SUZBIJANJE VISOKOTEHNOLOŠKOG KRIMINALITETA: MEĐUNARODNI STANDARDI I NACIONALNO ZAKONODAVSTVO SRBIJE*

Dr Sanja Ćopić
Institut za kriminološka i sociološka istraživanja, Beograd

Mr Slobodan Ćopić
MUP RS, Uprava granične policije, Beograd

Digitalizacija, brz razvoj kompjuterske industrije i sve šira upotreba informacionih i telekomunikacionih sistema rezultirali su pojavom novih vidova kriminaliteta i načina za vršenje tradicionalnih krivičnih dela, koji, ukupno gledano, čine tzv. visokotehnološki, odnosno kompjuterski ili sajber (cyber) kriminalitet. Visokotehnološki kriminalitet zaokuplja sve veću pažnju naučne i stručne javnosti, ali i međunarodnih organizacija i državnih institucija. Ovo posebno iz razloga što ga karakteriše visoka tamna brojka, jer je usled korišćenja sve sofisticiranije tehnologije njegovo otkrivanje i dokazivanje otežano, dok je, s druge strane, šteta koja se nanosi kako pojedincima, tako i pravnim licima i državama sve veća. Prvi korak u suzbijanju visokotehnološkog kriminaliteta predstavlja uspostavljanje odgovarajućeg pravnog i institucionalnog okvira. Polazeći od toga, u prvom delu rada analizira se Konvencija Saveta Evrope o visokotehnološkom kriminalu, kako bi se ukazalo na ključne standarde i principe u pogledu normiranja ove materije. U drugom delu rada analizirano je pozitivno zakonodavstvo Republike Srbije relevantno za krivičnopravnu zaštitu, kako bi se uočilo u kojoj meri su postojeća rešenja usklađena sa zahtevima koje postavlja ova Konvencija, te u kom pravcu bi trebalo dalje razvijati pravni i institucionalni okvir kako bi suprotstavljanje visokotehnološkom kriminalitetu bilo efikasnije.

KLJUČNE REČI: visokotehnološki kriminaliteta / međunarodni standardi / krivičnopravna zaštita / Srbija

* Rad je nastao kao rezultat na projektu broj 47011 koji finansira Ministarstvo prosvete, nauke i tehnološkog razvoja RS

UVOD

Razvoj modernih tehnologija i upotreba računara, a posebno Interneta, značajno su doprineli novim vidovima komunikacije, povezivanju, umrežavanju i razmeni podataka i informacija. Kako primećuju pojedini autori, Internet, kao globalni računarski sistem, "danas predstavlja medij preko koga se realizuju servisi elektronskog poslovanja (e-business) i elektronske vlade (e-government)" (Lepojević i Kovačević-Lepojević, 2007: 266). Informacione i komunikacione tehnologije su, kako se navodi u *Strategiji razvoja informacionog društva u Republici Srbiji do 2020. godine*, "tokom samo jedne ljudske generacije revolucionarno promenile način života, učenja, rada i zabave," postepeno transformišući "način interakcije ljudi, preduzeća i javnih institucija".[1] Međutim, pored brojnih prednosti, razvoj kompjuterske industrije i sve šira upotreba informaciono-komunikacionih tehnologija rezultirali su i pojavom novih vidova kriminaliteta i načina za vršenje tradicionalnih krivičnih dela, koji, ukupno gledano, čine tzv. visokotehnološki, odnosno kompjuterski ili sajber (*cyber*) kriminalitet. Drugim rečima, "računari i informaciona tehnologija su postali ili sredstvo za lakše i efikasnije izvršenje određenih krivičnih dela, ili su sami postali objekt napada" (Stojanović, 2006: 662). Utoliko se visokotehnološki kriminalitet može posmatrati u užem i širem smislu. U užem smislu, visokotehnološki kriminalitet predstavlja vid kriminalnog ponašanja kod koga se kompjuter javlja kao sredstvo ili cilj izvršenja krivičnog dela, dok u širem smislu on obuhvata i krivična dela kod kojih korišćenje kompjuterske tehnologije i informacionih sistema predstavlja način izvršenja (tradicionalnih) krivičnih dela. Visokotehnološki kriminalitet ima niz pojavnih oblika, koji se s napretkom tehnologije permanentno menjaju i inoviraju (Konstantinović-Vilić, Nikolić-Ristanović i Kostić, 2009: 182-183; Urošević, Uljanov i Vuković, 2012).

Jedno istraživanje je pokazalo da je oko 65% korisnika Interneta bilo žrtva nekog vida visokotehnološkog kriminaliteta, uključujući ubacivanje virusa, prevare putem Interneta, neovlašćeno upadanje na profile na društvenim mrežama, prevare u vezi sa kreditnim karticama, seksualno uznemiravanje i slično.[2] Međutim, sve sofisticiranija tehnologija koju primenjuju učinioci značajno otežava otkrivanje i dokazivanje ovog oblika kriminaliteta, što rezultira visokom tamnom brojkom. Sajber prostor osigurava visok nivo anonimnosti, što umanjuje rizik od otkrivanja. Uz to, u vršenju krivičnih dela koja spadaju u visokotehnološki kriminalitet neretko postoje i elementi organizovanog i prekograničnog kriminaliteta, dok žrtve često nisu ni svesne svoje viktimizacije pa je ni ne prijavljuju (Urošević, Uljanov i Vuković, 2012). S

[1] Strategija razvoja informacionog društva u republici Srbiji do 2020. godine, Službeni glasnik RS, br. 101/2007 i 65/2008. Tekst Strategije dostupan na http://www.digitalnaagenda.gov.rs/FileSystem/SiteDocuments/strategije/Strategija_razvoja_informacionog_drustva_2020.pdf, pristupljeno 15. aprila 2013. godine.

[2] Podaci dostupni na interent stranici UNICRI (United Nations Interregional Crime and Justice Research Institute), http://www.unicri.it/special_topics/cyber_threats/cyber_crime/, pristupljeno 19. aprila 2013. godine.

druge strane, pak, šteta koja nastaje usled krivičnih dela koja spadaju u visokotehnološki kriminalitet je ogromna, kako za pojedince, tako i za pravna lica i države. Procenjuje se da šteta od ovog vida kriminaliteta na godišnjem nivou iznosi oko 100 milijardi američkih dolara.[3] Iako se o pojavi kompjuterskog kriminaliteta može govoriti već od sedamdesetih godina XX veka, ovo su samo neki od razloga zbog kojih je pitanje visokotehnološkog kriminliteta posebno aktuelizovalo tokom osamdesetih i naročito devedesetih godina prošlog veka, zaokupljajući pažnju naučne i stručne javnosti, ali i državnih institucija i međunarodnih organizacija.

Prvi korak u suprotstavljanju visokotehnološkom kriminalitetu predstavlja uspostavljanje odgovarajućeg pravnog i institucionalnog okvira za njegovo suzbijanje. Polazeći od toga, cilj ovog rada je da se ukaže na ključne međunarodne standarde u pogledu normiranja ove materije, posebno one koje predviđa Konvencija Saveta Evrope o visokotehnološkom kriminalu, kao i da se sagleda u kojoj meri je pozitivno zakonodavstvo Republike Srbije, posebno u domenu krivičnopravne zaštite, usklađeno sa njima, te u kom pravcu bi trebalo dalje razvijati zakonodavni i institucionalni okvir kako bi suprotstavljanje visokotehnološkom kriminalitetu bilo efikasnije. Imajući to u vidu, u fokusu rada biće odredbe onih zakona koji su od značaja za inkriminisanje, otrkivanje i dokazivanje ponašanja koja spadaju u visokotehnološki kriminalitet, i to: Krivični zakonik[4], Zakonik o krivičnom postupku[5] i Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala[6].

KONVENCIJA SAVETA EVROPE O VISOKOTEHNOLOŠKOM KRIMINALU: POSTAVLJANJE OKVIRA ZA SUZBIJANJE VISOKOTEHNOLOŠKOG KRIMINALITETA

Konvencija Saveta Evrope o visokotehnološkom kriminalu,[7] doneta 2001. godine,[8] predstavlja prvi međunarodni ugovor o krivičnim delima izvršenim putem Interneta ili drugih računarskih mreža. Konvencija na prilično obuhvatan i celovit način postavlja osnov za inkriminisanje ponašanja koja spadaju u visokotehnološki kriminalitet i stvaranje normativnog okvira za uvođenje dodatnih ovlašćenja i procedura u cilju njegovog efikasnijeg otkrivanja i procesuiranja. U ovom dokumentu definišu se dve osnovne grupe

[3] Ibidem.
[4] Službeni glasnik RS, br. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009 i 121/2012.
[5] Službeni glasnik RS, br. 72/2011, 101/2011, 121/2012 i 32/2013.
[6] Službeni glasnik RS, br. 61/2005, 104/2009.
[7] Konvencija o visokotehnološkom kriminalu usvojena je od strane Komiteta ministara Saveta Evrope na 109. sednici održanoj 8. novembra 2001. godine, a Konvencija je otvorena za potpisivanje u Budimpešti 23. novembra 2001. godine. Tekst Konvencije i prateći izveštaj dostupni su na internet stranici Saveta Evrope http://conventions.coe.int/Treaty/EN/Treaties/Html/185., pristupljeno 15. marta 2013. godine.
[8] Ova Koncencija je 2003. godine dopunjena usvajanjem Dodatnog protokola koji se odnosi na kažnjavanje akata rasizma i ksenofobije učinjenih putem kompjuterskih sistema.

mera: mere koje države potpisnice treba da preduzmu na nacionalnom nivou i mere, odnosno načela vezana za međunarodnu saradnju, koja se posebno apostrofira u preambuli ovog dokumenta. Usvajanje i primena ovih mera trebalo bi da olakšaju otkrivanje, dokazivanje i gonjenje za krivična dela koja čine visokotehnološki kriminalitet, kao i stvaranje uslova za efikasnu i pouzdanu saradnju na međunarodnom niovu. Shodno odredbama Konvencije, države potpisnice bi na nacionalnom nivou trebalo da preduzmu mere usmerene na razvoj i unapređenje krivičnog zakonodavstva, kako materijalnog tako i procesnog, kao i na stvaranje odgovarajućeg institucionalnog okvira za primenu postojećih rešenja i postupanje u praksi.

Prvi korak u stvaranju okvira za krivičnopravnu zaštitu predstavlja inkriminisanje ponašanja koja spadaju u domen visokotehnološkog kriminaliteta. U tom smislu, Konvencija postavlja obavezu državama potpisnicama da, u skladu sa svojim pravnim sistemom i tradicijom, kao krivična dela predvide ponašanja koja mogu da se svrstaju u četiti grupe: dela protiv poverljivosti, celovitosti i dostupnosti računarskih podataka i sistema; dela u vezi sa računarima; dela u vezi sa sadržajem, i dela u vezi sa kršenjem autorskih i srodnih prava. U prvu grupu dela spadali bi: nezakonit pristup računarskom sistemu ili jednom njegovom delu; nezakonito presretanje podataka, odnosno protivpravni prenos računarskih podataka koji nisu javne prirode, ka računarskom sistemu, od njega ili unutar samog sistema, uključujući i elektromagnetna emitovanja iz računarskog sistema kojim se prenose takvi podaci; potom, ometanje podataka, odnosno protivpravno oštećenje, brisanje, pogoršanje, menjanje ili prikrivanje računarskih podataka; ometanje sistema, i to unošenjem, prenošenjem, oštećenjem, brisanjem, pogoršanjem, menjanjem ili prikrivanjem računarskih podataka, i zloupotreba uređaja. Grupa dela u vezi sa računarima trebalo bi da obuhvati dela poput falsifikovanja i prevara u vezi sa računarima, dok bi u dela u vezi sa sadržajem spadala dela u vezi sa dečijom pornografijom.

U Konvenciji se insistira na tome da države potpisnice obezbede pravni osnov za kažnjavanje pokušaja, kao i pomaganja i podstrekavanja na vršenje ovih krivičnih dela, što govori o njihovoj društvenoj opasnosti i težini. Uz to, članom 12 Konvencije predviđena je odgovornost pravnih lica. Drugim rečima, države potpisnice bi trebalo da usvoje zakonodavne i druge mere kako bi se ozbezbedilo da se i pravna lica smatraju odgovornim za ova krivična dela a koja u njihovu korist izvrše fizička lica, delujući bilo kao pojedinci ili kao članovi organa tog pravnog lica, ako se nalaze na nekoj rukovodećoj poziciji. Pri tome, zavisno od pravnog sistema, ova odgovornost može da bude krivična, građanska ili administrativna, ali ona svakako ne isključuje krivičnu ogovornost fizičkog lica koje je preduzelo radnju izvršenja ili na drugi način učestvovalo u izvršenju krivičnog dela. Najzad, Konvencija predviđa da države potpisnice treba da predvide odgovarajuće i srazmerne sankcije, koje treba da deluju odvraćajuće, dakle, u pravcu generalne prevencije.

Drugi deo Konvencije postavlja osnov za razvoj procesnog zakonodavstva u smislu predviđanja ovlašćenja i postupaka usmerenih na otkrivanje ovih dela i vođenje krivičnih postupaka. Tako se države potpisnice ohrabruju da predvide hitne mere zaštite računarskih podataka i to onda kada postoji opasnost da oni budu izgubljeni ili izmenjeni, što može da oteža ili onemogući dalje postupanje u konkrenom slučaju; potom, da regulišu izdavanje naredbe o predaji računarskih podataka, kao i pretraživanje i zaplenu sačuvanih računarskih podataka, prikupljanje podataka o saobraćaju u realnom vremenu i presretanje podataka. Sve ove mere usmerene su na obezbeđivanje dovoljno dokaza za pokretanje i vođenje postupka, što je posebno bitno ako se ima na umu činjenica da se radi o kriminalitetu sa veoma visokom tamnom brojkom.

U trećem delu Konvencije ukazuje se na to da svaka država potpisnica treba da reguliše pitanje nadležnosti za postupanje u slučaju krivičnih dela predviđenih ovim dokumentom kada su ona izvršena na njenoj teritoriji i od strane njenih državljana.

Poseban deo Konvencije posvećen je međunarodnoj saradnji, bez koje teško da može da se zamisli efikasno suzbijanje ovog vida kriminaliteta. Ako se ima na umu činjenica da se visokotehnološki kriminalitet dešava u virtuelnom, tzv. sajber (*cyber*) prostoru, koji ne poznaje granice, onda načelo teritorijalne nadležnosti može da predstavlja prepreku za efikasno otkrivanje i procesuiranje slučajeva visokotehnološkog kriminaliteta. Stoga se u Konvenciji posebno ukazuje na potrebu regulisanja ekstradicije, pružanja uzajamne pomoći i prosleđivanja tzv. slučajnih informacija.

U Konvenciji je zauzet stav da krivična dela koja su ovim instrumentom predviđena podležu ekstradiciji. U tom smislu, apostrofira se da države potpisnice prilikom potpisivanja ugovora o ekstradiciji obavezno treba da uključe dela iz ove Konvencije u grupu krivičnih dela koja podležu ekstradiciji. Takođe, predviđena je i uzajamna pomoć država, i to u najširem mogućem obimu u istragama ili postupcima koji se odnose na krivična dela u vezi sa računarskim sistemima i podacima, ili prikupljanju dokaza u elektronskom obliku o izvršenom krivičnom delu. S obzirom na značaj saradnje među državama, Konvencija sadrži posebne odredbe koje se odnose na postupke u slučaju uzajamne pomoći. Najzad, u članu 26 navodi se da "strana ugovornica može, u granicama domaćeg prava i bez prethodnog zahteva, da drugoj strani ugovornici prosledi informacije do kojih je došla u okviru sopstvenih istraga". Cilj takvog postupanja je pomoć drugoj državi u pokretanju ili vođenju istraga ili postupaka ili, pak, postavljanje osnova za uzajamnu saradnju. Vezano za međunarodnu saradnju, posebno značajnom čini se odredba o mreži 24/7, shodno kojoj svaka država ugovornica treba da odredi mesto za kontakt koje je dostupno 24 časa dnevno, sedam dana u nedelji, a u cilju pružanja pomoći u istragama i postupcima, odnosno prilikom prikupljanja potrebnih dokaza u elektronskom obliku o izvršenom krivičnom delu.

KRIVIČNOPRAVNA ZAŠTITA OD VISOKOTEHNOLOŠKOG KRIMINALITETA U SRBIJI

Iako je Konvencija o visokotehnološkom kriminalu potpisana 2005. godine, Zakon o potvrđivanju Konvencije[9] usvojen je tek 2009. godine, čime se Srbija obavezala na preduzimanje niza mera i aktivnosti na planu sprečavanja i otkrivanja visokotehnološkog kriminaliteta. Pa ipak, može se primetiti da su koraci ka uspostavljanju pravnog okvira za suzbijanje ovog vida kriminaliteta preduzeti znatno ranije. Naime, krivična dela protiv bezbednosti računarskih podataka uvedena su u krivično zakonodavstvo Srbije već 2003. godine (Stojanović, 2006: 663), da bi bila unapređena sa usvajanjem Krivičnog zakonika 2005. godine. Iste godine (2005) usvojen je i Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, koji je postavio osnov za razvoj institucionalnog okvira za suzbijanje visokotehnološkog kriminaliteta. U godinama koje su usledile, inovirano je i krivičnoprocesno zakonodavstvo kroz predviđanje niza rešenja usmerenih na postavljanje boljeg osnova za otkrivanje i dokazivanje krivičnih dela, posebno iz nekih grupa, uključujući i dela koja spadaju u visokotehnološki kriminalitet.

Materijalno krivično pravo

Polazeći od odredaba Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, visokotehnološki kriminalitet definiše se kao skup krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi produkti u materijalnom i elektronskom obliku. Stoga se krivičnopravna zaštita postiže na dva načina: kroz predviđanje posebne grupe krivičnih dela protiv bezbednosti računarskih podataka i kroz predviđanje niza drugih krivičnih dela kod kojih se računari i računarske mreže pojavljuju kao sredstvo izvršenja dela. Pod određenim uslovima, u ovu drugu grupu spadaju krivična dela protiv intelektualne svojine, imovine i pravnog saobraćaja, kao i krivična dela protiv slobode i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti RS. S obzirom da su dela koja spadaju u ovu grupu brojna, na ovom mestu nećemo ulaziti u njihovu analizu, već ćemo pažnju usmeriti na dela predviđena u glavi XXVII Krivičnog zakonika RS, dakle, na krivična dela protiv bezbednosti računarskih podataka.

Krivičnim delima protiv bezbednosti računarskih podataka štiti se "korišćenje informacione tehnologije u dozvoljene svrhe, odnosno pruža se zaštita samom funkcionisanju informacione tehnologije" (Stojanović, 2006: 662-663). U ovu grupu krivičnih dela spadaju: oštećenje računarskih podataka i programa (član 298), računarska sabotaža (član 299), pravljenje i unošenje računarskih virusa (član 300), računarska prevara (član 301), neovlašćeni pristup zaštićenom

[9] Službeni glasnik RS br.19/2009.

računaru, računarskoj mreži i elektronskoj obradi podataka (član 302), sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 303), neovlašćeno korišćenje računara ili računarske mreže (član 304) i pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka (član 304a). Ovim krivičnim delima inkriminišu se gotovo sva ponašanja na koja ukazuje Konvencija o visokotehnološkom kriminalu, a koja spadaju u grupu dela protiv poverljivosti, celovitosti i dostupnosti računarskih podataka i sistema i dela u vezi sa računarima. Ono što se uočava je da još uvek nije na odgovarajući način inkriminisano neovlašćeno presretanje podataka. Bez obzira na to, može se zaključiti da je zakonodavstvo Srbije u pogledu kriminalizacije ponašanja koja spadaju u domen visokotehnološkog kriminaliteta u značajnoj meri usklađeno sa obavezama koje proističu iz Konvencije o visokotehnološkom kriminalu.

Sva krivična dela protiv bezbednosti računarskih podataka, sem jednog – neovlašćeno korišćenje računara ili računarske mreže, za koje se goni po privatnoj tužbi – gone se po službenoj dužnosti, što govori o njihovoj društvenoj opasnosti. U slučaju dva krivična dela – neovlašćeno korišćenje računara ili računarske mreže i računarska prevara, kao element bića krivičnog dela predviđeno je pribavljanje, odnosno namera pribavljanja protivpravne imovinske koristi, što ovim delima daje lukrativni karakter. Kažnjavanje za pokušaj, kao i za pomaganje i podstrekavanje ostvaruje se primenom opštih krivičnopravih normi. Odgovornost pravnih lica regulisana je posebnim zakonom – Zakonom o odgovornosti pravnih lica za krivična dela[10], pa se i u tom smislu može reći da je materijalno krivično zakonodavstvo usklađeno sa odredbama Konvencije o visokotehnološkom kriminalu.

Kada je u pitanju krivičnopravna zaštita, zanimljivo je pogledati i podatke o broju procesuiranih slučajeva visokotehnološkog kriminaliteta posmatranog u užem smislu, kako bi se, makar delimično, sagledala primena postojećih rešenja u praksi. Podaci Republičkog zavoda za statistiku (Republički zavod za statistiku, 2012) pokazuju da je još uvek mali broj podnetih krivičnih prijava, a posebno optuženja i osuda za krivična dela iz grupe krivičnih dela protiv bezbednosti računarskih podataka (Tabela 1).

Tabela 1: Broj podnetih krivičnih prijava, optuženja i osuda prema godinama za krivična dela protiv bezbednosti računarskih podataka

	2006.	2007.	2008.	2009.	2010.	2011.
Krivične prijave	23	8	25	45	20	22
Optuženja	6	3	10	6	4	10
Osude	5	2	5	4	4	7

U 2011. godini, od 22 krivične prijave, u 7 slučajeva prijava je podneta zbog krivičnog dela računarske prevare, u 6 slučajeva zbog neovlašćenog pristupa

[10] Službeni glasnik RS, br. 97/2008.

zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka, u pet slučajeva zbog računarske sabotaže, u tri zbog oštećenja računarskih podataka i programa i u jednom slučaju zbog pravljenja, nabavljanja i davanja drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka. U samo dva slučaja krivičnu prijavu su podneli građani; u 16 slučajeva je to uradila policija, u jednom oštećeno pravno lice, a u tri slučaja ostali. To govori o potrebi podizanja svesti javnosti o ovoj vrsti kriminaliteta kako bi i sami građani mogli da prepoznaju sopstvenu viktimizaciju i prijave je nadležnim organima.

U svega 10 slučajeva je tokom 2011. godine došlo do optuženja, dok je 7 lica proglašeno krivim i izrečene su im sankcije. Pri tome, u dva slučaja je izrečena kazna zatvora i to u trajanju od dve do tri godine, odnosno od tri do šest meseci, u dva slučaja je izrečena novčana kazna, a u tri uslovna osuda. S obzirom na još uvek relativno mali broj procesuiranih slučajeva, teško je izvlačiti neke opštije zaključke. Uz to, kako primećuju pojedini autori, statistički podaci nisu dovoljno precizni pokazatelji pojavnih oblika i stvarnog obima ovog vida kriminaliteta (Urošević, Uljanov i Vuković, 2012), pa ova oblast zahteva i dodatna istraživanja kako bi se došlo do preciznijih podataka o njegovoj rasprostranjenosti.

Krivičnoprocesno zakonodavstvo

Za otkrivanje i dokazivanje krivičnih dela koja spadaju u domen visokotehnološkog kriminaliteta relevantne su odredbe Zakonika o krivičnom postupku (u daljem tekstu ZKP), i to kako opšte,[11] tako i one čija je primena dozvoljena samo u slučaju određenih krivičnih dela i pod određenim uslovima. Polazeći od odredbi Konvencije o visokotehnološkom kriminalu u delu koji se tiče procesnog zakonodavstva, čini se da su upravo odredbe ZKP koje se odnose na posebne dokazne radnje od naročitog značaja za suzbijanje visokotehnološkog kriminaliteta.

Kako je navedeno u članu 161 ZKP, primena posebnih dokaznih radnji dozvoljena je u slučaju kada postoje osnovi sumnje da je lice učinilo neko od zakonom predviđenih krivičnih dela, i to onda kada dokazi za krivično gonjenje ne mogu da se prikupe na drugi način ili bi njihovo prikupljanje bilo znatno otežano. Pri tome, zakonodavac je ograničio primenu posebnih dokaznih radnji na dva načina, odnosno na dve grupe krivičnih dela: prvu grupu, koja je određena na jedan opšti način, čine sva krivična dela za koja

[11] Tu se misli na dokazne radnje koje se preduzimaju u slučaju bilo kog krivičnog dela, uz određene specifičnosti kada se radi o njihovom preduzimanju u slučaju dela koja spadaju u visokotehnološki kriminaliteta. Na primer, privremeno oduzimanje predmeta, pod kojim se podrazumevaju i uređaji za automatsku obradu podataka i uređaji i opema na kojoj se čuvaju ili se mogu čuvati elektronski zapisi, ili pretresanje, koje u slučaju dela iz domena visokotehnološkog kriminaliteta podrazumeva pretresanje uređaja za automatsku obradu podataka i opreme na kojoj se čuvaju ili se mogu čuvati elektronski zapisi, a koje se može preduzeti samo na osnovu naredbe suda.

je posebnim zakonom određeno da postupa javno tužilaštvo posebne nadležnosti, što uključuje dela koja spadaju u domen visokotehnološkog kriminaliteta, i drugu grupu u kojoj su taksativno pobrojana krivična dela u odnosu na koja mogu da se odrede posebne dokazne radnje.

Zakonodavac je predvideo sledeće posebne dokazne radnje: tajni nadzor komunikacije, tajno praćenje i snimanje, simulovani poslovi, računarsko pretraživanje podataka, kontrolisana isporuka i prikriveni islednik. U pogledu primene posebnih dokaznih radnji zakonodavac je postavio i neka ograničenja. Tako je angažovanje prikrivenog islednika, kao posebna dokazna radnja, dozvoljeno samo za krivična dela za koja je posebnim zakonom određeno da postupa javno tužilaštvo posebne nadležnosti, pa se može zaključiti da je primena moguća u slučaju krivičnih dela koja spadaju u visokotehnološki kriminalitet.

S druge strane, pak, u članu 162 stav 3 ZKP navedeno je da kada su ispunjeni opšti uslovi za primenu posebnih dokaznih radnji, dokazna radnja koja se sastoji u tajnom nadzoru komunikacije može da se primeni i u slučaju taksativno navedenih krivičnih dela iz grupe krivičnih dela protiv bezbednosti računarskih podataka i to: oštećenje računarskih podataka i programa, računarska sabotaža, računarska prevara i neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka. Međutim, ono što ostaje nejasno je odnos ovog rešenja i odredbe o tome da se posebne dokazne radnje mogu primeniti u slučaju krivičnih dela za koja je uspostavljena nadležnost posebnog tužilaštva, što je predviđeno u istom članu, dakle, članu 162 stav 1 tačka 1. Stiče se utisak da su ove dve odredbe u koliziji. Naime, ako je generalno dozvoljena primena svih posebnih dokaznih radnji u slučaju svih krivičnih dela za koja se uspostavlja nadležnost posebnog tužilaštva, a to je u ovom slučaju posebno tužilaštvo za visokotehnološki kriminal, što uključuje i sva dela iz grupe krivičnih dela protiv bezbednosti računarskih podataka, i to kada su ispunjeni opšti uslovi za preduzimanje posebnih istražnih radnji, onda nije jasno zašto se posebno ističe mogućnost primene radnje koja se sastoji u tajnom nadzoru komunikacije u slučaju samo nekih dela iz glave XXVII KZ RS. Ovo rešenje upućuje na zaključak da pravne norme u ovom segmentu još uvek nisu dovoljno usklađene, kako na nivou jednog zakonskog teksta, tako ni među zakonima. To može da rezultira pravnom nesigurnošću i zloupotrebama, što mogu da budu prepreke za primenu rešenja koja mogu da obezbede efikasno dokazivanje ovih krivičnih dela. Međutim, kako se radi o nedavno unetim izmenama, a ovaj ZKP tek počinje sa primenom, ostaje da se vidi na koji način će se ova rešenja primenjivati u praksi i da li će se i na kakve probleme i izazove nailaziti.

INSTITUCIONALNI OKVIR ZA SUZBIJANJE VISOKOTEHNOLOŠKOG KRIMINALITETA U SRBIJI

Donošenjem Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala 2005. godine postavljen je pravni osnov za uspostavljanje institucionalnog okvira za suzbijanje ovog vida kriminaliteta. Kako je navedeno u članu 1 ovog zakona, njime se uređuje "obrazovanje, organizacija, nadležnost i ovlašćenja posebnih organizacionih jedinica državnih organa radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela" koja čine visokotehnološki kriminalitet. Posebne organizacione jedinice formirane su na niovu organa unutrašnjih poslova, tužilaštva i suda. Njihovo formiranje praktično znači primenu principa stvarne a ne mesne nadležnosti za otkrivnje i gonjenje učinilaca krivičnih dela koja spadaju u domen visokotehnološkog kriminaliteta, čime se postiže bolja specijalizacija ovih organa i osigurava efikasnije postupanje. Posebne organizacione jedinice nadležne su za postupanje u slučaju krivičnih dela koja spadaju u visokotehnološki kriminalitet, onosno za postupanje u slučaju krivičnih dela protiv bezbednosti računarskih podataka, krivičnih 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 i elektronskom obliku, kao i krivična dela protiv slobode i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti RS i to u slučaju kada se računari i računarske mreže javljaju kao sredstvo izvršenja. Na taj način, nadležnost posebnih organizacionih jedinica je sasvim opravdano proširena na brojna krivična dela koja mogu da budu izvršena upotrebom računara i računarskih mreža, što se može oceniti kao pozitivan korak u pravcu harmonizacije domaće legislative sa Konvencijom o visokotehnološkom kriminalu.

Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala predviđeno je da se u okviru ministarstva nadležnog za unutrašnje poslove formira služba za borbu protiv visokotehnološkog kriminala, koja postupa po zahtevima posebnog tužioca za visokotehnološki kriminal. Ova služba je formirana 2007. godine i to kao Odeljenje za borbu protiv visokotehnološkog kriminala u okviru Službe za borbu protiv organizovanog kriminala u Upravi kriminalističke policije.[12] Odeljenje za borbu protiv visokotehnološkog kriminala u svom sastavu ima dva odseka: Odsek za suzbijanje elektronskog kriminaliteta i Odsek za suzbijanje kriminaliteta u oblasti intelektualne svojine (Urošević, Uljanov i Vuković, 2012).

Kada je u pitanju krivično gonjenje za dela visokotehnološkog kriminaliteta, u okviru Višeg javnog tužilaštva u Beogradu formirano je posebno odeljenje

[12] Više o tome videti na interent stranici Ministarstva unutrašnjih poslova http://www.mup.gov.rs/cms_cir/UKP.nsf/sbpok.h#link07.html, pristupljeno 22. aprila 2013. godine.

za borbu protiv visokotehnološkog kriminala (tzv. posebno tužilaštvo). Radom ovog odeljenja rukovodi posebni tužilac za visokotehnološki kriminal, koga postavlja Republički javni tužilac, a koji poseduje posebna znanja iz oblasti informatičkih tehnologija.

Najzad, za suđenje u slučaju krivičnih dela koja spadaju u domen visokotehnološkog kriminaliteta nadležan je Viši sud u Beogradu, u okviru koga je obrazovano Odeljenje za borbu protiv visokotehnološkog kriminala. Kao i u slučaju posebnog tužilaštva, prilikom raspoređivanja sudija u ovo odeljenje prednost se daje onima koji poseduju posebna znanja iz oblasti informatičkih tehnologija, čime se dodatno osigurava profesionalno postupanje i specijalizacija ovih organa.

ZAKLJUČAK

Nakon političkih i društvenih reformi 2000. godine, u Srbiji je usledila i reforma zakonodavstva, što se reflektovalo i na razvoj i dalje unapređenje pravnog okvira za suzbijanje visokotehnološkog kriminaliteta. Reformom krivičnog (materijalnog i procesnog) zakonodavstva postavljen je pravni osnov za bolju krivičnopravnu zaštitu od ovog vida kriminaliteta, a usvajanjem Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala postavljen je osnov za izgradnju odgovarajućeg institucionalnog okvira.

Analiza zakonskih tekstova relevantnih za obezbeđivanje krivičnopravne zaštite od visokotehnološkog kriminaliteta pokazuje da su postojeća rešenja u velikoj meri inovirana i usklađena sa zahtevima postavljenim u Konvenciji Saveta Evrope o visokotehnološkom kriminalu. Inkriminisana su gotovo sva ponašanja koja ulaze u domen visokotehnološkog kriminaliteta i predviđene su posebne dokazne radnje. Pa ipak, kao što je navedeno, još uvek postoji nedovoljna međusobna usklađenost postojećih rešenja, i to kako na nivou jednog zakonskog teksta, tako i među njima. S druge strane, obrazovanje posebnih organizacionih jedinica državnih organa značajan je korak u pravcu specijalizacije državnih organa za suzbijanje visokotehnološkog kriminaliteta, što je jedna od ključnih pretpostavki za efikasniju krivičnopravnu zaštitu, ako se imaju na umu specifičnosti ovog vida kriminaliteta i stalni napredak tehnologije koji je potrebno pratiti.

Ono što se, međutim, nameće kao zaključak je da postoji permanentna potreba za usklađivanjem pravne regulative sa savremenim oblicima izvršenja krivičnih dela koja spadaju u visokotehnološki kriminalitet, jer sa brzim razvojem tehnologije i *modus operandi* se veoma brzo menja i prilagođava novim dostignućima (Urošević, Uljanov i Vuković, 2012). Uz to, obučavanje ljudi u posebnim organizacionim jedinicama državnih institucija i njihova dobra tehnička opremljenost su *conditio sine qua non* uspešnog suprotstavljanja ovom vidu kriminaliteta.

Imajući sve to u vidu, ono što se nameće kao naredni korak jeste sagledavanje problema i izazova u pogledu praktične primene postojećih rešenja, a što zajedno sa analizom koja je data u ovom radu, može da predstavlja osnov za ukazivanje na dalje pravce unapređivanja pravnog i institucionalnog okvira za suzbijanje visokotehnološkog kriminaliteta, pa to ostaje da bude predmet nekog narednog rada.

LITERATURA

1. Konstantinović-Vilić, S., Nikolić-Ristanović, V., Kostić, M. (2009) *Kriminologija*. Niš: Pelikan Print.
2. Konvencija Saveta Evrope o visokotehnološkom kriminalu, http://conventions.coe.int/Treaty/EN/Treaties/Html/185, pristupljeno 15. marta 2013. godine.
3. Lepojević, B., Kovačević-Lepojević, M. (2007) Međunarodni standardi i suprotstavljanje kompjuterskom (cyber) kriminalu i njihova primena u Srbiji, *Zbornik Instituta za kriminološka i sociološka istraživanja*, br. 1-2, str. 265-291.
4. Republički zavod za statistiku (2012) *Punoletni učinioci krivičnih dela u Republici Srbiji – prijave, optuženja i osude,* Bilten br. 558, Beograd: Republički zavod za statistiku, dostupno na http://webrzs.stat.gov.rs/WebSite/repository/documents/00/00/89/64/SB_558_Punoletni_ucinioci_kd.pdf, pristupljeno 19. aprila 2013. godine.
5. Stojanović, Z. (2006) *Komentar Krivičnog zakonika*, Beograd: Službeni glasnik.
6. Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine, dostupno na http://www.digitalnaagenda.gov.rs/FileSystem/SiteDocuments/strategije/Strategija_razvoja_informacionog_drustva_2020.pdf, pristupljeno 15. aprila 2013. godine.
7. Urošević, V., Uljanov, S., Vuković, R. (2012) Policija i visokotehnološki kriminal: Primeri iz prakse i problemi u radu MUP-a Republike Srbije, dostupno na http://ebookbrowse.com/urosevic-v-uljanov-s-vukovic-r-policija-i-visokotehnoloski-kriminal-pdf-d390247822, pristupljeno 19. aprila 2013. godine.

SUPPRESSING COMPUTER CRIME: INTERNATIONAL STANDARDS AND NATIONAL LEGISLATION OF SERBIA

Digitalization, fast development of the computer industry and a widespread use of the information and telecommunication technology resulted in the new forms of crime and new forms of committing traditional criminal offences, which generally speaking present the so called computer or cyber crime. More and more attention has been paid to the computer crime by the academic and general public, but also by the state institutions and international organizations. Some of the key reasons

for that could be seen in the high dark figure of this form of crime, because criminals are using more sophisticated technology, which hardens uncovering and processing of this form of crime, while, on the other hand, the damage caused to the individuals, legal entities and states is becoming enormous. Thus, establishing legal and institutional framework is the first step in suppressing computer crime. Taking that as a departure point, in the first part of the paper we analyze the Council of Europe Convention on Cyber Crime in order to point out to the main standards and principles set forth in this international treaty. In the second part of the paper we analyze the positive legislation of the Republic of Serbia in order to notice to what extent our legislation is in compliance with the requirements set forth in the Convention and what could be further directions of the improvement of both legal and institutional framework in order to provide for the more efficient suppression of the computer crime.

KEYWORDS: computer crime / international standards / criminal protection / Serbia