

IZMENE U ZAKONODAVSTVU REPUBLIKE SRBIJE I BORBA PROTIV VISOKOTEHNOLOŠKOG KRIMINALA

Prof. dr Milan Milošević¹
Prof. dr Želko Nikač²

Rezime: Prepoznajući potrebu saradnje između država i privatnih privrednih subjekata u borbi protiv visokotehnoškog kriminala i potrebu zaštite legitimnih interesa u korišćenju i razvoju informacione tehnologije, Narodna skupština Republike Srbije je početkom 2009. godine posebnim zakonima ratifikovala Konvenciju Saveta Evrope o visokotehnoškom kriminalu i Dodatni protokol uz tu Konvenciju, koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko kompjuterskih sistema, nakon čega su bitno inovorani i drugi važnii propisi iz ove oblasti: Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnoškog kriminala, Zakonik o krivičnom postupku i Krivični zakonik. Polazeći od toga, u radu je analiziran katalog inkriminacija kojima se u Republici Srbiji suzbijaju takvi oblici kriminaliteta, kao i tekuće reforme specijalizovanih državnih organa u izmenjenom legislativnom i društvenom okruženju Republike Srbije. Ukazano je i na neke od postojećih i predstojećih problema u vezi sa otkrivanjem i dokazivanjem kompjuterskog kriminala

Ključne reči: Konvencija Saveta Evrope o visokotehnoškom kriminalu, kompjuterski kriminal, policija, krivično pravo, krivični postupak, računarski sistemi, računarski podatak, digitalni dokazi.

Uvod

Poznato je da je Konvencija Saveta Evrope o visokotehnoškom kriminalu potpisana u Budimpešti 23. novembra 2001. godine, dok je Dodatni protkol koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko kompjuterskih sistema sačinjen u Strazburu 28. januara 2005. godine. Takođe je poznato da Republika Srbija je 16. aprila 2005. godine u Helsinkiju potpisala kako Konvenciju o visokotehnoškom kriminalu, tako i Dodatni protokol uz tu Konvenciju, ali ih sve do nedavno nije ratifikovala.

Važan deo Konvencije o visokotehnoškom kriminalu posvećen je obavezama država da stvore normativne pretpostavke za uvođenje dodatnih procedura i ovlašćenja, kako bi se omogućilo efikasno otkrivanje i procesuiranje slučajeva kompjuterskog kriminala. U tom smislu esencijalni značaj ima formiranje posebnih državnih organa specijalizovanih za borbu protiv visokotehnoškog kriminala. Formalno-pravno, međutim, takve obaveze su postale aktuelne tek nakon ratifikacije pomenute Konvencije i Dodatnog protokola

¹ Udruženje IT Veštak, Beograd

² Kriminalističko-policijska akademija, Beograd

Uprkos tome, zakonodavac Republike Srbije je u periodu od aprila 2005. do marta 2009. godine usvojio više propisa kojima se Konvencija i Dodatni protokol implementiraju u naš pravni sistem. Najvažniji među njima su: Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, Krivični zakonik, Zakon o odgovornosti pravnih lica za krivična dela, Zakonik o krivičnom postupku, Zakon o policiji, Zakon o autorskim i srodnim pravima, Zakon o telekomunikacijama, Zakon o elektronskom potpisu, Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine, i Pravilnik o uslovima za pružanje internet usluga i sadržaju odobrenja.

Tokom marta 2009. godine Narodna skupština Republike Srbije je konačno ratifikovala Konvenciju o visokotehnološkom kriminalu i Dodatni protokol. Nakon toga su bitno inovirani drugi važni propisi iz ove oblasti, i to najpre Zakonik o krivičnom postupku, a potom i Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, te Krivični zakonik, čime je stvoren institucionalni okvir za efikasniju borbu protiv visokotehnološkog kriminala. Pri tome se Krivični zakonik morao uskladiti sa Konvencijom o visokotehnološkom kriminalu, dok se Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala morao uskladiti kako sa inoviranim Krivičnim zakonikom, tako i sa novim zakonima o javnom tužilaštvu, o uređenju sudova i o sedištim i područjima sudova i javnih tužilaštava.

Iako nova zakonska rešenja predstavljaju daleko kvalitetniji osnov za efikasno borbu protiv visokotehnološkog kriminala, s pravom im se upućuju i zamerke. Ovo utoliko pre, što je poznato da je tzv. tamna brojka kod ove vrste krivičnih dela i dalje visoka. Polazeći od toga, u daljem tekstu ćemo sagledati da li i kakvog efekta ima izmenjeno legislativno i društveno okruženje Republike Srbije, odnosno da li su i u kolikoj meri novele najvažnijih zakonskih propisa iz ove oblasti unapredile borbu protiv visokotehnološkog kriminala.

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

Tokom aprila meseca 2005. godine usvojen je već pomenuti Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala. Specijalizacija državnih organa na ovom planu inače je neophodna, imajući u vidu specifičnosti visokotehničkog kriminala, kao i stalni razvoj tehnologije koji je potrebno pratiti radi njegovog otkrivanja i suzbijanja. Naime, otkrivanje, krivično gonjenje i suđenje za ova dela zahteva obrazovanje posebnih organizacionih jedinica postojećih državnih organa, čije će delovanje na planu prevencije i, pogotovu, represije kriminaliteta u budućnosti doprineti boljoj zaštiti prava intelektualne svojine i unaprediti ambijent za investicije u privredi i poslovanje privrednih subjekata.

Po tom zakonu, koji je bitno inoviran je krajem 2009. godine tako da se sa svim izmenama u sadržaju primenjuje od prvog dana 2010. godine, funkciju krivičnog gonjenja izvršilaca pomenutih krivičnih dela vrši *Posebno odeljenje za borbu protiv visokotehnološkog kriminala Višeg javnog tužilaštva u Beogradu* („Posebno tužilaštvo“). Inače je Posebno tužilaštvo osnovano 20. februara 2007. godine, a bilo je organizovano kao posebno odeljenje tadašnjeg Okružnog javnog tužilaštva u Beogradu. Sada ga čine: Posebni tužilac za visokotehnološki kriminal, zamenici tužioca, portparol, sekretar i ostalo tužilačko osoblje. Po zakonu, ali i po samoj prirodi stvari, prednost prilikom postavljenja imaju oni tužioci, odnosno zamenici koji poseduju posebna znanja iz oblasti informatičkih i radiodifuznih tehnologija.

Posebnog tužioca postavlja Republički javni tužilac iz redova zamenika tužilaca, koji ispunjavaju uslov da budu zamenici višeg javnog tužioca, a uz pismenu saglasnost lica koje će biti postavljeno. Posebni tužilac se postavlja na period od četiri godine i može biti ponovo

postavljen, ali ga Republički javni tužilac može razrešiti i pre isteka vremena na koje je postavljen. Pre postavljenja Posebnog tužioca, Republički javni tužilac donosi rešenje o upućivanju datog lica u Posebno tužilaštvo, s tim što se po prestanku funkcije Posebni tužilac vraća se na funkciju koju je vršio pre postavljenja.

S druge strane, sva prvostepena suđenja po odgovarajućim predmetima ovog tipa kriminala u nadležnosti su *Odeljenja za borbu protiv visokotehnoškog kriminala Višeg suda u Beogradu*. Predsednik Višeg suda u Beogradu raspoređuje sudije u pomenuto Odeljenje iz reda sudija datog suda, uz njihovu saglasnost. Pri tome prednost imaju sudije koje poseduju posebna znanja iz oblasti informatičkih tehnologija. Osim toga, Predsednik Višeg suda u Beogradu može u Odeljenje rasporediti i sudije drugih sudova upućenih na rad u taj sud, uz njihovu saglasnost. U svakom slučaju raspoređivanje traje najduže dve godine, a može biti i produženo odlukom predsednika Višeg suda u Beogradu, takođe uz pismenu saglasnost raspoređenog lica.

Saglasno potrebnim kompetencijama i potrebama specijalizacije, prednost u raspoređivanju konkretnih sudija u Odeljenje imaju nosioci sudijskih funkcija koji imaju iskustva u borbi protiv visokotehnoškog kriminala. Po prirodi stvari, takve bi trebalo da budu i one sudije koje su uključene u PACO program. Poznato je, naime, da je Projekat za borbu protiv ekonomskog kriminala u Republici Srbiji (PACO Serbia) započet tokom decembra 2005. godine, a bavi se edukacijom iz oblasti zloupotrebe informatičkih tehnologija u kriminalne svrhe. Sprovodi ga Savet Evrope, finansira Evropska Unija, a realizuje Evropska agencija za rekonstrukciju. Najzad, za odlučivanje po pravnim lekovima (u drugom stepenu) za dela visokotehnoškog kriminala nadležan je *Apelacioni sud*.

Iz ovako određene nadležnosti pravosudnih (javnotužilačkih i sudskih) organa nadležnih za borbu protiv visokotehnoškog kriminala, uočava se da je blagovremeno ostvareno usklađivanje Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnoškog kriminala morao uskladiti sa Zakonom o javnom tužilaštvu, Zakonom o uređenju sudova i Zakonom o sedištim i područjima sudova i javnih tužilaštava, tj. sa novom organizacijom pravosudnih organa u Republici Srbiji koja je u funkciji od početka 2010. godine.

Najzad, na planu obezbeđenja relevantnih dokaza za dela kompjuterskog kriminala i elektronskog piratstva deluje specijalizovana policijska *Služba za borbu protiv visokotehnoškog kriminala* („Služba“). U stvari, ona je formirana kao Odeljenje za borbu protiv visokotehnoškog kriminala u okviru Službe za borbu protiv organizovanog kriminala, što znači da je sistematizovana u Upravi kriminalističke policije Direkcije policije, tj. u sedištu Ministarstva unutrašnjih poslova.[10] U svakom slučaju, starešinu Službe postavlja i razrešava Ministar unutrašnjih poslova po pribavljenom mišljenju Posebnog tužioca. Isto tako, predviđeno je da ovaj Ministar bliže uredi rad Službe odgovarajućim podzakonskim aktom u skladu sa zakonom.

Odeljenje za borbu protiv visokotehnoškog kriminala je po prirodi stvari upućeno na saradnju sa drugi organizacionim celinama Službe za suzbijanje organizovanog kriminala, posebno sa Odsekom za prikupljanje i obradu digitalnih dokaza u okviru Službe za specijalne istražne metode, ali i sa ostalim organizacionim jedinicama Direkcije policije i pojedinim službama bezbednosti Republike Srbije (BIA,VBA). Isto važi i za odgovarajuću saradnju sa službama u inostranstvu, odnosno sa organima stranih zemalja kojima je u nadležnost stavljeno otkrivanje, praćenje i presecanje delatnosti organizacija i pojedinaca usmerenih na vršenje krivičnih dela protiv intelektualne svojine, imovine i pravnog saobraćaja. Takva je, na primer, britanska služba za suzbijanje organizovanog kriminala (SOCA), u okviru koje deluje Nacionalna jedinica za borbu protiv visokotehnoškog kriminala (NHTCU) sa sedištem u Londonu.

U međuvremenu je Odeljenje za borbu protiv visokotehnološkog kriminala razvijalo svestranu saradnju i sa Nacionalnim centralnim biroom Interpola Beograd, budući da visokotehnološki kriminal predstavlja jedan od najčešće korišćenih oblika prekograničnog (transnacionalnog) kriminala. Ovo utoliko pre što je mesto za kontakte koje je dostupno 24 sata svakog dana u nedelji („punkt 24/7“), trenutno locirano u okviru pomenutog Nacionalnog centralnog biroa.

Krivični zakonik i dela visokotehnološkog kriminala

Borba protiv visokotehnološkog kriminala u Srbiji podrazumeva procesuiranje izvršilaca dela protiv bezbednosti računarskih podataka određenih Krivičnim zakonikom. U osnovi isto važi i za dela protiv intelektualne svojine, imovine i pravnog saobraćaja, i druga krivična dela kod kojih se, kao objekat ili kao sredstvo izvršenja, javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku.

Pre svega, reč je o takzovanoj intelektualnoj (elektronskoj, digitalnoj) pirateriji, odn. zloupotrebi i neovlašćenom stavljanju u promet zaštićenih autorskih dela iz sfere tzv. industrije sadržaja (filmska, muzička, izdavačka-knjige, software), i dr. Propisano je, međutim, da se odredbe Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala mogu primeniti radi otkrivanja, krivičnog gonjenja i suđenja kod ovog tipa krivičnih dela samo ako broj autorskih primeraka prelazi 2000 ili ako nastala materijalna šteta prelazi iznos od 1000 000 dinara.

U smislu Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, pod proizvodima u elektronskom obliku podrazumevaju se „računarski programi i autorska dela koja se mogu upotrebiti u elektronskom obliku“. Iz toga se zaključuje da su usklađene krivičnopravna i građanskopravna zaštita autorskih prava budući da se, prema aktuelnom Zakonu o autorskim i srodnim pravima, autorskim delima smatraju „naročito računarski programi u bilo kojem obliku njihovo izražavanja, uključujući i pripremni materijal za njihovu izradu, zatim muzička dela sa reči sa reči ili bez reči, kao i filmska (kinematografska i televizijska) dela“.

Iz ove i drugih odgovarajućih definicij proizlazi da pojmovi: računar, računarski podatak, računarski program, računarski virus, računarski sistem i računarska mreža, imaju značenje u smislu inoviranog čl. 112 Krivičnog zakonika Republike Srbije. Pri tome sa sigurnošću se može zaključiti da je zakonodavac imao sluha za kritičke stavove naše stručnoj javnosti. Naime, do decembra 2009. godine s pravom je ukazivano da su odredbe Krivičnog zakonika vezane na visokotehnološki kriminal zastarele i nedovoljno adekvatne, a u značajnoj meri i nepotpune (npr. Krivični zakonik nije definisao osnovni hardver – računar).[7,11]

Po aktuelnoj odredbi čl. 112 st. 17-20 33 i 34. Krivičnog zakonika, računarski podatak je svako predstavljanje činjenica, informacija ili koncepta u obliku koji je podesan za njihovu obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski sistem obavlja svoju funkciju. Računarskom mrežom smatra se skup međusobno povezanih računara, odnosno računarskih sistema koji komuniciraju razmenjujući podatke. Računarskim programom smatra se uređeni skup naredbi koji služe za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara.

Osim toga, računarski virus predstavlja 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. Računar je

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

Posebno treba apostrofirati okolnost da nakon novele Krivičnog zakonika s kraja 2009. godine u kategoriju visokotehnološkog kriminala svrstavaju delikti koji se mogu grupisati na sledeći način: (1) svi koji za grupni zaštitni objekat imaju bezbednost računarskih podataka, (2) protiv intelektualne svojine, imovine, privrede 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 primeraka prelazi 2000 ili ako nastala materijalna šteta prelazi iznos od 1000000 dinara, i (3) protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, za koje se zbog načina izvršenja ili upotrebljenih sredstava sa sigurnošću može zaključiti da su dela visokotehnološkog kriminala.

Iz ovako određenog kataloga visokotehnoloških krivičnih dela takođe se uočava da je zakonodavac Republike Srbije respektovao inicijativu za hitnu izmenu Zakonika, koju je Posebno tužilaštvo za borbu protiv visokotehnološkog kriminala tokom februara 2009. godine uputilo republičkom Ministarstvu pravde, sa obrazloženjem da su „pozitivnopravnim propisima iz stvarne nadležnosti Posebnog tužilaštva neopravdano izostavljena krivična dela koja se odnose na zloupotrebu platnih kartica i internet pornografiju“.

Pokazalo se, naime, da u periodu od 2005. do 2009. godine, pomenutim katalogom nisu bila obuhvaćena neka od krivičnih dela iz ove kategorije koja su u praksi najbrojnija, odnosno dela čija je društvena opasnost znatno izražena. U prvom redu reč je o krivičnom delu falsifikovanja i zloupotrebe platnih kartica iz čl. 225. KZ.[4] Isto važi i za distribuiranje tzv. dečje pornografije putem Interneta, tj. za krivično delo prikazivanja pornografskog materijala i iskorišćavanje dece za pornografiju iz čl. 185 st. 3 KZ.

Sasvim na kraju može se zaključiti da je krajem 2009. godine došlo do manjih izmena i kod „bazičnih“ inkriminacija visokotehnološkog kriminala, tj kod dela iz glave XXVII Krivičnog zakonika Republike Srbije. Konkretno, izmenjen je teži oblik neovlašćenog pristupa zaštićenom računaru, računarskoj mreži ili elektronskoj obradi podataka (čl. 302 st. 2 KZ), tako da se izvršiocem smatra onaj ko snimi ili upotrebi podatak dobijen putem neovlašćenog pristupa zaštićenom računaru, računarskoj mreži ili elektronskoj obradi podataka. Zaprećena sankcija u tom slučaju je novčana kazna ili zatvor do dve godine.

Radi usklađivanja sa Konvencijom Saveta Evrope o visokotehnološkom kriminalu, propisano je i novo krivično delo sa nazivom: „Pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka“. Izvršilac tog delikta je svako ko poseduje, pravi, nabavlja i daje drugom na upotrebu računare, računarske sisteme, računarske podatke i programe za izvršenje krivičnih dela protiv bezbednosti računarskih podataka (čl.304a KZ). Za ovo delo je zaprećena kazna zatvorom od šest meseci do tri godine, a propisano je i da se takvi predmeti, tj. sredstva za izvršenje krivičnih dela protiv bezbednosti računarskih podataka moraju oduzeti.

Zakonik o krivičnom postupku u funkciji borbe protiv visokotehnološkog kriminala

Efikasno otkrivanje i suzbijanje visokotehnološkog kriminala uključuje i veoma specifične operativne mere i radnje, kao i posebne dokazne radnje („specijalne istražne

tehnike“). U pitanju su internet patrole, presretanje telekomunikacija u realnom vremenu, traganje na mreži – Tracing i sl. Ovakve i slične mere često se sreću u uporednom pravu. Šta više, neke nacionalne policijske jedinice "patroliraju" Internetom da bi obezbedile javnu bezbednost i u toj oblasti. Te jedinice su razvile specifične softverske alate da bi otkrile krivična dela kao što su hakovanje ili distribuiranje tzv. dečje pornografije.

U Republici Srbiji je, na žalost, mogućnost Posebnog tužilaštva za visokotehnološki kriminal za primenu specijalnih istražnih tehnika u dužem periodu bila ograničena samo na primenu čl. 234 ZKP koji se odnose na dostavljanje podataka o stanju poslovnih i ličnih računa osumnjičenih, ali samo za krivična dela za koja je propisana kazna zatvora od najmanje četiri godine. Zbog toga su nadležni državni organi bili prinuđeni da se koriste postojećim, „klasičnim“ ovlašćenjima.

Tako se pribavljanje elektronske pošte osumnjičenog, odn. okrivljenog od internet provajdera, uz naredbu istražnog sudije, sprovodi primenom čl. 85 ZKP kojim je regulisana predaja pisama, telegrama i drugih pošiljki od strane subjekata registrovanih za prenos informacija, upućenih okrivljenom ili koje on odašilje, ako postoje okolnosti zbog kojih se može osnovano očekivati da će date pošiljke poslužiti kao dokaz u krivičnom postupku.[7]

Poštanska, telegrafska i druga preduzeća, društva i lica registrovana za prenošenje informacija inače su dužna da ovlašćenim službenicima policije (odn. BIA i VBA) omoguće izvršenje navedenih mera. Nesporno je da to omogućavalo prikupljanje komunikacionih podataka u skladu sa odredbama Konvencije o visokotehnološkom kriminalu, ali problemi u praksi nastajali zbog specifičnosti načina pribavljanja dokaza za tako sofisticirana krivična dela, budući da se do njih često dolazi monitoringom na mreži u realnom vremenu ("on line").

Za suzbijanje visokotehnološkog kriminala značajna je i novina sadržana u članu 82. st. 2 ZKP, po kojoj u predmete koji se mogu privremeno oduzeti spadaju i uređaji za automatsku obradu podataka i oprema na kojoj se čuvaju ili se mogu čuvati elektronski zapisi. Lice koje se koristi ovim uređajima i opremom dužno je da organu koji vodi postupak, na zahtev suda, omogući pristup i da pruži obaveštenja potrebna za njihovu upotrebu. Pre oduzimanja ovih predmeta organ koji vodi postupak će u prisustvu stručnog lica izvršiti pregled uređaja i opreme i popisati njihovu sadržinu. Najzad, ako korisnik prisustvuje ovoj radnji može staviti primedbe. Očigledno da je zakonodavac u ovom slučaju uvažio argumentovane zahteve tužilačke struke. [8]

U teoriji je izražen i stav da su krivičnoprocesne odredbe koje su od posebnog značaja za borbu protiv visokotehnološkog kriminala sadržane u članu 232. ZKP kojim se daje mogućnost da istražni sudija, na pismeni i obrazloženi predlog javnog tužioca, naredi nadzor i snimanje telefonskih i drugih razgovora ili komunikacija drugim tehničkim sredstvima (npr. telefaksom, teleprinterom, pejdžerom, elektronskom poštom - Internetom i dr.) onih lica za koja postoji osnovana sumnja da su sama ili sa drugim licima izvršila određena krivična dela. Ovakvo shvatanje je bilo prihvatljivo samo delimično i uslovno, na primer kada konkretan slučaj visokotehnološkog kriminala odnosi na pranje novca.

S tim u vezi treba naglasiti da se izmenama i dopunama aktuelnog ZKP od 2009. godine za otkrivanje nekih od tipičnih dela visokotehnološkog kriminala može koristiti i mera automatskog računarskog pretraživanja ličnih i drugih podataka, koja je značajna zbog sve izraženije kompjuterizacije ličnih i drugih podataka, te velikih mogućnosti koji ti podaci pružaju u vezi pribavljanja dokaza. Ovu radnju, po naređenju istražnog sudije, sprovode kriminalistička policija, Bezbednosno-informativna agencija, Vojno-bezbednosna agencija, organi carinske službe ili drugi državni organi, odnosno druga pravna lica koja na osnovu zakona vrše određena javna ovlašćenja. Mera može trajati najviše šest meseci, a iz važnih razloga njeno trajanje se može produžiti za još tri meseca.

Automatsko računarsko pretraživanje ličnih i drugih sa njima povezanih podataka sastoji se u automatskom pretraživanju već pohranjenih ličnih i sa njima neposredno povezanih podataka i njihovom automatskom poređenju sa podacima koji se odnose na krivično delo iz čl. 504a ZKP i na osumnjičenog, da bi se kao mogući osumnjičeni isključila lica u pogledu kojih ne postoji verovatnoća da su povezana sa krivičnim delom (čl. 504lj ZKP). Po svojoj suštini ovo je tzv. negativna raster potraga koja doprinosi eliminaciji određenih lica iz kruga osumnjičenih automatizovanim pretragama kroz policijske, administrativne i druge evidencije. Drugim rečima, ovaj metod eliminiše određena lica iz kruga onih koja se služe lažnim identitetom, tuđim kreditnim karticama i tome slično.

Automatsko računarsko pretraživanje ličnih i drugih sa njima povezanih podataka i njihova elektronska obrada može se preduzeti ako postoje osnovi sumnje da je učinjeno krivično delo iz člana 504a ZKP, ako se na drugi način ne mogu prikupiti dokazi za krivično gonjenje ili bi njihovo prikupljanje bilo znatno otežano. Izuzetno se može odrediti i ako postoje osnovi sumnje da se priprema neko od krivičnih dela iz člana 504a ZKP, a okolnosti slučaja ukazuju da se na drugi način delo ne bi moglo otkriti, sprečiti ili dokazati, ili bi to izazvalo nesrazmerne teškoće ili veliku opasnost. Suština ovog metoda je slobodan pristup policije svim evidencijama koje se vode automatizovano, što odudara od načela zaštite prava na privatnost građana i informatičko samoodređenje.[10]

Uygred da napomenemo da poslednjih godina u našoj stručnoj javnosti egzistira i predlog da se koriguju odredbe člana 225. stav 2. ZKP koje se odnose na ovlašćenje policijskih službenika da u pretkrivičnom postupku preduzimaju potrebne mere i radnje, u smislu da tu odredbu de lege ferenda treba dopuniti eksplicitnim ovlašćenjem policije da, po naredbi istražnog sudije, u pretkrivičnom postupku vrše tzv. on line pretres računarskih podataka na kompjuteru ili kompjuterskoj mreži, odnosno drugom uređaju ili predmetu koji sadrži takve podatke. Ovo utoliko pre, što se u uporednom pravu (Francuska i dr.) eksplicitno dozvoljava on line pretres, koji se vrši ubacivanjem određenog kompjuterskog programa pomoću kojeg se podaci na ciljanom računaru pregledaju dok je na Internetu. [5]

Zaključna razmatranja

Kontinuirani razvitak nauke i tehnike izvršio je značajan uticaj i na oblike i metode suzbijanja kriminaliteta, dok je ekspanzija razvoja informacionih tehnologija i telekomunikacija omogućila korišćenje dokaza u elektronskoj formi. Ubrzani razvoj kompjuterskih tehnologija zahteva budnost zakonodavca i neprestano praćenje promena koje se dešavaju, te fino podešavanje pozitivnog zakonodavstva kako bi se moglo odgovoriti novim izazovima.[6] Ratifikovanje Konvencije o visokotehnološkom kriminalu i Dodatnog protokola uz tu Konvenciju koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko kompjuterskih sistema, otvara značajne mogućnosti u tom pravcu.

Nesporno je, naime, da nakon ratifikovanja Konvencije o visokotehnološkom kriminalu i Dodatnog protokola, odnosno nakon noveliranja Zakonika o krivičnom postupku Republike Srbije iz 2001.godine (kojim je stavljen van pravne snage odgovarajući Zakonik iz 2006. godine) i, posebno, Krivičnog zakonika, u ključne faktore na ovom planu spadaju usklađivanje Zakona o organizaciji i nadležnosti državnih organa u borbi protiv visokotehnološkog kriminala sa Krivičnim zakonikom, Zakonom o javnom tužilaštvu, Zakonom o uređenju sudova i Zakonom o sedištim i područjima sudova i javnih tužilaštava.

Naročit značaj na tom planu ima odredba čl.2 Zakona o izmenama i dopunama Zakona o organizaciji i nadležnosti državnih organa u borbi protiv visokotehnološkog kriminala, kojim je precizirana i proširena nadležnost posebnih državnih organa za borbu protiv visokotehnološkog kriminala i na krivična dela protiv privrede kod kojih se kao objekat ili sredstvo izvršenja, javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, odnosno na druga krivična dela za koje se zbog načina izvršenja ili upotrebljenih sredstava sa sigurnošću može zaključiti da su dela visokotehnološkog kriminala. Nesporo je, naime, da će proširivanje nadležnosti posebnih državnih organa za borbu protiv visokotehnološkog kriminala i na takva krivična dela, omogućiti brže i efikasnije njihovo otkrivanje i procesuiranje.

Iako aktuelna zakonska rešenja predstavljaju solidan osnov i objektivno pružaju mogućnost za efikasno suzbijanje visokotehnološkog kriminala, niz zamerki koje su teoretičari i praktičari iz ove oblasti s pravom upućivali pre zakonskih novela iz 2009. godine još nisu prevaziđene. Često se, na primer, navodi da postojeći ZKP ne daje ni elementarnu definiciju dokaza, a kamo li elektronskog dokaza koji se pojavljuje u vezi sa izvršenjem krivičnih dela visokotehnološkog kriminala. S pravom se kritikuje i rešenje u Zakonu o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine (jer ne predviđa odgovarajuće oblike odgovornosti za samostalne trgovinske radnje), a predlaže se i otklanjanje nedostataka u Pravilniku o uslovima za pružanje internet usluga i sadržaju odobrenja. [8,11]

Najzad, evidentno je da radnje u pretkrivičnom postupku i istrazi za ovaj tip krivičnih dela po prirodi stvari moraju zadirati u privatnost lica, zbog čega je bitno da to bude samo u meri koja je nužna i saglasna međunarodnim standardima u ovoj oblasti. U tom smislu s pravom se insistira na poštovanju osnovnih standarda ustavom garantovane zaštite od nezakonitog pretresanja (presretanja i analize poruka) i zaplene (sakupljanja poruka, programa i računara), tako da u postupanju postoji ravnoteža između interesa zaštite privatnosti i društvenog interesa za krivični progon. [9] S tim u vezi treba podsetiti i na činjenicu da podatke kojima se narušava pravo na privatnost, a do kojih dođu organi otkrivanja i krivičnog gonjenja u toku pretkrivičnog postupka (prethodne istrage) ili istrage, oni moraju čuvati kao službenu tajnu i ne smeju ih koristiti ni u kakve svrhe osim za potrebe krivičnog postupka.

Reference

1. Britz M.T., *Computer forensics and cyber crime: An introduction*, Pearson Education, New Jersey, 2004
2. Vetsbi DŽ. R. i dr., *Međunarodni vodič za borbu protiv kompjuterskog kriminala*, Produktivnost AD, Beograd, 2004.
3. Casey E. (edit), *Handbook of computer crime investigation: forensic tools and technology*, Elsevier Academic Press, London ; San Diego, 2004.
4. Đokić Z., „Falsifikovanje i zloupotreba platnih kartica“, *Primjena savremenih metoda i sredstava u suzbijanju kriminaliteta* (zbornik), Internacionalna asocijacija kriminalista, Brčko, 2008, str. 482-497.

5. Đokić Z.; Živanović S., „Problemi pribavljanja, obezbeđivanja i korišćenja dokaza u elektronskoj formi, od značaja za krivični postupak“, *Teški oblici kriminala* (zbornik), IKSI;VŠUP, Budva, 2004, str. 305-318.
6. Jerković R., „Visokotehnološki kriminal – akteri i žrtve“, *Revija za bezbednost*, br. 3/2009, str. 27-34.
7. Komlen-Nikolić L., „Problemi domaćeg pravosuđa u borbi protiv visokotehnološkog kriminala“, *Revija za bezbednost*, br. 9/2008, str. 20-25.
8. Komlen-Nikolić L. i dr, *Suzbijanje visokotehnološkog kriminala*, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd, 2010.
9. Krstić J., "Standardi u postupanju tužilaca u borbi protiv kompjuterskog kriminala", : *ZITEH* (zbornik), Udruženje IT veštaka, Tara, 2004.
10. Milošević M.; Kesić T., *Policija u krivičnom postupku*, Kriminalističko-policijska akademija, Beograd, 2009.
11. Radulović S., „Pretnje visokotehnološkog kriminala i domaća zakonska regulativa“, *Revija za bezbednost*, br. 8/2008, str. 18-24.
12. Stephson, P., *Investigating Computer-Related Crime*, CRC Press, Boca Raton (etc.), 2000

Summary: Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies, on the beginning of year 2009, the National Assembly of the Republic of Serbia signed the Convention on cybercrime and Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, which is soon going to be fully implemented in our criminal legislation. Meanwhile, our legislative and social surroundings have changed, creating qualitatively new possibilities in fight against all aspects of computer crime. This paper analyzes incriminations used for repression of these forms of crime in the Republic of Serbia and current reforms of specialized police and jurisdictional agencies. This paper also considers specific operations of preliminary investigation and acquiring of evidence used for collections and verifying of digital evidence and forensic analysis. The paper also points out to some existing and future problems in detecting and proving of cybercrime.

Key words: Council of Europe Convention on Cybercrime, hi-tech crime, police, criminal law, crim procedure, computer system, computer data, digital evidences.