodavca u inferioran položaj da u neravnopravnoj trci stalno sustiže inventivnost kriminalaca, iznova formulišući pravne norme, često anahrone već u trenutku njihovog donošenja.

U tom kontekstu, ni srpsko zakonodavstvo nije izuzetak.

Kada je u pitanju krivično zakonodavstvo, značajnu pomoć u otklanjanju navedenih problema i u osavremenjavanju krivičnih propisa iz oblasti visokotehnološkog kriminala svakako predstavljaju smernice eksperata Saveta Evrope iz oktobra 2007. godine, sadržane u izveštaju pod nazivom „Usklađenost KZ i ZKP Republike Srbije sa zahtevima Konvencije Saveta Evrope o visokotehnološkom kriminalu".[296]

Navedeni izveštaj izrađen je u okviru Projekta Saveta Evrope[297] za borbu protiv ekonomskog kriminala u trenutku kada je Republika Srbija bila samo potpisnica Konvencije o visokotehnološkom kriminalu.

---

[296] *Convention on Cybercrime,* Budapest, 23. XI 2001.

[297] *PACO Serbia – Project against economic crime in the Republic of Serbia.*

Dana 14. aprila 2009. godine Republika Srbija ratifikovala je Konvenciju i stala u red ne tako velikog broja evropskih država koje su to učinile pre nje. Ovim činom ona je preuzela obavezu da uskladi svoja zakonodavna rešenja sa standardima ponuđenim u Konvenciji, koji autorima ovog projekta predstavljaju pravni okvir za izmenu zakonodavstva, na način kako to dalje sledi.

Autori ovog projekta dalje smatraju da bi ponuđene standarde u najvećem obimu trebalo prihvatiti, bez korišćenja „prava na rezervu"[298] propisanu Konvencijom, s obzirom na to da široko definisanim pojmovima i savremenim normama na najbolji način regulišu ovu oblast, anticipirajući nove pojavne oblike kriminala koji samo još neupućenima mogu da izgledaju kao deo neostvarivog SF scenarija.

Iako se omaškom eksperata Saveta Evrope deo primedbi iz izveštaja ne odnosi na važeći, već na novi Zakonik o krivičnom postupku,[299] mišljenja smo da iznete primedbe treba uvažiti i na odgovarajući način inkorporirati u novi tekst Zakona o krivičnom postupku, koji je ponovo u izradi. Da li će se osavremenjivanje procesnog zakona svesti samo na promociju koncepta „tužilačke istrage", u ovom trenutku nije izvesno. Ono što je izvesno jeste činjenica da je postojeći procesni zakonik u tolikoj meri anahron da ozbiljno otežava primenu KZ-a, koji unošenjem novih pojmova i čitavih poglavlja novih krivičnih dela u dobroj meri prati tendencije savremenog krivičnog zakonodavstva.

Krivično zakonodavstvo Republike Srbije svakako je unapređeno i donošenjem Zakona o odgovornosti pravnih lica za krivična dela,[300] Zakona o pružanju međunarodne pravne pomoći u krivičnim stvarima[301] i Zakona o oduzimanju imovinske koristi iz krivičnog dela.[302] Međutim, problem neodgovarajuće zakonske regulative ne odnosi se samo na odredbe krivičnog zakonodavstva.

Uspešno suzbijanje visokotehnološkog kriminala i uspostavljanje bezbednosti svih korisnika informacionih tehnologija podrazumeva revidiranje postojećih i donošenje novih propisa kojima se reguliše oblast telekomunikacija,

[298] Svaka država može da, pismenim obaveštenjem generalnom sekretaru Saveta Evrope prilikom potpisivanja ili deponovanja instrumenata o potvrđivanju, prihvatanju, odobravanju ili pristupanju, izjavi da koristi pravo na rezervu propisanu u članu 4, stav 2; članu 6, stav 3; članu 9, stav 4; članu 10, stav 3; članu 11, stav 3; članu 14, stav 3; članu 22, stav 2; članu 29, stav 4 i članu 41, stav 1 (član 42 Konvencije).

[299] Najnovijim izmenama, primena Zakona odložena je do 31. decembra 2010. godine.

[300] „Službeni glasnik RS", br. 97/2008.

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

[302] „Službeni glasnik RS", br. 97/2008. Odredbe ovog zakona primenjuju se i na krivično delo Prikazivanje pornografskog materijala i iskorišćavanje dece za pornografiju – član 185, st. 2 i 3 Krivičnog zakonika.

zaštita ljudskih prava i intelektualne svojine. U tom delu, zakonodavna aktivnost u Republici Srbiji nije mnogo stagnirala, što je imalo za rezultat donošenje Zakona o zaštiti podataka o ličnosti,[303] Zakona o elektronskom potpisu[304] i Zakona o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine[305] koji bi trebalo izmeniti u pogledu odgovornosti samostalnih trgovinskih radnji i drugih preduzetnika zbog izvršenih prekršaja i privremenih prestupa, predviđenih ovim zakonom.

Što se tiče upotpunjavanja pravne regulative u okviru koje bi se odvijala borba protiv visokotehnološkog kriminala, potrebno je napomenuti da se Zakon o elektronskoj trgovini[306] nalazi u skupštinskoj proceduri, Nacrt zakona o elektronskom dokumentu[307] u fazi javne rasprave, dok za Zakon o optičkim diskovima, koji u ovom trenutku svakako nedostaje, sa žaljenjem moramo da konstatujemo da se ne nalazi čak ni u fazi nacrta za čiju je izradu zaduženo resorno Ministarstvo za kulturu Republike Srbije.

Naravno, u preporukama za izmenu zakonodavstva RS mesto je našao i predlog izmena *Zakona o organizaciji i nadležnosti državnih organa u suzbijanju visokotehnološkog kriminala,*[308] koje bi se sastojale u proširivanju stvarne nadležnosti ovih organa na sva krivična dela koja po načinu, sredstvima i objektu izvršenja predstavljaju dela iz oblasti visokotehnološkog kriminala.

Uvereni smo da će donošenje ovih zakona i izmena postojećih dati dovoljno kvalitetan i celovit pravni okvir koji će pružiti sve preduslove za suprotstavljanje visokotehnološkom kriminalu na mnogo efikasniji način od sadašnjeg.

Bez folklornih, tradicionalnih ili drugih lokalnih obeležja, visokotehnološki kriminal svojim nadnacionalnim i transnacionalnim karakterom snažno nameće unifikaciju zakonodavnih rešenja, ne toliko zbog nužnosti uspostavljanja svih oblika međunarodne saradnje, koliko zbog činjenice da pravna nauka nužno mora da prati logiku razvoja, upotrebe i zloupotrebe informacionih tehnologija koje po svojoj egzaktnoj, matematičkoj prirodi binarnog koda ne dopuštaju različit pristup i razumevanje, u zavisnosti od rase, kulture ili društveno-političkog uređenja.

---

[303] „Službeni glasnik RS“, br. 97/2008.
[304] „Službeni glasnik RS“, br. 135/2004.
[305] „Službeni glasnik RS“, br. 46/2006.
[306] *www.parlament.sr.gov.yu/content/lat/akta/akta_detalji.asp?Id=710&t=P#*
[307] *www.mtid.gov.rs/upload/documents/Nacrt zakona o elektronskom dokumentu 22. 3. 2009.pdf*
[308] „Službeni glasnik RS“, br. 61/2005.

2. PREDLOZI IZMENA

2.1. Krivično zakonodavstvo

Predlozi izmena koji slede odnose se na dva najvažnija sistemska zakona, Krivični zakonik i Zakonik o krivičnom postupku.

2.1.1. Krivični zakonik

Glava XII Krivičnog zakonika

Predlog izmena započeli bismo već od Glave XII KZ-a, u kojoj se definiše značenje izraza u zakonu.

Član 112 u tačkama 16, 17, 18, 19 i 20 sadrži definiciju određenih pojmova vezanih za visokotehnološki kriminal, međutim, shodno primedbama koje su navedene u Ekspertizi, smatramo da bi u Glavi XII Krivičnog zakonika trebalo *uneti, odnosno izmeniti sledeće pojmove*:

1. „*Računar*“

Poslednjim izmenama Krivičnog zakonika, u poglavlju „Značenje izraza u zakonu“ propušteno je unošenje pojma „računar“ i njegove definicije. Njegovo unošenje i pravilna definicija od posebnog su značaja s obzirom na raznolikost uređaja koji kao jednu od svojih funkcija mogu imati – osim prenosa podataka i automatsku obradu podataka – AOP (*mobilni telefoni, PDA uređaji i sl*.).

Stoga, u Krivični zakonik potrebno je uneti pojam „računar“ čija bi definicija trebalo da glasi:

Računar predstavlja svaki elektronski uređaj koji na osnovu programa automatski obrađuje i razmenjuje podatke.

2. „*Računarski sistem*“

Takođe, u Krivični zakonik potrebno je uneti i pojam „računarski sistem“ koji bi svojom širom definicijom *zamenio* pojam i definiciju računarske mreže iz tačke 18, a njegova definicija trebalo bi da glasi:

Računarski sistem je svaki uređaj ili grupa međusobno povezanih ili zavisnih uređaja, od kojih jedan ili više njih na osnovu programa vrši automatsku obradu i razmenu podataka.

3. „*Računarski podatak*“

Potrebno je *izmeniti* definiciju „računarskog podatka“ koja je data tačkom 17 Krivičnog zakonika, te bi ona sada trebalo da glasi:

*Računarski podatak je svako predstavljanje činjenica, informacija ili koncepata**,** u obliku prikladnom za obradu u računarskom sistemu.*

Ovim izmenama Krivični zakonik bi bio u potpunosti usklađen sa članom 1 Konvencije o sajber kriminalu.

Sledeći set predloga izmena Krivičnog zakonika odnosio bi se na pojedinačno predviđene radnje izvršenja krivičnih dela koja su definisana u više glava Krivičnog zakonika, a koja bi usvojenom izmenom Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala bila u nadležnosti Posebnog tužilaštva za visokotehnološki kriminal.

Krivična dela protiv polne slobode

Član 9 Konvencije o sajber kriminalu uspostavlja određene obaveze po pitanju definicije zaštitnog objekta, kao i po pitanju radnji izvršenja ovog krivičnog dela, zbog čega smatramo da bi član 185 KZ-a morao u velikom delu da bude izmenjen, počevši od samog naziva krivičnog dela, kako bi bio u skladu sa Konvencijom o sajber kriminalu.

On bi sada, po našem predlogu, trebalo da glasi:

Prikazivanje i posedovanje pornografskog materijala i iskorišćavanje dece i maloletnika za pornografiju

Član 185.

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

kazniće se novčanom kaznom ili zatvorom do šest meseci.

(2) Ko iskoristi dete ili maloletnika za proizvodnju slika, audio-vizuelnih ili drugih predmeta pornografske sadržine ili za pornografsku predstavu,

kazniće se zatvorom od šest meseci do pet godina.

(3) Ko poseduje, prodaje, prikazuje, javno izlaže ili na drugi način čini dostupnim slike, audio-vizuelne ili druge predmete pornografske sadržine koji prikazuju decu ili maloletnike u seksualno eksplicitnom ponašanju,

kazniće se zatvorom do dve godine.

4) Predmeti iz člana od 1 do 3 ovog stava oduzeće se.

Smatramo da je neophodno ozbiljno razmotriti pitanje visine zaprećene kazne zatvora propisane u članu 185, s obzirom na to da su u uporednom zakonodavstvu za samo posedovanje zaprećene strože kazne zatvora. Inače, član 9 Konvencije o sajber kriminalu jasno uspostavlja obavezu definisanja inkriminacije i za samo posedovanje materijala dečje pornografije – što u dosadašnjem Krivičnom zakoniku nije bio slučaj, a kao takvo je inkriminisano u zakonodavstvu kako susednih zemalja, tako i zemalja Evropske unije.

Posebno ističemo sledeće:

Imajući u vidu preporuke sadržane u ekspertizi Saveta Evrope, smatramo da je *neophodno definisati novi član Krivičnog zakonika* koji bi imao numeraciju „član 185a“ i koji bi se odnosio na proizvodnju, distribuciju, nabavljanje i posedovanje dečje pornografije *preko računarskog sistema*.

Izvršenje krivičnog dela iz člana 185 KZ uz pomoć računarskog sistema ili mreže u uporednom zakonodavstvu predviđeno je kao poseban oblik izvršenja i kao takvom, unošenjem novog člana Zakona, dato mu je zasebno mesto, između ostalog, zbog specifičnosti njegovog otkrivanja, prikupljanja, čuvanja i prezentovanja dokaza, te zbog svih drugih specifičnosti koje su zajedničke za krivična dela iz oblasti visokotehnološkog kriminala.

Predložena numeracija poznata je i u uporednom zakonodavstvu susednih država *(Kazneni zakon Republike Hrvatske takođe je uneo novi član Zakona, označavajući ga brojem već postojećeg, uz dodavanje slova „A“ iza postojeće numeracije)*.

Prema tome, novo krivično delo trebalo bi da glasi:

Dečja pornografija na računarskom sistemu ili mreži

(1) Ko pomoću računarskog sistema ili mreže proizvodi, nudi, distribuira, pribavlja za sebe ili drugog, ili ko u računarskom sistemu ili na mestima za skladištenje računarskih podataka poseduje pornografske sadržaje koji prikazuju decu ili maloletnike, ili simulovano realne slike koje predstavljaju decu ili maloletnike, koji učestvuju u seksualno eksplicitnoj radnji,

kazniće se kaznom zatvora od jedne do deset godina.

(2) Ko detetu ili maloletniku posredstvom računarskog sistema, mreže ili medija za skladištenje računarskih podataka učini dostupnim slike, audiovizuelne sadržaje ili druge predmete pornografskog sadržaja,

kazniće se novčanom kaznom ili kaznom zatvora do tri godine.

(3) Predmeti, sredstva i podaci korišćeni za izvršenje krivičnih dela iz st. 1 i 2 ovog člana, oduzeće se.

Pri razmatranju osnovanosti unošenja člana 185a u Krivični zakonik moramo imati u vidu da je iz analize zakonodavne prakse drugih država koje su ratifikovale, ili samo potpisale, Konvenciju proistekao zaključak da je distribucija ovakve vrste materijala putem računarskih sistema mnogo ozbiljnije krivično delo nego distribucija materijala uz pomoć drugih medija, što je uslovilo i propisivanje zaprećene kazne zatvora u dužem trajanju.

Opravdanje za strožu kaznenu politiku leži u činjenici rasprostranjenosti računarskih sistema i mreža, kao i u njihovoj dostupnosti sve većem broju ljudi, te lakoći pristupa inkriminisanim sadržajima.

Što se tiče kažnjivosti distribucije simulovanih realnih slika koje predstavljaju maloletnika koji učestvuje u eksplicitno seksualnoj radnji, ona je kao takva posledica preporuke Saveta Evrope i Konvencije o sajber krimina-

lu, a proističe iz činjenice da se na internetu nalazi veliki broj ovakvih sadržaja u vidu animiranih filmova, stripova i crteža (npr. hentai anime filmovi ili manga stripovi).

Krivična dela protiv intelektualne svojine

S obzirom na činjenicu da se autorska dela neovlašćeno mogu umnožavati i stavljati u promet i u okviru delatnosti privrednih subjekata (preduzeća i preduzetnika), smatramo da je navedenu pojavu neophodno krivično sankcionisati (prema postojećim zakonskim rešenjima u Republici Srbiji, inkriminacije protiv intelektualne svojine učinjene od strane preduzetnika nisu predviđene ne samo kao krivično delo već one ne predstavljaju ni prekršaj) između ostalog i zbog činjenice što je radnje izvršenja krivičnih dela protiv intelektualne svojine koje se preduzimaju kroz obavljanje redovne delatnosti privrednih subjekata teže uočiti – otkriti, što ih načelno čini društveno opasnijim u odnosu na inkriminisane radnje preduzete od strane pojedinca.

U tom smislu, u opisu svih krivičnih dela iz Glave XX, na svim mestima, iza reči „ko“ trebalo bi dodati reči „samostalno ili u okviru svoje delatnosti subjekta privrednog poslovanja“. Sledstveno tome, u ovom i nekim drugim poglavljima Krivičnog zakonika neophodno bi bilo propisati odgovornost i krivične sankcije za pravna i odgovorna lica u pravnom licu, koja u okviru svojih poslova ili ovlašćenja učine krivično delo, što bi predstavljalo doslednu primenu postojećih odredaba Zakona o odgovornosti pravnih lica za krivična dela, koji je, van svake logike, donet u vidu posebnog zakona umesto u okviru izmena postojećeg KZ-a. S obzirom na to da Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine kvalifikuje inkriminacije pravnih lica kojima se povređuje pravo na intelektualnu svojinu kao privredni prestup, mišljenja smo da bi navedeni predlog u pogledu odgovornosti pravnih lica za krivična dela mogao stvoriti probleme u praksi u vidu primene odgovarajućih propisa, što ukazuje na potrebu izmene kaznenih odredaba navedenog zakona, čime bi kvalifikacija izvršenog privrednog prestupa bila rezervisana isključivo za lakše oblike inkriminacija koje se u svom opisu ne podudaraju sa već propisanim krivičnim delima.

U pogledu visine zaprećenih kazni, smatramo da je za učinioce krivičnog dela iz člana 199, stav 4 KZ-a i 200 KZ-a trenutno propisana preblaga krivična sankcija. Ovo stoga što je reč o inkriminisanim radnjama kojima se uklanjaju ili zaobilaze tehnološke mere namenjene sprečavanju povreda autorskih i srodnih prava i koje kao takve omogućavaju izvršenje krivičnih dela iz čl. 198 i 199 KZ-a, odnosno izvršenje krivičnih dela protiv intelektualne svojine, te zato smatramo da je adekvatno sankcionisanje izvršilaca krivičnih dela iz

člana 199, stav 4 i 200 KZ-a jedan od neophodnih preduslova da bi se fenomen piraterije uopšte i suzbio (prevazilaženje ili uklanjanje DRM zaštite autorskih dela ili, npr. uklanjanje sa mobilnog telefona originalnog fabrički podešenog softvera – kodiranog za određenu mrežu mobilne telefonije i instaliranje izmenjenog softvera – tzv. dekodiranje).

S obzirom na napred navedeno, smatramo da bi adekvatna krivična sankcija za oba krivična dela bila kazna zatvora od tri meseca do pet godina.

Krivična dela protiv privrede

Falsifikovanje i zloupotreba platnih kartica – član 225 Krivičnog zakonika

Osnovni problem u vezi sa dosadašnjim definisanjem krivičnog dela Falsifikovanje i zloupotreba platnih kartica iz člana 225 KZ-a jeste u činjenici da je zakonodavac imao u vidu isključivo platne kartice u fizičkom obliku, te je mogućnost njihove zloupotrebe sveo isključivo na ovaj oblik, istovremeno previdevši mogućnost zloupotrebe jedinstvenih podataka o platnoj kartici, bez njene fizičke upotrebe i bez pravljenja i posedovanja platne kartice u njenom fizičkom obliku (*E-banking* i *E- Commerce*).

Mišljenja smo da se navedeno mora imati u vidu i da se Krivičnim zakonikom mora predvideti i ovaj oblik izvršenja krivičnog dela iz razloga što u konkretnom slučaju nastupa ista štetna posledica, a izvršilac krivičnog dela i oštećeni su identični, bilo da je zloupotreba platne kartice izvršena u njenom fizičkom obliku, ili u odnosu na podatke koje sadrži i služe za njenu identifikaciju u platnom prometu u elektronskom obliku.

U tom smislu, *izmene* bi bile sadržane u stavu 4 člana 225 KZ-a, koji bi sada trebalo da glasi:

(4) Kaznom iz st. 2 i 3 ovog člana kazniće se učinilac koji to delo učini neovlašćenom upotrebom tuđe kartice, ili poverljivih podataka koji jedinstveno određuju tu karticu u platnom prometu.

Pravljenje, nabavljanje i davanje drugom sredstava za falsifikovanje – član 227 Krivičnog zakonika

Mišljenja smo da treba pooštriti krivičnu sankciju za radnju izvršenja opisanu u stavu 2 člana 227 KZ-a, s obzirom na to da je reč o ravnopravnom sredstvu plaćanja, te da platne kartice sve više učestvuju u ukupnom platnom prometu, a strože inkriminisanje radnji opisanih u navedenom stavu preduslov su i uspešnog suzbijanja izvršenja krivičnih dela iz člana 225 KZ-a.

U tom smislu, kao krivičnu sankciju za inkriminaciju opisanu u stavu 2 člana 227 *predlažemo* izricanje kazne zatvora od šest meseci do pet godina.

Krivična dela protiv bezbednosti računarskih podataka

Napomena: s obzirom na predložene nove definicije pojmova u članu 112 KZ-a, odnosno davanja definicije „računarskog sistema" kao pojma koji u sebi sadrži i definiciju pojma „računarska mreža", shodno tome – na svim mestima u Glavi XXVIII pojam „računarske mreže" treba *zameniti* pojmom „računarski sistem".

Konvencija o sajber kriminalu preporučuje u članu 3 da svaka strana ugovornica treba da usvoji i zakonodavne mere neophodne da bi se kao krivično delo u domaćem zakonodavstvu propisalo i protivpravno presretanje prenosa računarskih podataka koji nisu javne prirode.

Pored navedenog, imajući u vidu i ekspertski izveštaj Saveta Evrope o usklađenosti domaćeg krivičnog zakonodavstva sa Konvencijom o sajber kriminalu, analizom krivičnih dela iz ove glave Zakonika utvrđeno je da ista ne propisuju radnju izvršenja koja bi se odnosila na presretanje računarskih podataka u opisanom smislu, uz preporuku je da je to potrebno učiniti.

Kako smo mišljenja da su iznete primedbe ekspertize u tom delu osnovane, smatramo da bi navedene inkriminisane radnje trebalo definisati *u okviru* postojećeg krivičnog dela opisanog u članu 302 Krivičnog zakonika, čiji bi naziv sada trebalo da glasi:

Neovlašćen pristup zaštićenom računaru, računarskom sistemu i presretanje nejavnog prenosa računarskih podataka

Shodno napred navedenom, predmetnu radnju izvršenja potrebno je definisati u *novom stavu 4* člana 302 koji treba da glasi:

(4) Kaznom iz stava 1 ovog člana kazniće se ko presretne ili snimi nejavni prenos računarskih podataka koji mu nisu namenjeni, prema računarskom sistemu, od njega ili unutar samog sistema, uključujući i elektromagnetna emitovanja iz računarskog sistema kojim se prenose takvi podaci.

Takođe, predlažemo da se u postojeći član 302 unese i *novi stav 5* koji bi trebalo da glasi:

(5) Ako je delo iz st. 1, 2 i 4 ovoga člana učinjeno u odnosu na zaštićeni računar, računarski sistem i nejavni prenos podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte,

kazniće se kaznom zatvora od šest meseci do pet godina.

U vezi sa napred datom definicijom, smatramo da bi eventualno trebalo razmisliti o izostavljanju reči „*koji su od značaja za*" iz člana 229 i člana 302 KZ-a, s obzirom na činjenicu da su računarski sistemi svih državnih organa i

javnih službi, kao i podaci koji su u njemu sadržani, po svojoj prirodi, od posebnog javnog interesa.

U napred navedenom smislu, smatramo da je potrebno precizno definisati pojam „računarski sistemi i podaci državnih organa i javnih službi", s obzirom na to da izvršenje krivičnih dela u odnosu na ovakve sisteme i podatke nesporno predstavlja kvalifikovani oblik, te ga je kao takvog potrebno strože inkriminisati.

Formulacija koja se koristi u krivičnom delu Računarska sabotaža iz člana 299 KZ-a i koja je sledstveno tome implementirana u predloženi stav 5 člana 302 – „*koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte*" smatramo da je nedovoljno precizna i ne sledi ideju potrebe zaštite javnog interesa kroz poistovećivanje sa „drugim subjektima" – pod kojim pojmom se mogu podrazumevati i subjekti čija delatnost nije od javnog interesa.

Ukoliko bi se pojam „javnog interesa" implementirao u opis krivičnih dela iz poglavlja krivičnog dela protiv bezbednosti računarskih podataka, to bi pretpostavljalo i davanje precizne definicije u članu 112 KZ-a „Značenje izraza u zakonu".

Pored navedenog, formulacija „*koji su od značaja za*", a koja se kao takva koristi u članu 299 KZ-a, ostavlja širok prostor za tumačenje – šta bi se trebalo smatrati takvim računarskim podatkom ili računarskim sistemom u smislu zaštitnog objekta, odnosno da li su to podaci u okviru računarskog sistema državnih organa, što bi bilo nesporno, ili su to i podaci koji se nalaze i van takvog sistema, a od značaja su za državne organe i javne službe.

Članom 6 Konvencije o sajber kriminalu preporučeno je i usvajanje zakonodavnih mera kojima bi se sprečila protivpravna proizvodnja, prodaja, nabavljanje radi upotrebe, uvoz i distribucija, kao i drugi oblici stavljanja na raspolaganje uređaja, računarskih programa, računarskih lozinki, pristupnih šifara ili sličnih podataka – izrađenih ili prilagođenih prvenstveno u svrhu izvršenja krivičnih dela iz Poglavlja XXVIII Krivičnog zakonika.

Takođe, navedenim članom Konvencije predloženo je inkriminisanje i samog posedovanja takvih uređaja i programa, međutim, kako u našem Krivičnom zakoniku navedene radnje nisu inkriminisane, predlažemo *unošenje novog člana* u Krivični zakonik, sa numeracijom „član 305" koji bi imao naziv:

Neovlašćena proizvodnja, nabavljanje, stavljanje u promet i posedovanje uređaja i sredstava koji se koriste u izvršenju krivičnih dela protiv bezbednosti računarskih podataka, a trebalo bi da glasi:

Član 305.

(1) Ko neovlašćeno proizvodi, prodaje, nabavlja radi upotrebe, uvozi, distribuira, poseduje ili stavlja drugom na raspolaganje posebne uređaje, sredstva, računarske podatke ili programe napravljene ili prilagođene u cilju izvršenja krivičnih dela iz člana 298 KZ-a, 299, 300, 301, 302, 303, 304 i 306 KZ-a,

kazniće se zatvorom od šest meseci do pet godina.

(2) Posebni uređaji, sredstava, računarski podaci ili programi, proizvedeni ili prilagođeni za izvršenje krivičnih dela iz stava 1 ovog člana, oduzeće se.

Članom 7 Konvencije o sajber kriminalu preporučeno je usvajanje zakonodavnih mera kojima bi se kao krivično delo propisalo unošenje, menjanje, brisanje ili prikrivanje računarskih podataka, koje za posledicu ima neverodostojnost podataka, u nameri da se oni smatraju verodostojnim i da se sa njima u pravnom saobraćaju postupa kao da su verodostojni, bez obzira na to da li su ti podaci direktno čitljivi i razumljivi, kada je to učinjeno sa namerom i protivpravno. U tom smislu, primedbe iznete u Ekspertizi smatramo osnovanim, između ostalog, imajući u vidu i činjenicu da je u Republici Srbiji razvoj u smeru uvođenja i upotrebe digitalnih dokumenata u pravni saobraćaj podržan, između ostalog i izradom zakonske osnove u vidu donetog Zakona o elektronskom potpisu.

U tom smislu predlažemo da se u Poglavlju XXVIII „Krivična dela protiv bezbednosti računarskih podataka", sa numeracijom u vidu člana 306**,** definišu napred pomenute inkriminacije u novom krivičnom delu koje bi nosilo naziv *Računarsko falsifikovanje*, a koje bi trebalo da glasi:

Član 306.

(1) Ko neovlašćeno izradi, unese, izmeni, izbriše ili na drugi učini neupotrebljivim računarske podatke ili programe, bez obzira na to da li su direktno čitljivi i razumljivi, koji su od značaja za pravni saobraćaj u nameri da se oni upotrebe kao pravi ili ko upotrebi takve programe ili podatke, ili ih nabavi radi upotrebe,

kazniće se novčanom kaznom ili kaznom zatvora do tri godine.

(2) Ako je krivično delo iz stava 1 ovog člana učinjeno u odnosu na računarske podatke ili programe državnih organa, javnih službi, ustanova, preduzeća ili drugih subjekata ili je prouzrokovana znatna šteta, učinilac će se

kazniti kaznom zatvora od tri meseca do pet godina.

(3) Za pokušaj krivičnog dela iz stava 1 i 2 ovog člana kazniće se.

U vezi sa upotrebljenim pojmovima „*...državnih organa, javnih službi, ustanova, preduzeća ili drugih subjekata*", ostajemo pri iznetoj sugestiji u pogledu određivanja pojma javnog interesa i preciznog definisanja značaja računarskih podataka i sistema državnih organa i javnih službi.

I najzad, u skladu sa primedbama iznetim u ekspertskom izveštaju Saveta Evrope, koje se odnose na krivično delo Pravljenje i unošenje računarskih virusa iz člana 300 KZ-a, u smislu da ovaj član inkriminiše samo stvaranje i unošenje računarskog virusa *(dok ostali napadi prouzrokovani računarskim crvom ili bilo kojim drugim oblikom zlonamernih programa ostaju neinkri-*

minisani), smatramo da je prethodno potrebno u okviru člana 112 Krivičnog zakonika definisati pojam „zlonamernog programa“ koja bi trebalo da glasi:

Zlonamerni program je svaki program napravljen ili iskorišćen u nameri da na bilo koji način ošteti računar ili računarski sistem, ili oteža, ili onemogući njihovo korišćenje, a potom, u skladu sa tim *izmeniti* naziv i tekst krivičnog dela iz člana 300 KZ-a, koji bi sada trebalo da glase:

Pravljenje i unošenje računarskih virusa ili zlonamernih programa

(1) Ko napravi računarski virus ili zlonamerni program u nameri njegovog unošenja u tuđ računar ili računarski sistem,

kazniće se novčanom kaznom ili zatvorom do šest meseci.

(2) Ko unese računarski virus ili zlonamerni program u tuđ računar ili računarski sistem i time prouzrokuje štetu,

kazniće se novčanom kaznom ili zatvorom do dve godine.

(3) Uređaj i sredstva kojima je učinjeno krivično delo iz st. 1 i 2 ovog člana, oduzeće se.

U skladu sa napred navedenim, smatramo da bi trebalo razmisliti i o uvođenju kvalifikovanog oblika ovog krivičnog dela ukoliko bi objekat izvršenja bili računarski sistemi državnih organa ili javnih službi.

2.1.2. Zakonik o krivičnom postupku

Iako se omaškom eksperata Saveta Evrope deo primedbi iz izveštaja ne odnosi na važeći,[309] već na novi Zakonik o krivičnom postupku,[310] čija je primena odložena do 31. decembra 2010. godine, mišljenja smo da bi iznete primedbe trebalo uvažiti i na odgovarajući način inkorporirati u novi tekst Zakona o krivičnom postupku, koji je *ponovo u izradi*.

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 priključio 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*. Treba imati u vidu da

[309] „Službeni list SRJ“, br. 70/2001, 68/2002, „Službeni glasnik RS“, br. 58/2004, 85/2005, 115/2005, 49/2007, 122/2008, 20/2009.

[310] „Službeni glasnik RS“, br. 46/2006, 49/2007, 122/2008.

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.

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

Odsustvo pravne regulative koja bi se odnosila na procesni aspekat progona krivičnih dela iz oblasti visokotehnološkog kriminala najuočljivije je u članu 221 Glave XVII ZKP-a, u kojem nije dato značenje nijednog zakonskog izraza koji bi se odnosio na visokotehnološki kriminal.

Postojeći ZKP ne daje ni elementarnu definiciju dokaza, a kamoli elektronskog,[311] koji se pojavljuju u vezi sa izvršenjem krivičnih dela visokotehnološkog kriminala.

U tom delu, „novi" ZKP, sa odloženom primenom, učinio je mali pomak u odnosu na postojeći, pružajući u okviru člana 22 značenje izraza „*isprava*",[312] te izraza „*spis, pismeno, pošiljka i drugi dokumenti*".[313]

Uz proširivanje liste zakonskih izraza čije bi značenje trebalo dati u ZKP-u, koji je trenutno u izradi, unošenje napred navedenih ima svoje opravdanje, naročito značenje izraza „*spis, pismeno, pošiljka i drugi dokumenti*" koji se prema datoj definiciji odnose i na dokaze i isprave sadržane u spisima, što je od izuzetne važnosti u postupku izvođenja i prezentacije dokaza pred sudom. Unošenjem navedenih odredaba u finalnu verziju ZKP-a, „validirala" bi se aktuelna sudska i tužilačka praksa da dokazi i isprave sadržani u spisima mogu biti u elektronskoj formi, odnosno nalaziti se snimljeni na optičkom disku, ili drugom odgovarajućem medijumu predviđenom za pohranjivanje i čuvanje računarskih podataka.[314]

---

[311] Elektronski dokaz je informacija ili podatak koji su značajni za istragu, 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, 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.

[312] Ispravom se smatra svaki predmet koji je podoban ili određen da služi kao dokaz kakve činjenice, koji ima značaj za pravne odnose ili je značajan u krivičnom postupku, što se odnosi i na računarske podatke zabeležene u odgovarajućem nosiocu podataka.

[313] 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.

[314] Enormno veliki broj naslova autorskih dela koji bi se morao navesti u potvrdi o privremeno oduzetim predmetima, u formi kataloga, prilaže se uz potvrdu na optičkom disku i čini njen sastavni deo.

S obzirom na činjenicu da važeći Zakonik o krivičnom postupku ne predviđa posebne dokazne radnje niti posebna ovlašćenja vezana za otkrivanje dela iz oblasti VT kriminala, za početak, lista zakonskih izraza čije bi značenje trebalo dati u ZKP-u, koji je u izradi, morala bi da obuhvati pojmove/izraze kao što su: računar, računarski podatak, relevantan računarski podatak, računarski program, računarski sistem, davalac internet usluga, davalac usluge hostovanja, podaci o pretplatniku, internet, podatak o internet saobraćaju, vreme zadržavanja podataka, presretanja komunikacije u realnom vremenu, mreža 24/7 itd.

Dužina liste zakonskih izraza čije bi značenje trebalo dati u ZKP-u direktno će zavisiti od obima implementiranih zakonodavnih rešenja ponuđenih Konvencijom,[315] pri čemu se mora voditi računa o već postojećim definicijama pojmova u aktuelnom Krivičnom zakoniku.

Odredbe ZKP-a koje se u odsustvu odgovarajućih, primenom analogije, primenjuju u postupku otkrivanja krivičnog gonjenja i suđenja zbog učinjenih krivičnih dela iz oblasti VT kriminala jesu:

Odredbe koje se odnose na radnje dokazivanja iz Glave VII, i to:

1. Pretresanje stana i lica iz čl. 77–81 (radnje relevantne za obezbeđivanje dokaza koji se nalaze u stanu počinioca);

Privremeno oduzimanje predmeta, iz čl. 82–85 (oduzimanje i pečaćenje kućišta računara i druge tehničke opreme, mogućnost kontrole pisama i pošiljki osumnjičenog, koje praksa tretira i kao elektronsku poštu, prispele novčane i druge pošiljke proistekle iz bavljenja „piraterijom“ i dr.);

Uviđaj, iz čl.110–112 (pregled računara i druge tehničke opreme na licu mesta uz prisustvo stručnog lica koje će, po potrebi, preduzeti i pronalaženje, obezbeđivanje ili opisivanje tragova, izvršiti potrebna merenja i snimanja, sačiniti skice ili prikupiti druge podatke);

Veštačenje, iz čl. 113–123 (veštačenja od strane veštaka informatičke struke ili ustanove i dela državnog organa kao što je Služba za specijalne istražne metode MUP-a RS).

2. Odredbe ZKP-a iz člana 220, kojima je predviđena obaveza svih državnih organa da sudovima i drugim organima koji učestvuju u krivičnom postupku pruže potrebnu pomoć, naročito ako je reč o otkrivanju krivičnih dela i pronalaženju učinilaca (*nesankcionisana dispozicija koja bi se mogla koristiti prilikom obraćanja za dostavljanje relevantnih podataka*).

3. Odredbe ZKP-a iz člana 234, koje predviđaju uslove za izdavanje naredbe bankarskoj, finansijskoj ili drugoj organizaciji za dostavljanje podataka o stanju na poslovnim ili ličnim računima osumnjičenog lica za krivična dela za

[315] *Convention on Cybercrime,* Budapest, 23. XI 2001.

koja je zakonom propisana kazna zatvora od najmanje četiri godine (*pribavljanje podataka od banaka i pošte radi utvrđivanja visine imovinske koristi pribavljene izvršenjem, npr. krivičnih dela iz člana 199, stav 3 ili 208, st. 3 i 4 u vezi sa st. 1 i 2 KZ-a*).

4. Odredbe ZKP-a iz člana 238, koje predviđaju mogućnost da za krivična dela za koja je propisana kazna zatvora do deset godina organi unutrašnjih poslova mogu sami obaviti uviđaj i odrediti veštačenja koja ne trpe odlaganje, ako istražni sudija nije u mogućnosti da odmah izađe na lice mesta.

Nažalost, odredbe člana 232 ZKP-a, 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.

Ukoliko, polazeći od ovoga, uporedimo operativne kapacitete ZKP-a sa jednim od zakonodavnih rešenja krivičnog zakonodavstva Republike Francuske, kojim se omogućava pretres ciljnog računara preko interneta,[316] uz prethodno dobijenu naredbu istražnog sudije, lako možemo shvatiti u kolikoj meri zaostajemo za savremenim zakonodavstvom.

Ostale specijalne istražne metode[317] 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, i za krivična dela protiv čovečnosti i međunarodnog prava.

Paradoks je da su specijalna istražna radnja „Snimanje telefonskih i drugih razgovora“ (npr. *fiksna i mobilna telefonija, Skype i Voip*) i „obična“ 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! Suspendovanje takvih dokaznih radnji ravno je

[316] Onlajn pretres ubacivanjem određenog programa dok je ciljni računar konektovan na internet, koji vrši pregled računara i dostavljanje potrebnih podataka.

[317] Glava XXIXa ZKP-a „Posebne odredbe o postupku za krivična dela organizovanog kriminala“.

situaciji u kojoj bi, na primer, bila isključena mogućnost fiksiranja materijalnih tragova putem vršenja uviđaja, iz čl.110–112. ZKP-a, u prikupljanju dokaza povodom izvršenih krivičnih dela protiv javnog saobraćaja.

Zakonik o krivičnom postupku, koji je u izradi, moraće da predvidi posebne dokazne radnje i ovlašćenja u vezi sa otkrivanjem dela iz oblasti VT kriminala.

U pogledu izmene članova ZKP-a iz glave VII, kojim se propisuju radnje dokazivanja, uz odgovarajuću stilizaciju, u iste bi trebalo uneti:

- u članu 85, odredbe koje se tiču naredbe istražnog sudije internet i hosting provajderima i drugim pravnim i fizičkim licima za hitnu zaštitu određenih računarskih podataka koji će biti zadržani i potom predati sudu,[318] kao i odredbe koje se tiču prikupljanja podataka o ostvarenom saobraćaju;[319]
- u čl. 77–81, odredbe koje se tiču procedure pretresa stana i drugih prostorija u kojima je zatečena računarska oprema;
- u članu 82 odredbe koje se tiču zaplene[320] zatečene računarske opreme ili podataka;
- u tački 7 poglavlja u kojoj su definisane dokazne radnje veštačenja, samostalne odredbe koje se tiču stručnog profila lica i ustanova koje vrše IT veštačenja, procedure u radu na oduzetoj računarskoj opremi i podacima, i načini izrade nalaza i mišljenja tako obavljenih veštačenja;
- u članu 232, odredbe koje bi proširile primenu postojećih i u odnosu na komunikaciju podataka u realnom vremenu i njihovo presretanje.[321]

Sa aspekta otkrivanja i krivičnog gonjenja učinilaca krivičnih dela iz oblasti visokotehnološkog kriminala, kao i sa aspekta upotrebe informacionih tehnologija radi lakše primene i sprovođenja materijalnih zakona, pre svega KZ-a, Zakonik o krivičnom postupku moraće da doživi temeljne izmene.

---

[318] Ovaj instrument je neophodan da bi se obezbedilo da relevantni računarski podaci ne budu izbrisani pre nego što organi za sprovođenje zakona budu imali priliku da ih fiksiraju i obezbede za potrebe samog krivičnog postupka.

[319] IP-adresa je klasična informacija o saobraćaju koja nastaje prilikom korišćenja internet usluga. Bez pristupa tim podacima, skoro da je nemoguće identifikovati nepoznatog osumnjičenog.

[320] Procedura zaplene u nekim pravnim sistemima ograničava se na zaplenu fizičkih predmeta. To može da prouzrokuje teškoće u onim slučajevima kada su relevantne informacije zapamćene na serveru sa podacima stotina ostalih korisnika koji više neće biti dostupni kada organi za sprovođenje zakona zaplene server. Drugi primer kada tradicionalni pretres i zaplena materijalnih predmeta nisu dovoljni jeste slučaj kada organi za sprovođenje zakona ne znaju fizičku lokaciju servera ali mogu da mu pristupe preko interneta.

[321] To uključuje fajlove preuzete sa veb sajtova ili sistema za razmenu fajlova, elektronsku poštu poslatu ili primljenu od strane učinioca krivičnog dela i sadržaj četovanja.

U tom smislu, „novi“ ZKP uneo je novinu u član 200, predviđajući pozivanje učesnika u postupku i obaveštavanje o odlukama koje se tiču odlaganja glavnog pretresa ili drugih zakazanih radnji, putem elektronske poštom ili drugih elektronskih prenosilaca poruka, pod uslovom da je takvim načinom pozivanja moguće obezbediti povratni podatak o prijemu takvog poziva, ili obaveštenje. Ovaj zakon članom 145 razradio je i mogućnost dokazivanja fotografijama, slušanjem zvučnih i gledanjem video-snimaka, na kojima se može zasnivati i sama odluka suda.

Korak dalje, ZKP bi morao da predvidi i mogućnost saslušanja putem video-konferencijske veze, u slučajevima kada je iz objektivnih ili bezbednosnih razloga nemoguće obezbediti nesmetano saslušanje učesnika u postupku, u sedištu organa gde se saslušanje obavlja.

Kada je u pitanju implementacija najsavremenijih zakonodavnih rešenja, ono što onespokojava jeste činjenica da su u međuvremenu doneti neki veoma važni zakoni koji nisu uvažili smernice eksperata Saveta Evrope i pravne standarde ponuđene Konvencijom o visokotehnološkom kriminalu.

Jedan od takvih nesumnjivo je i već pominjani Zakon o pružanju međunarodne pravne pomoći u krivičnim stvarima, čijim su donošenjem stavljene van snage odredbe ZKP-a iz Glave XXXII, koje se tiču postupka za pružanje međunarodne pravne pomoći i izvršenje međunarodnih ugovora u krivičnopravnim stvarima. Naime, ovaj Zakon propustio je da reguliše aspekte pružanja međunarodne pravne pomoći u krivičnim stvarima iz oblasti visokotehnološkog kriminala u kojoj je, više nego u bilo kojoj drugoj, brzina[322] u postupanju od presudnog značaja za uspešno vođenje krivičnog postupka. U tom smislu, osim što je previdео postojanje mreže 24/7,[323] zakon je propustio da predvidi upotrebu modernih načina komuniciranja,[324] 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.

[322] 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.

[323] 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 trebalo bi da bude u stanju da obezbedi momentalnu pomoć u istragama i sudskim postupcima.

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

Pri postojanju samo jednog člana[325] čije odredbe regulišu postupak hitnog dostavljanja zamolnica, navedeni zakon deluje ne samo „tromo“ već i anahrono, što zaprepašćuje s obzirom na datum njegovog donošenja![326]

Iako Zakon u članu 83 nabraja „ostale oblike međunarodne pravne pomoći“,[327] u vidu:

- *izvršenja procesnih radnji* kao što su pozivanje i dostavljanje pismena, saslušanje okrivljenog, ispitivanje svedoka i veštaka, uviđaj, pretresanje prostorija i lica, *privremeno oduzimanje predmeta*;[328]
- *primene mera* kao što su nadzor i snimanje telefonskih i drugih razgovora ili komunikacija i optička snimanja lica, kontrolisana isporuka, pružanje simulovanih poslovnih usluga, sklapanje simulovanih pravnih poslova, angažovanje prikrivenog islednika, *računarsko pretraživanje i obrada podataka*;[329]
- *razmene obaveštenja i dostavljanja pismena i predmeta* koji su u vezi sa krivičnim postupkom u državi molilji;
- dostavljanja podataka bez zamolnice, korišćenja audio i video-konferencijske veze,[330] kao i formiranja zajedničkih istražnih timova, smatramo da navedene odredbe nisu dovoljno razrađene, što lako može da dovede u pitanje njihovu primenu koja bi bila od neprocenjivog značaja.

Kako smo se već „dotakli“ pitanja međunarodne pravne pomoći, poglavlja ZKP-a u kojem je dato značenje izraza u zakonu i dokaznih radnji vezanih za rasvetljavanje krivičnih dela VT kriminala, završne opservacije usmerili bismo na probleme pravilnog određivanja stvarne nadležnosti sudova i preporuke za izmenu zakona, koje bi ove probleme trebalo da reše.

---

[325] Član 6: „Zamolnica i druga pismena domaćeg pravosudnog organa dostavljaju se inostranom organu preko ministarstva nadležnog za pravosuđe. Na zahtev zamoljene države, zamolnica i druga pismena dostavljaju se diplomatskim putem. Zamolnica i pismena iz stava 1 ovog člana se pod uslovom uzajamnosti: 1. dostavljaju neposredno inostranom pravosudnom organu, 2. mogu u hitnim slučajevima dostaviti posredstvom Međunarodne organizacije kriminalističke policije (INTERPOL).“

[326] 19. mart 2009. godine.

[327] Odredbe su opšte prirode i nisu specifično osmišljene za pomoć u slučajevima visokotehnološkog kriminala.

[328] Postojeća formulacija eksplicitno ne isključuje pravnu pomoć u slučajevima VT kriminala, ali, u najmanju ruku, ostaje nejasno da li navedene odredbe podrazumevaju i zaplenu vezanu za računarske podatke ili je ona ograničena samo na materijalne predmete.

[329] Smisao odredbe jeste da omogući računarsko pretražvanje, a ne prikupljanje i presretanje računarskih podataka i komunikacije u realnom vremenu.

[330] Odredba je u tom delu apsolutno nerazrađena.

Za razliku od „novog“ ZKP-a koji je u tom delu uneo „kozmetičke promene“, u vidu člana 27 pod nazivom „Mesna nadležnost za krivična dela učinjena *u* sredstvima javnog informisanja ili *putem* globalne informativne mreže“, postojeći ZKP nije definisao mesnu nadležnost suda u situacijama kada je krivično delo izvršeno uz pomoć računara i računarskih mreža. Uz izvesno modifikovanje, sadržina odredaba kojima bi se regulisala mesna nadležnost suda u slučajevima VT kriminala mogla bi predstavljati kombinaciju odredaba člana 17 KZ-a i člana 30 ZKP-a, pri čemu bi se „dorađene“ odredbe člana 29 ZKP-a, kojima se određuje nadležnost suda za tzv. „štamparke“, odnosile na izvršenje krivičnih dela protiv časti i ugleda, krivičnog dela Izazivanje nacionalne, rasne i verske mržnje i netrpeljivosti iz člana 317 KZ-a, kao i drugih sličnih krivičnih dela koja nisu u nadležnosti Posebnog tužilaštva, a mogu biti izvršena uz pomoć računara i računarskih mreža.

Potreba zasebnog propisivanja mesne nadležnosti suda u situacijama kada je krivično delo izvršeno uz pomoć računara i računarskih mreža leži u specifičnoj prirodi samih krivičnih dela kod kojih se neretko ne može utvrditi mesto izvršenja,[331] kod kojih se skoro po pravilu razlikuju mesto izvršenja i mesto nastupanja posledice, te kod kojih se nastupanje štetne posledice, usled jedne preduzete radnje, često javlja na više različitih mesta.

S obzirom na maršrutu kriminalnog akta iz oblasti visokotehnološkog kriminala koja se u sajber 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*[332] *crime*, svojim odredbama nisu regulisali ni KZ ni ZKP. Takva situacija, gde bi više od jedne države moglo da zahteva nadležnost, može da bude 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 broju informacionih sistema na globalnom nivou.

Postojeći ZKP u stavu 2 člana 27 propisuje nadležnost u slučajevima kada je krivično delo izvršeno ili pokušano na područjima raznih sudova, ili na granici tih područja, međutim, intencija zakonodavca nije bila, niti je s obzirom na vreme donošenja ZKP-a mogla biti da navedenim članom reguliše višestruku nadležnost sudova različitih država, zbog čega je odredbe navedenog člana potrebno „doraditi“, a do tog časa sudskoj i tužilačkoj praksi ne

[331] Korišćenje nonimnih proxy servera i sl.

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

ostaje ništa drugo nego da se koristi analogijom kao jedinim mogućim rešenjem.

Da bi se poboljšao ishod sudskih postupaka i izbegla konkurencija između pravosudnih sistema i zakona različitih država, Konvencija o visokotehnološkom kriminalu u članu 22, stav 5 predviđa obavezu uključenih država da se, „kada je to celishodno", međusobno konsultuju po pitanju „najpogodnije nadležnosti za sudsko gonjenje".

Iako takva obaveza nije imperativna, čini se da aktuelne odredbe ZKP-a ne olakšavaju takvo konsultovanje, tim pre što su odredbe o pružanju međunarodne pravne pomoći izmeštene u poseban zakon koji je po našem mišljenju ostao u velikoj meri nedorečen.

2.2. Ostali zakoni

Kao što smo već napred istakli, zakonodavni okvir Republike Srbije u kojem se odvija borba protiv visokotehnološkog kriminala čine i propisi koji se striktno ne mogu podvesti pod pojam krivičnog zakonodavstva.

Predlozi izmena koji slede odnose se na Zakon o organizaciji i nadležnosti državnih organa u suzbijanju visokotehnološkog kriminala i na Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine. Ovi zakoni zaslužuju našu pažnju i analizu ne toliko zbog njihovog značaja, koliko zbog manjkavosti čije bi otklanjanje umnogome učinilo efikasnijom borbu državnih organa protiv visokotehnološkog kriminala.

2.2.1. Zakon o organizaciji i nadležnosti državnih organa u suzbijanju visokotehnološkog kriminala

Izmene ovog organizacionog zakona kojim je i uspostavljeno postojanje posebnih državnih organa u sudu, tužilaštvu i policiji za borbu protiv VT kriminala, sastojale bi se u proširivanju stvarne nadležnosti ovih organa na sva krivična dela koja po načinu, sredstvima i objektu izvršenja predstavljaju dela iz oblasti visokotehnološkog kriminala.

Naime, članom 3 Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala stvarna nadležnost je definisana taksativnim navođenjem grupe krivičnih dela iz Krivičnog zakonika Republike Srbije,[333] čime se došlo do situacije da su određena krivična dela izostala iako bi, po objektivnim kriterijumima, trebalo da budu u nadležnosti posebnog odeljenja Okružnog javnog tužilaštva u Beogradu za borbu protiv VT kriminala. Tu pre svega mislimo na zloupotrebu platnih kartica i pedofiliju na

[333] „Službeni glasnik RS", br. 85/05, 88/05, 107/05.

internetu. Naravno, ovde se ne završava spisak krivičnih dela koja bi trebalo da budu u nadležnosti Posebnog tužilaštva, već je samo reč o krivičnim delima koja su u praksi učestala a koja su, protivno logici, ostala izvan stvarne nadležnosti Posebnog tužilaštva.

S druge strane, ukoliko bi se napred predloženim izmenama u poglavlju XVII Krivičnog zakonika, pod nazivom „Krivična dela protiv bezbednosti računarskih podataka", unelo novo krivično delo „*Računarsko falsifikovanje*" sa numeracijom u vidu člana 306**,** stvorili bi se uslovi da se iz stvarne nadležnosti definisane članom 3 izostavi grupa krivičnih dela protiv pravnog saobraćaja, čiji zaštitni objekat prema intenciji zakonodavca i nije *pravni saobraćaj* elektronskih, već isključivo materijalnih dokumenata, kako je to, uostalom, regulisano i u većini drugih krivičnopravnih sistema.

2.2.2. Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine

Ovim zakonom predviđaju se konkretne mere koje su državni organi (*tržišna i druge inspekcije, poreski inspektori, poreska policija i Republička radiodifuzna agencija*) ovlašćeni da preduzmu u cilju zaštite prava intelektualne svojine priznatih zakonima i međunarodnim ugovorima.

Za razliku od ostalih zakona u ovoj oblasti koji obezbeđuju zaštitu isključivo u sudskim postupcima, što podrazumeva složenu i često sporu proceduru, ovaj zakon omogućava neposredno angažovanje administrativnih organa u hitnom postupku.

Ovaj zakon je u dobroj meri razradio pitanje odgovornosti pravnih i fizičkih lica, međutim, u slučajevima povređivanja prava intelektualne svojine od strane samostalnih trgovinskih radnji i drugih preduzetnika, zakon nije predvideo prekršajnu odgovornost ni i odgovornost zbog izvršenih privrednih prestupa, rezervišući ove vidove odgovornosti samo za pravna lica, što STR i drugi preduzetnici, svakako, nisu.

U tom delu, izmene Zakona su hitne i neophodne ne samo zbog postojanja „pravne praznine" već i zbog činjenice da se distribucija neovlašćeno umnoženih autorskih dela u praksi često vrši upravo na tezgama STR i drugih preduzetnika.

S obzirom na to da Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine kvalifikuje kao privredni prestup samo inkriminacije pravnih lica, mišljenja smo da će se nakon usklađivanja Krivičnog zakonika sa odredbama Zakona o odgovornosti pravnih lica za krivična dela pojaviti problemi u praksi prilikom izbora primene zakona, odnosno odgovarajućih pravnih normi – što ukazuje na potrebu izmene kaznenih odredaba Zakona o posebnim ovlašćenjima, koji bi kvalifikaciju izvršenog privrednog pres-

tupa rezervisao isključivo za lakše oblike inkriminacija, koje se svojim opisom ne bi podudarale sa opisom krivičnih dela propisanih Krivičnim zakonikom, za koja bi mogla odgovarati i pravna lica.

2.3. Podzakonski akti

Kada su u pitanju podzakonski akti, kao najznačajniji izdvojili bismo *Pravilnik o uslovima za pružanje internet usluga i ostalih usluga prenosa podataka i sadržaju odobrenja,* koji je nakon burne javne debate donet 23. septembra 2008. godine[334] propisujući u članu 15, stav 7 obavezu internet provajdera da o svom trošku obezbede opremu koja će omogućiti čuvanje *relevantnih podataka* u periodu od šest meseci, kao minimalnom i dve godine, kao maksimalnom, uz realnu opasnost da usled nepoštovanja ove obaveze ostane bez odobrenja za pružanje usluga.

Smatramo da navedena odredba ne pruža dovoljno pouzdan osnov nadležnim državnim organima za prikupljanje svih potrebnih dokaza u vezi sa izvršenjem krivičnih dela iz ove oblasti.

Minimalan period čuvanja podataka u trajanju od šest meseci neprimereno je kratak, a još veći problem može da predstavlja tumačenje odredaba od strane internet provajdera, prvenstveno u pogledu prirode podataka koje je potrebno čuvati, imajući u vidu nepreciznu formulaciju – „relevantni podaci". To u praksi znači da državni organi ne mogu sa sigurnošću očekivati da će u postupanju u okviru konkretnog krivičnog predmeta moći da pribave sve neophodne dokaze, s obzirom da to umnogome zavisi od poimanja pojma *relevantan podatak* od strane svakog pojedinačnog internet provajdera.

Nedoumica bi svakako bila otklonjena da je u članu 2 Pravilnika dato značenje navedenog pojma, što nije učinjeno.

U praksi nekih evropskih zemalja koje mnogo više pažnje posvećuju preciznosti u regulisanju ovih pitanja, obaveza internet provajdera je uspostavljena imperativnim odredbama[335] ili komercijalizacijom[336] ove obaveze, ali u

[334] Pravilnik je donet od strane Upravnog odbora Republičke agencije za telekomunikacije.

[335] U Norveškoj ne samo što je propisana obaveza internet provajdera u pogledu dostavljanja svih potrebnih podataka državnim organima već je, imajući u vidu da je prema norveškom zakonodavstvu kažnjiv i sam pristup internet sajtovima sa sadržajem dečje pornografije, obaveza internet provajdera da izrade filtere koji sprečavaju korisnike da pristupe ovakvim internet sajtovima i da ih konstantno dopunjuju novim adresama.

[336] U Francuskoj u cilju olakšanja ove obaveze internet provajdera i smanjenja troškova postoji cenovnik prema kome, npr. dostavljanje podataka u vezi sa jednom IP adresom košta osam evra.

bilo kojoj varijanti pruža sigurnost nadležnim organima u pogledu mogućnosti prikupljanja potrebnih dokaza.

Ovakva zakonodavna rešenja evropskih zemalja nameću potrebu preispitivanja donetih rešenja u smislu izmeštanja pravne regulative iz podzakonskih u zakonske akte i sankcionisanja navedene dispozicije krivičnim, a ne administrativnim merama u upravnom postupku.

U skladu sa tim, izmene materijalnog zakona morale bi da prate i izmene procesnog, na način o kojem je prethodno bilo reči.

* * *

Na kraju svake diskusije o legislativi na polju borbe protiv visokotehnološkog kriminala uvek ostaje isto pitanje: šta činiti dalje? Na osnovu izloženog, jasno je da se značajni napori preduzimaju kako na međunarodnom, tako i na nacionalnom nivou, kako bi se ustanovili zakonodavni okviri za efikasnu borbu protiv sajber kriminala: okviri koji bi bili dovoljno fleksibilni da budu primenjivi u svim pravnim sistemima i dovoljno efikasni da proizvedu rezultate u vidu povećane sigurnosti u sajber prostoru. Ako je ikada pitanje međunarodne saradnje na praktičnom, a ne teorijskom, nivou igralo važnu ulogu u razvoju pojedinih oblasti prava, onda je visokotehnološki kriminal jedna od tih oblasti.

Na osnovu dosadašnjih iskustava, jasno je da razvoj računarskih tehnologija nameće potrebu konstantnog revidiranja postojećih rešenja i njihovo usklađivanje sa realnošću koja se menja iz dana u dan. Pravo mora da se prilagođava aktuelnom trenutku, inače će rešenja i mehanizmi koji su danas efikasni za nekoliko meseci biti zastareli i prevaziđeni. Zbog toga, kada odgovaramo na pitanje šta dalje, u stvari, govorimo o različitim pravcima delovanja koji bi, uzimajući u obzir postignuti nivo saradnje i kvalitet legislativnih rešenja, omogućili viši stepen sigurnosti u sajber prostoru i efikasniju zaštitu od opasnosti koje iz njega dolaze, kako za pojedinca i pravna lica, tako i za međunarodnu bezbednost.

O kojim pravcima delovanja je konkretno reč? Verovatno bi se mogla postići apsolutna saglasnost barem o sledećim:

- *dalje usklađivanje materijalnog krivičnog zakonodavstva*, oslanjajući se prvenstveno na rešenja predviđena Konvencijom Saveta Evrope o visokotehnološkom kriminalu;
- *dalje usklađivanje procesnog prava, naročito u oblasti istrage i krivičnog progona,* gde bi se takođe mogli poslužiti rešenjima predviđenim Konvencijom Saveta Evrope, naročito u oblasti dostupnosti elektronskih podataka koje poseduju internet provajderi a koji mogu da služe kao dokaz u sudskom postupku;

– *sprečavanje zloupotrebe interneta za vršenje terorističkih akata* kroz ratifikaciju i primenu odredaba Konvencije Saveta Evrope o sprečavanju terorizma i Konvencije o visokotehnološkom kriminalu. One države koje ne ratifikuju Konvenciju trebalo bi da se njenim sadržajem posluže kao osnovom za pravno regulisanje ove materije u svojim nacionalnim zakonodavstvima;
– *saradnja na globalnom nivou i razmena informacija,* a u ove aktivnosti trebalo bi da budu uključene najznačajnije međunarodne, regionalne i specijalizovane organizacije kao što su: Međunarodna telekomunikaciona unija, Interpol, Grupa država G-8, Savet Evrope, Organizacija američkih država (OAS), Arapska liga, Afrička unija, Evropska unija, NATO, OEBS itd;
– *mere za zaštitu privatnosti i ljudskih prava*: prilikom sprovođenja istrage i krivičnog gonjenja visokotehnološkog kriminala mora da se očuva balans između prava države da krivično goni izvršioce i prava pojedinaca na privatnost i drugih ljudskih prava garantovanih zakonima i međunarodnim dokumentima;
– *mere građanskopravne i upravnopravne prirode*: koje bi obuhvatile pravo na naknadu štete i druge naknade oštećenim licima, kao i efikasnu kontrolu subjekata koji obavljaju delatnosti u vezi sa primenom visokih tehnologija, mrežne infrastrukture, digitalne opreme i softvera.

U svetlu navedenog treba posmatrati i ulogu Srbije u borbi protiv visokotehnološkog kriminala i njenu obavezu da postignuti nivo legislative unapredi u skladu sa dostignutim međunarodnim standardima. Prvi korak mogao bi da bude inkorporacija odredaba nedavno ratifikovane Konvencije Saveta Evrope o visokotehnološkom kriminalu u nacionalno zakonodavstvo.

SADRŽAJ

UDRUŽENJE JAVNIH TUŽILACA I
ZAMENIKA JAVNIH TUŽILACA SRBIJE

www.aecid.es