

KOMPARATIVNA ANALIZA KOMPJUTERSKOG KRIMINALA U ZAKONODAVSTVIMA REPUBLIKE SRBIJE I NEKIH STRANIH ZEMALJA

Dipl. pravnik, Vanesa Polić, master diplomac, Univerzitet Singidunum

vanesapolic@gmail.com

Apstrakt: U radu je napravljen pristup, sa pravnog aspekta, rešavanju problema kompjuterskog kriminala. Pisan je sa ciljem da omogući zakonodavcu, kao i stručnjacima iz oblasti kompjuterske tehnologije kako se nositi sa brojnim zloupotrebama u domenu ove nove sfere kriminala. Ono što je neophodno u suzbijanju te pojave jeste utemeljen i stabilan pravni sistem sa jakom zakonskom regulativom. Takav sistem bi doprineo IKT zaštiti od raznih vidova zloupotreba i ojačao poverenje u pravni sistem, a IKT stručnjaci bi mogli uvoditi nove metode i tehnike zaštite, znajući da su zakonski pokrivene. Bazira se na stanju u našem pravnom sistemu, metodima i regulativama, ali i osvrću na zakonodavstvo u stranim pravosudnim sistemima i njihov pristup u rešavanju ovog ozbiljnog i rasprostranjenog vida kriminala. Namenjen je, pre svega, pravosudnim organima i ustanovama, koje imaju akcenat na borbu protiv kompjuterskog kriminala.

Ključne reči: Kompjuterski kriminal, zakonodavac, pravni sistem, zakonska regulativa, IKT zaštita, pravosudni organi

1. UVOD

Živimo u modernom informacionom dobu, gde su računari jeftini, a ipak moćan alat koji se može koristiti u sprovođenju brojnih kriminalnih aktivnosti. Kompjuterski kriminal je pojava novijeg vremena. Predstavlja oblik kriminalnog ponašanja, kod koga se korišćenje kompjuterske tehnologije i informacionih sistema ispoljava kao način izvršenja krivičnog dela ili se upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka, u krivično – pravnom smislu, relevantna posledica.

U uslovima nagle ekspanzije i razvoja informaciono – komunikacione tehnologije (IKT), posebno Internet tehnologija, otvoreni su i brojni putevi za potencijalne opasnosti za informacionu imovinu (informacije i druge resurse IKT sistema) pravnih i političkih subjekata. Evidentno je da mogućnost pristupa i upotrebe računara, sa kriminalnim namerama, nesumnjivo može stvoriti bogatstvo vrednih dokaza. U realnom okruženju ne postoji apsolutna zaštita IKT sistema, bilo da su u pitanju napadi sa Interneta, uključujući brojne maliciozne programe ili se radi o napadima ljudskog faktora, poput hakera, krakera, vandala ili kompjuterskih terorista. Dakle, realno ne postoji IKT sistem koji je apsolutno siguran i otporan na kriminalne aktivnosti, jer je ekonomski neopravdan, nerentabilan ili se tako procenjuje.

Kompjuterski kriminal je postao deo našeg svakodnevnog života, iako često nismo ni svesni da se sa njim susrećemo, ili čak u njemu učestvujemo. Danas, gotovo sve informatički razvijene zemlje, kao i one koje to pretenduju da budu, formiraju posebne organe, komisije, komitete, ili radne grupe eksperata koji prate i istražuju kompjuterski kriminal na nacionalnom i međunarodnom planu. Zbog svog specifičnog karaktera, velike

društvene opasnosti i visoke stope rasta, u sve većoj meri postaje veoma ozbiljan društveni problem s kojim se treba suočiti društvo u celini, kao i pravni subjekti – organizacije i korporacije. Sve to zaslužuje pažnju države, njenih organa, ali i cele međunarodne zajednice.

Neophodan je odgovarajući zakonski i pravni okvir koji će pravno onemogućiti svaki vid slučajnog, ili namernog narušavanja ili sprečavanja funkcionisanja IKT sistema, kao i uništenje, neovlašćeno menjanje ili korišćenje podataka i informacija. Dakle, reč je o sponi pravne i informacione oblasti, koje zajedničkom saradnjom mogu doprineti uspešnom rasvetljavanju slučaja iz oblasti kompjuterskog kriminaliteta i sankcionisanju počinitelja. U suprotnom, nepostojanje zakonske regulative predstavlja posebnu teškoću, jer nameće istražnim organima ponekad i pretešku obaveznu da slučajeve kompjuterskog podvode pod standarde forme klasičnog kriminala.

2. KOMPJUTERSKI KRIMINAL U ZAKONODAVSTVU REPUBLIKE SRBIJE

2.1. Vrste kompjuterskog kriminala

Krivičnim zakonikom Republike Srbije 2005 godine, u naš pravni sistem uvedena su kompjuterska krivična dela [3]. U Glavi XXVII pomenutog Zakonika predviđena su krivična dela protiv bezbednosti računarskih podataka. Time se ujedno i naša zemlja pridružila nizu zemalja koje se odgovarajućim preventivnim i represivnim merama pokušavaju suprotstaviti različitim oblicima i vidovima zloupotrebe kompjutera.

2.1.1. Oštećenje računarskih podataka i programa

Predviđeno je kažnjavanje za svako lice koje neovlašćeno izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljenim računarski podatak¹ ili računarski program.² Delo se može učiniti samo u odnosu na računarski podatak ili program koji pripada nekom fizičkom licu – pojedincu (kao napadni objekt) i to sa više alternativno predviđenih delatnosti. Zapravo, cilj preduzimanja ovih delatnosti je onesposobljavanje za korišćenje, u potpunosti ili delimično, računarskih podataka (jednog ili više njih) ili programa. Posledica se sastoji u povredi zaštićenog dobra. Može ga učiniti svako lice, koje će se kazniti novčanom kaznom ili kaznom zatvora do jedne godine, a u pogledu vinosti³ potreban je umišljaj.⁴

Zakonom je predviđeno kažnjavanje za ovo krivično delo i to ukoliko je delom prouzrokovana šteta u iznosu koji prelazi četristopedeset hiljada dinara, učinilac će biti kažnjen kaznom zatvora od tri meseca do tri godine, a ukoliko je prouzrokovana šteta u iznosu koji prelazi milion i petsto hiljada dinara učinilac će se kazniti zatvorom od tri meseca do pet godina.

¹ „Računarski podatak” predstavlja informaciju, znanje, činjenicu, koncept ili naredbu, koja se unosi, obrađuje ili pamti ili je uneta, obrađena ili zapamćena u računaru ili računarskoj mreži

² „Računarski program” je uređen skup naredbi koji služi za upravljanje radom računara, kao i za izvršavanje određenih zadataka pomoću računara

³ „Vinost” (krivica) postoji ako je učinilac u vreme kada je učinio krivično delo bio uračunljiv i postupao sa umišljajem, a bio je svestan ili je bio dužan i mogao biti svestan da je njegovo delo zabranjeno

⁴ „Umišljaj” pretpostavlja da je učinilac bio svestan svog dela i hteo njegovo izvršenje ili kada je učinilac bio svestan da može učiniti delo pa je na to pristao

2.1.2. Računarska sabotaža

Krivično delo računarske sabotaže predviđa kažnjavanje kaznom zatvora od šest meseci do pet godina za svako lice koje unese, uništi, izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program i uništi, ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka sa namerom da onemogući ili znatno ometa postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte. Objekt napada je dvojako određen. Prvo, to je računarski podatak ili program, ali i računar odnosno drugi uređaj za elektronsku obradu ili prenos podataka. Drugo, objekti moraju da pripadaju državnom organu, javnoj službi ili drugim pravnim licima kao što su ustanove, preduzeća ili druge organizacije.

2.1.3. Pravljenje i unošenje računarskih virusa

Predstavlja vrstu krivičnog dela koje ima osnovni i teži oblik. Osnovni oblik čini lice koje napravi računarski virus⁵ u nameri da ga unese u tuđi računar ili računarsku mrežu.⁶ Radnja izvršenja je sačinjavanje, pravljenje virusa. Šta su to virusi, kako se prave, koje su njihove vrste ili karakteristike, svrha i sadržina, predstavljaju pitanja koja sudsko veće mora da reši u svakom konkretnom slučaju kao faktičko pitanje. U tome im stručnu pomoć pružaju lica sa posebnim znanjima i veštinama – u pitanju su veštaci informatičke struke. Delo je svršeno samim momentom pravljenja virusa u nameri da se unese u tuđi računar ili sistem bez obzira da li je takva namera i ostvarena u konkretnom slučaju ili ne, a predviđena kazna je novčana ili kazna zatvora do šest meseci. Ukoliko je ipak tako sačinjeni virus i unet, čime je prouzrokovana bilo imovinska bilo neimovinska šteta, radi se o težem obliku krivičnog dela, za koje je predviđena odgovarajuća novčana kazna ili kazna zatvora do dve godine.

2.1.4. Računarska prevara

U zavisnosti od visine pribavljene imovinske koristi za učinioca ili neko drugo lice, Zakon razlikuje dva oblika krivičnog dela. Osnovni oblik čini svako lice koje unese netačan podatak, propusti unošenje tačnog ili na neki drugi način prikrije ili lažno prikaže podatak, čime utiče na rezultat obrade i prenosa podataka u cilju pribavljanja imovinske koristi ili nanošenja imovinske štete drugome. Predviđena kazna je novčana ili kazna zatvora do tri godine. Postoji odredba po kojoj će se učinilac kazniti kaznom zatvora od jedne do osam godina ukoliko pribavljena korist prelazi iznos od četristopedeset hiljada dinara, odnosno kaznom zatvora od dve do deset godina ukoliko prelazi iznos od milion i petsto hiljada dinara. Učinilac koji ima nameru da drugog ošteti snosiće ili novčanu ili kaznu zatvora do šest meseci. Poseban oblik računarske prevare postoji kada je radnja krivotvorenja, prikrivanja ili lažnog prikazivanja podataka preduzeta u nameri da se drugom licu nanese kakva šteta. Ta šteta ne mora da nastupi u konkretnom slučaju, ali mora da bude pobuda, odnosno unutrašnji pokretač učinioca za preduzimanje radnje izvršenja. Može se raditi o imovinskoj, ali i o drugim vidovima neimovinske štete. Ono što karakteriše kompjuterske prevare jeste činjenica da daleko dopiru zbog veličine Interneta kao tržišta, da se brzo šire,

⁵ „Računarski virus“ je računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu, koji je napravljen da 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

⁶ „Računarska mreža“ je skup međusobno povezanih računara koji komuniciraju razmenjujući podatke

kao i izuzetno niski troškovi izvođenja takvih vrsta prevara. Kompjuterski prevaranti zloupotrebljavaju upravo one karakteristike Cyber–prostora koje doprinose rastu elektronske trgovine: anonimnost, distanca između prodavca i kupca i trenutna priroda transakcija. Uz to, koriste prednost činjenice da prevara preko Interneta ne zahteva pristup do nekog sistema za isplatu, kao što to zahteva svaka druga vrsta prevare i što je digitalno tržište još uvek nedovoljno uređeno i kao takvo konfuzno za potrošače, što predstavlja skoro idealne uslove za prevanu.

2.1.5. Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka

Delo ima osnovni i dva teža oblika ispoljavanja. Osnovni oblik čini lice koje kršeći mere zaštite neovlašćeno pristupi računaru ili računarskoj mreži. Dakle, radnja izvršenja jeste pristupanje, ulazak, upad u tuđi računar ili mrežu. Bitno je da je radnja preduzeta neovlašćeno, kršenjem predviđenih mera zaštite, a okolnosti moraju biti obuhvaćene umišljajem učinioca dela. Prvi teži oblik čini lice koje upotrebi podatak koji je pribavio, do koga je došao neovlašćenim pristupom zaštićenom računaru ili mreži. Ako je, pak, usled preduzete radnje došlo do nastupanja teških posledica za drugog radi se o najtežem krivičnom delu ove vrste za koji je zakon propisao kaznu. Bitno je da je posledica, i to teška, nastupila za drugog i da između nje i preduzete radnje upada u zaštićeni računarski sistem postoji uzročno – posledična veza. Krivičnim zakonikom je predviđena novčana ili kazna zatvora do šest meseci za svako lice koje kršeći mere zaštite, neovlašćeno uključi računar ili mrežu ili pristupi elektronskoj obradi podataka. Za lica koja upotrebe dobijene podatke na ovaj način predviđena je novčana ili kazna zatvora do dve godine, a ukoliko je usled dela došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili mreže učinilac će se kazniti zatvorom do tri godine.

2.1.6. Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži

U pitanju je krivično delo gde je objekt napada javna računarska mreža. Ima osnovni i teži oblik. Osnovni oblik čini lice koje neovlašćeno sprečava ili ometa pristup javnoj računarskoj mreži, a predviđena kazna je novčana ili kazna zatvora do jedne godine. U slučaju da se kao učinilac javi službeno lice u vršenju službe, radi se o kvalifikovanom delu. Zapravo, reč je o posebnom obliku krivičnog dela zloupotrebe službenog položaja službenog lica, koje sprečava ili ometa drugom fizičkom ili pravnom licu nesmetan pristup i korišćenje javne računarske mreže. Predviđena kazna za to lice je kazna zatvora do tri godine.

2.1.7. Neovlašćeno korišćenje računara ili računarske mreže

Postoje dva oblika ispoljavanja – osnovni i teži. Osnovni oblik se sastoji u neovlašćenom pristupu elektronskoj obradi podataka ili računarskoj mreži. Međutim, za postojanje dela nije dovoljno samo da neko lice neovlašćeno upadne u tuđi računarski sistem, već je potrebno da usled tako preduzete delatnosti dođe i do posledice u vidu povrede koja se manifestuje u zastoju ili poremećaju funkcionisanja, obradi ili prenosu računarskih podataka. Učinilac može biti svako lice, a u pogledu vinosti potreban je umišljaj. Teži oblik postoji ukoliko su usled preduzete radnje izvršenja osnovnog dela nastupile teške posledice. Koje su to teške posledice po računarski sistem, prenos, obradu podataka ili njegovo funkcionisanje, predstavlja faktičko pitanje koje sud mora da reši u svakom konkretnom slučaju na bazi svih objektivnih i subjektivnih okolnosti učinjenog dela i

ličnosti učinioca. Krivičnim zakonikom predviđena je novčana ili kazna zatvora do tri meseca, a gonjenje se preduzima po privatnoj tužbi.

<i>Član Zakonika</i>	<i>Krivično delo</i>	<i>Minimalna kazna</i>	<i>Maksimalna kazna</i>
čl. 298.	Oštećenje računarskih podataka i programa	Novčana kazna	Kazna zatvora od 5 godina
čl. 299.	Računarska sabotaza	Kazna zatvora od 6 meseci	Kazna zatvora od 5 godina
čl. 300.	Pravljenje i unošenje računarskih virusa	Novčana kazna	Kazna zatvora od 2 godine
čl. 301.	Računarska prevara	Novčana kazna	Kazna zatvora od 10 godina
čl. 302.	Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka	Novčana kazna	Kazna zatvora od 3 godine
čl. 303.	Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži	Novčana kazna	Kazna zatvora od 3 godine
čl. 304.	Neovlašćeno korišćenje računara ili računarske mreže	Novčana kazna	Kazna zatvora od 3 meseca

Tabela 1. Vrste i kazne za krivična dela kompjuterskog kriminala

2.2. Počinioci kompjuterskog kriminala

S obzirom da se počinioci kompjuterskog kriminala svrstavaju u različite kategorije prema pojavnim oblicima dela koja čine, ali i prema motivima koji ih pokreću u vršenju kriminalnih aktivnosti, ne može se govoriti o njihovom jedinstvenom profilu. Uopšteno, učinioci se mogu podeliti na zlonamerne, koji mogu da deluju radi ostvarenja imovinske koristi ili samo u cilju nanošenja štete, kao i na učinioce koji nisu motivisani ni na ostvarivanje koristi niti na prouzrokovanje štetnih posledica već jednostavno traže zadovoljstvo u neovlašćenom prodiranju u neki dobro obezbeđen informacioni sistem. Reč je o tzv. „hakerima“,⁷ koji koristeći svoje računarsko znanje, uz pomoć modema upadaju u tuđe kompjuterske sisteme. Po nekim istraživanjima koja su sprovedena u SAD-u i zemljama EU, došlo se do profila najčešćih počinilaca kompjuterskog kriminala. U pitanju su uglavnom mlađe osobe između 18 i 30 godina starosti, muškog pola, visokog koeficijenta inteligencije, ali i visokog stepena motivacije za ovu vrstu zloupotrebe. Tehnološki su veoma obrazovani, ranije neosuđivani, sa svega nekoliko godina radnog iskustva, bez problema na prethodnim radnim mestima i uglavnom sa višom kvalifikacijom od one koju zahteva posao na koji su raspoređeni. Dakle, u socio–demografskom smislu u pitanju su pretežno mladi i obrazovaniji ljudi, a u psihološkom, osobe koje su otvorene za nova iskustva, koje odlikuje maštovitost, ali često i stidljivost, povučenost i nedostatak samopouzdanja u realnom svetu. Počinioci ove vrste krivičnih dela imaju specifičnu motivaciju, koju čine, ne samo finansijski i ekonomski razlozi, već i tehnički sindrom, sindrom milosrđa, emotivni razlozi, visok nivo znanja, a izvršenje dela za njih uglavnom predstavlja izazov ili igru [4] [6].

⁷ „Haker“ podrazumeva benignu individu u koja pokušava da neovlašćeno prodre u tuđi informacioni sistem

2.2.1. Amateri

Grupi amatera pripadaju pojedinci koji najčešće imaju legalno zanimanje, a iz različitih razloga se povremeno upuštaju i u kriminalnu delatnost. Postoji nekoliko tipova amatera:

- a) Slabi i podložni pojedinci – često krađu ili vrše pronevere, a da prethodno uopšte nisu sagledali moguće posledice tog čina, što svakako ukazuje na njihov amaterizam. Radi se o pojedincima koji su najčešće izloženi pritiscima konkurencije, obaveštajnih službi ili profesionalnih kriminalaca;
- b) Ljudi sa porokom – kocka, droga, alkohol, kao i život iznad sopstvenih mogućnosti predstavljaju poroke koji pojedinca snažno motivišu za izvršavanje kriminalnih dela. U pitanju je tip amatera koji se redovno najlakše i najčešće otkriva, jer njegovi privatni problemi ne ostaju nezapaženi, s obzirom da bitno utiču na ponašanje na radnom mestu;
- c) Frustrirani pojedinci – u pitanju su nezadovoljni, razočarani, ogorčeni pojedinci. Predstavljaju tip kriminalaca koji bi se mogli svrstati u grupu opasnijih. Osećaj da su prevareni, nepravedno zapostavljeni ili zaobidjeni, u njihovim očima opravdava svaki nezakoniti čin, od sabotaže, preko krađa i pronevera, pa sve do vandalističkog ponašanja.

2.2.2. Profesionalni kriminalci

U pitanju su osobe kojima je jedno od glavnih, a često i jedino zanimanje bavljenje kriminalom. Ono što ih posebno karakteriše jeste laka prilagodljivost novim situacijama, pre svega onima koje nastaju kao posledica tehnološkog razvoja. U organizacionom smislu, nastupaju pojedinačno, u grupama ili u organizacijama.

- a) Individualni kriminalci – nastupaju samostalno i nezavisno u realizaciji ciljeva, koji se najčešće svode na ostvarivanje određene materijalne dobiti. Deluju u lokalu i nemaju dugoročnu strategiju i razrađenu taktiku, zbog čega im je potencijal za izvršavanje kriminalnih dela relativno ograničen;
- b) Organizovane grupe – ova kategorija predstavlja skupove pojedinaca koji imaju zajedničke interese, a u njihovoj realizaciji zajednički deluju. Potencijal za izvršavanje kriminalnih dela im je znatno veći u odnosu na pojedinca, ali još uvek ne toliki da bi posledice imale široke razmere. Međutim, promene koje donosi informaciona tehnologija dovode do drastičnog uvećavanja potencijala;
- c) Kriminalne organizacije – predstavljaju najviši organizacioni oblik kriminalaca, karakterističan po organizacionoj čvrstini, hijerarhijskim odnosima, strogoj disciplini, poslušnosti i ličnoj lojalnosti, uz izgrađenu dugoročnu strategiju i detaljno razrađenu taktiku. U pitanju su organizacije koje već uveliko koriste računare kao alat za planiranje i kontrolu svih svojih aktivnosti.

2.2.3. Hakeri

Napretkom tehnologije pojavljuje se i novi tip kompjuterskih kriminalaca. Reč je o hakerima, ljudima koji su opsednuti novom tehnologijom u toj meri da je svaki aspekt

njihovog života u manjoj ili većoj meri povezan sa kompjuterom. Njihova aktivnost, poznata pod nazivom haking,⁸ odvija se sa ciljem neovlašćenog provaljivanja u tuđe računarske sisteme, a specifični motivacioni faktori su: intelektualni izazov, radoznalost, zabava, osećaj svemoći, potreba za trijumfom, osveta, prestiž, nadoknada osećaja društvene ili lične manje vrednosti.

Vrhunsko zadovoljstvo nalaze u samom činu provaljivanja u višestruko obezbeđene informacione sisteme, te što su sistemi bolje čuvani, to za njih predstavlja veći izazov. Prema svom profesionalnom opredeljenju su najčešće programeri ili visoko obrazovani informatičari, mada je ponekad reč i o osobama koje su veštinu i znanje stekli baveći se kompjuterima iz hobija. U pitanju su veoma inteligentni učinioci, a jedina prava zaštita od njihovih provala je jačanje kriptografskih sistema zaštite, uz strogu kriminalnu politiku prema ovakvim učiniocima. Nezavisno od motiva koji ih pokreću predstavljaju veliku opasnost, naročito u situacijama kada se upuštaju u rizične informatičke avanture u osetljivim područjima, kao što su nacionalna bezbednost, industrija naoružanja, satelitska tehnologija i slično.

2.3. Visokotehnoški kriminal

Po Zakonu o organizaciji i nadležnosti državnih organa u borbi protiv visokotehnoškog kriminala, VTK

„predstavlja 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“ [9].

Zakon se primenjuje u cilju otkrivanja, krivičnog gonjenja i suđenja za krivična dela protiv bezbednosti računarskih podataka i krivična dela protiv intelektualne svojine, imovine i pravnog saobraćaja kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku. U praksi su najizraženiji neki oblici VTK.

2.3.1. Povreda intelektualne svojine

Intelektualna svojina predstavlja skup prava koja se odnose na književna, umetnička i naučna dela, interpretacije umetnika, pronalasci i kao rezultat inventivnog napora, naučna otkrića, industrijski dizajn, žigove, zaštitu prava od nelojalne konkurencije, kao i sva druga prava koja su rezultat intelektualnog napora u industrijskom, naučnom i umetničkom domenu [10].

Društvena zajednica je obezbedila pravo na intelektualnu svojinu radi podsticanja izuma i kreativnih ostvarenja od kojih društvo ima koristi, kao i da bi pomogla inovatorima i stvaraocima da žive od svog rada. Naime, zaštita intelektualne svojine doprinosi ekonomskom rastu kako u razvijenim, tako i u zemljama u razvoju na način što podstiče inovacije, kulturnu raznolikost i tehnički razvoj kao deo šireg političkog okvira. Pravilno upravljanje intelektualnom svojinom može postati moćan alat rasta i progressa u društvu.

⁸ „Haking“ je neovlašćen nasilni pristup, odnosno pokušaj pristupa informacionim sistemima, najčešće sa udaljene lokacije

Pitanje povrede intelektualne svojine i zaštita kompjuterskih programa regulisana je i odredbama Zakona o autorskim i srodnim pravima,⁹ po kojem autor¹⁰ računarskog programa ima isključivo pravo da drugome zabrani ili dozvoli davanje na poslu¹¹ primeraka svog dela [7]. Ukoliko je autorsko delo¹² računarski program, predviđena je mogućnost da se dozvoli licu koje je na zakonit način pribavilo primerak računarskog programa, da radi sopstvenog uobičajenog namenskog korišćenja programa, bez dozvole autora i bez plaćanja autorske naknade smešta program u memoriju računara i pušta u rad, otklanja greške i vrši druge neophodne izmene.

2.3.2. Piraterija

Piraterija predstavlja izuzetno rasprostranjeno kompjutersko krivično delo, čija je osnovna karakteristika korišćenje ili umnožavanje, kao i distribucija softvera i programa koji nisu nabavljeni na legalan način. Postoje brojni razlozi iz kojih pirati krađu softver, a kreću se od ignorisanja zakona do ostvarivanja profita. Razlikujemo pet osnovnih vrsta softverske piraterije, a to su:

- 1) Piraterija krajnjeg korisnika – javlja se kada zaposleni reprodukuje softverske kopije bez autorizacije;
- 2) Klijent–server prevelika upotreba – javlja se u situacijama kada previše zaposlenih na mreži koriste centralnu kopiju programa u isto vreme;
- 3) Internet piraterija – kada se softver preuzima sa Interneta;
- 4) Snimanje na hard disk – kada firme koje prodaju nove računare kopiraju ilegalne kopije softvera na hard disk kako bi prodaju računara učinile atraktivnijom;
- 5) Falsifikovanje softvera – predstavlja ilegalno dupliranje i prodaju autorizovanog materijala sa namerom da se direktno imitira zaštićeni proizvod.

2.3.3. Kompjuterska krađa

Reč je o krivičnom delu oduzimanja tuđe pokretne stvari u nameri pribavljanja protivpravne imovinske koristi. Pod krađu se, u kompjuterskom kriminalu, mogu podvesti krađe računara i njegovih komponenti, krađa razne vrste robe, podataka, lozinki, zloupotreba platnih kartica. Zauzima izuzetno visoko mesto u oblasti kompjuterskog kriminaliteta. Naime, predstavlja posebno društveno – opasnu radnju, a procene stručnjaka su da će intenzivno rasti uporedo sa porastom elektronske trgovine.

2.3.4. Pranje novca

Skupština Republike Srbije je 18. marta 2009. godine usvojila Zakon o sprečavanju pranja novca i finansiranja terorizma. Zakonom se propisuju radnje i mere koje se preduzimaju radi otkrivanja i sprečavanja pranja novca i finansiranja terorizma, čime je ujedno prestao

⁹ „Zakon o autorskim i srodnim pravima“, „Službeni list SCG“, br. 61/04, 22.XII 2004.

¹⁰ „Autor“ je fizičko lice čije su ime, pseudonim ili znak naznačeni na primercima dela, ili navedeni prilikom objavljivanja dela, dok se ne dokaže drugačije; on je nosilac autorskog prava

¹¹ „Davanje na poslu“ je davanje primeraka dela drugome od strane institucija dostupnih javnosti, bez neposredne ili posredne imovinske koristi

¹² „Autorsko delo“ je originalna duhovna tvorevina autora, izražena u određenoj formi bez obzira na njegovu umetničku, naučnu ili drugu vrednost, njegovu namenu, veličinu, sadržinu i način ispoljavanja, kao i dopuštenost javnog saopštavanja njegove sadržine

da važi prethodni Zakon o sprečavanju pranja novca iz 2005. godine. U sastavu Ministarstva nadležnog za poslove finansija obrazuje se Uprava za sprečavanje pranja novca, kao njen organ. Zadatak uprave se sastoji u prikupljanju, obrađivanju, analiziranju i prosleđivanju nadležnim organima informacija, podataka i dokumentacije koju pribavlja u skladu sa zakonom i vrši druge poslove koji se odnose na sprečavanje i otkrivanje pranja novca i finansiranje terorizma. Zakon je širi u odnosu na prethodni i po pitanju saradnje sa pravosudnim organima i učešćem advokata u postupku. Cilj zakona jeste sprečavanje štetnih posledica po rad organa i organizacija koji su nadležni za borbu protiv pranja novca, finansiranja terorizma i drugih oblika kriminala, a pre svega organizovanog i finansijskog kriminala i korupcije [12].

2.4. Značaj specijalizovanih pravosudnih organa u borbi protiv VTK

Broj krivičnih dela iz oblasti kompjuterskog kriminala u stalnom je porastu sa uvođenjem IKT u svakodnevni život kako firmi, tako i građana. S vremenom, u Ministarstvu unutrašnjih poslova i tužilaštvu, problem definisanja kriminala, stvaranje adekvatne zakonske regulative i obučavanje kadrova za borbu protiv VTK postaje jedan od važnijih za rešavanje.

Za postupanje po ovom pitanju nadležno je Okružno javno tužilaštvo u Beogradu, u okviru koga je obrazovano posebno odeljenje za borbu protiv VTK. Njegovim radom rukovodi posebni tužilac za VTK, koji ima prava i dužnosti kao i javni. Postavlja ga Republički javni tužilac, a prednost pri izboru imaju javni tužioci odnosno njihovi zamenici koji poseduju posebna znanja iz oblasti informatičkih tehnologija. Što se suda tiče, u Okružnom sudu u Beogradu za postupanje u predmetima krivičnih dela, obrazuje se Veće za borbu protiv VTK. Sudije u Veće raspoređuje predsednik Okružnog suda iz reda sudija tog suda, a prednost pri izboru imaju sudije koje poseduju posebna znanja iz oblasti informatičkih tehnologija [8].

U Ministarstvu unutrašnjih poslova trenutno ne postoji posebna organizaciona jedinica koja se bavi sprečavanjem i suzbijanjem kompjuterskog kriminala, osim Odseka za suzbijanje kompjuterskog kriminala, koji je sistematizovan u okviru Službe za borbu protiv organizovanog kriminala Uprave kriminalističke policije (SBPOK). Imajući u vidu ekspanziju ove vrste kriminala, izražen je stav da bi trebalo formirati posebne službe za borbu protiv VTK. Jedna od najpoznatijih takvih službi, koja je ujedno i deo kriminalističke policije, jeste National Hi-Tech Crime Unit (NHTCU)¹³ sa sedištem u Londonu. Osnovana je u aprilu 2001. godine i sastoji se od četiri sekcije: za istrage; za prikupljanje operativnih saznanja, odnosno za "obaveštajni rad"; za otkrivanje digitalnih dokaza; i za taktičku i tehničku podršku.

Nesporno je da konstituisanjem specijalizovanih pravosudnih organa postupak pred sudom za odgovarajuća krivična dela treba biti kraći i efikasniji, s obzirom na to da su mnogo bolje opremljeni i osposobljeni za borbu protiv kompjuterskog kriminala, kao i drugih vidova sofisticiranog kriminala kako unutar zemlje, tako i u međunarodnim okvirima.

¹³ *National Hi-Tech Crime Unit (NHTCU) – Nacionalna jedinica za borbu protiv VTK*

2.5. Konvencija o VTK

Konvencija o VTK je usvojena na Komitetu ministara Saveta Evrope, 8. novembra 2001. godine, a otvorena za potpisivanje u Budimpešti 23. novembra iste godine. Predstavlja rezultat četvorogodišnjeg rada ekspertske grupe Saveta Evrope potpomognute stručnjacima iz Sjedinjenih Američkih Država, Kanade, Japana i drugih država nečlanica Saveta Evrope. Još u preambuli se navodi da je jedan od razloga za njeno donošenje uverenje da efikasna borba protiv kompjuterskog kriminala zahteva uvećanu, brzu i funkcionalnu saradnju u krivičnim stvarima i upravo to moraju imati u vidu zemlje našeg regiona ukoliko žele da ostvare rezultate u borbi protiv kompjuterskog kriminala [11].

Ciljevi Konvencije su harmonizacija domaćih materijalno-pravnih odredbi koje su u vezi sa kompjuterskim kriminalom, obezbeđivanje domaćem procesnom pravu sredstava neophodnih za sprovođenje istrage i pokretanje postupaka protiv učinilaca krivičnih dela iz oblasti kompjuterskog kriminala i krivičnih dela izvršenih upotrebom kompjuterske tehnologije.

Sa stanovišta pravne logike i generalnog pristupa koji Konvencija zagovara iznete su neke kritike [1]. Jedna od značajnijih je ona koja kaže da Konvencija ne uvažava druge pravne kulture i da se ne vodi dovoljno računa o postojanju strukturalne disproporcije u razvoju IKT. Značajan broj država u svetu pripada upravo tom tehnološki zaostalom ili tek probuđenom krugu članica međunarodne zajednice. Uz to pisana je u okviru Saveta Evrope, uz snažan uticaj SAD, Kanade i Japana, tako da više odslikava njihove potrebe i interese nego većine ostalih zemalja, a posebno onih u razvoju. Upravo zbog te činjenice je većina zemalja doživljava kao politički instrument u rukama vojno – politički tehnološki najuticajnijih država. Ipak, bez obzira na potencijalne kritike, predstavlja dosad najznačajniji međunarodno – pravni okvir i uputstvo za suprotstavljanje rastućem VTK.

3. KOMPJUTERSKI KRIMINAL U PRAVOSUDNIM SISTEMIMA STRANIH ZEMALJA

3.1. Regulisanje pitanja kompjuterskog kriminala u pojedinim zemljama

Budući da preventivne mere (opšteg i specijalnog karaktera) često nisu dovoljne niti jedine mere kojima se društvo suprotstavlja naraslim i nabujalim oblicima i vidovima zloupotrebe kompjutera u različite svrhe, logično je da sva savremena krivična zakonodavstva u sistemu inkriminacija poznaju jedno ili više kompjuterskih krivičnih dela za koja su propisane različite vrste i mere krivičnih sankcija [2] [5].

3.1.1. Kompjuterski kriminal u zakonodavstvu SAD

Po svom unutrašnjem uređenju, SAD je federativna država, a jedna od posledica takvog društvenog uređenja je upravo dvostruki pravni poredak. Naime, svaka od saveznih država ima svoj pravni poredak i set propisa, a za međudržavne (između saveznih država) i međunarodne sporove zaduženo je pravo federacije. Što se krivičnog prava tiče, u federalni domen često spadaju i ponašanja za koja je zakonodavac smatrao da su previše bitna da bi bila prepuštena samo sistemima saveznih država. U SAD se u skladu sa posebnim zakonom – *Computer Matching Act* iz 1998 godine, koriste slične mere u različite svrhe. Naime, uz pomoć kompjutera i postojećih banaka podataka iz kriminalističkih evidencija, izrađuje se kompjuterski profil učinilaca različitih izvršilaca krivičnih dela, tzv. *Computer*

profiling, što policiji služi u operativne svrhe. Naravno, pribavljeni podaci se mogu koristiti samo u navedene svrhe, što je uređeno Zakonom o privatnosti, koji sadržava opšte odredbe o zaštiti podataka. Cilj *Hi-Tech Crime Research programme* istraživanja, koji se sprovodio, bio je da se identifikuje kriminal i zlonamerne pretnje vezane za zloupotrebu računara i Interneta. Studija je imala tri ključna cilja: da identifikuje koja područja Interneta i Internet tehnologije će biti moguće žarište kriminalnih aktivnosti u tri do pet godina; da se ispita koja područja Interneta i Internet tehnologija imaju potencijal da budu zloupotrebljena od strane kriminalaca i predstavljaju izazov za sprovođenje zakona, kao i da istraži kako se različiti sektori mogu pripremiti za takve pretnje i izazove. Američko zakonodavstvo poseduje bogat asortiman zakona, kojima se reguliše pitanje zaštite od kompjuterskog kriminala. Neki od najznačajnijih, koje treba pomenuti su 4th Amendment,¹⁴ *Computer Fraud and Abuse Act of 1986*,¹⁵ *Electronic Communications Privacy Act of 1986*,¹⁶ *Computer Virus Eradication Act of 1988*,¹⁷ *Electronic Espionage Act of 1996*,¹⁸ *Child Pornography Prevention Act*,¹⁹ *USA Patriot Act*.²⁰ Svaki od navedenih zakona, u velikoj meri, doprinosi kvalitetu američkog zakonodavstva po pitanju suzbijanja svih oblika kompjuterskog kriminala, a ujedno predviđa i izuzetno stroge sankcije za počinioce tih dela. Takav je, na primer, *Electronic Communications Privacy Act* (ECPA), koji je potpisao tadašnji predsednik SAD, Regan, u oktobru 1986. godine. Njime je predviđena zaštita prenosa i skladištenja digitalnih komunikacija, te pokrivanje svih komunikacionih usluga. Za počinioce je predviđena kazna zatvora od 5 godina za prvi napad, a 10 godina za naknadni prekršaj za oštećenje saveznog računarskog sistema. Sasvim očekivano, pravni sistem SAD je otišao najdalje u zaštiti nesmetanog funkcionisanja kompjuterskih sistema i Interneta. I sudska praksa i zakonodavstvo su definitivno najznačajniji izvor podataka i iskustva za druge pravne sisteme.

3.1.2. Kompjuterski kriminal u zakonodavstvu Velike Britanije

Sve do 1990. godine Velika Britanija je bila primer zemlje koja je rešavala pitanja iz područja kompjuterskog kriminala kroz postojeće propise. To su bili: *Theft Act* (1968),²¹ *Forgery and Counterfeiting Act* (1981),²² *Data Protection Act* (1998).²³ Naravno, postojao je i propis o zaštiti autorskih i srodnih prava, tzv. *Copyright, Design and Patents Act* (1988).²⁴ U Velikoj Britaniji je 1990. godine donet poseban Zakonik o zloupotrebi kompjutera, koji predviđa niz krivičnih dela vezanih za zloupotrebu kompjutera i drugih informacionih sistema za koje su propisane veoma stroge kazne. Kada je reč o usaglašenosti ovog zakona i Konvencije o VTK, budući da je Ujedinjeno kraljevstvo država sa *common law*²⁵ pravnim sistemom, poput SAD i drugih država *Commonwealth*,²⁶ konkretni doseg ovog propisa će zavisiti od sudova koji će ga primjenjivati. Naime, sudovi u *common law* sistemima imaju kreativnu ulogu, a njihove

¹⁴ Četvrti amandman

¹⁵ Zakon o kompjuterskim prevarama i zloupotrebama

¹⁶ Zakon o privatnosti elektronskih komunikacija

¹⁷ Zakon o iskorenjivanju računarskih virusa

¹⁸ Zakon o elektronskoj špijunaži

¹⁹ Zakon o prevenciji dečje pornografije

²⁰ Zakon o borbi protiv terorizma

²¹ Zakon o krađi

²² Zakon o falsifikovanju i krivotvorenju

²³ Zakon o zaštiti podataka

²⁴ Zakon o zaštiti autorskih i srodnih prava

²⁵ „Common law“ – opšte pravo

²⁶ „Commonwealth“ (Komonvelt nacija) je udruženje nezavisnih suverenih zemalja širom sveta od kojih su većina nekadašnji članovi Britanske imperije

odluke (presedani) su bitan izvor prava. Takođe je oformljen i Nacionalni centar za VTK, kao i agencije koje se bave zločinima kompjuterskog kriminala, čiji fokus je usmeren na složene mrežne kapacitete, što stvara platformu za činjenje kriminalnih aktivnosti. Kriminalistička policija je primenjivala, sve do kraja 1999. godine, različite prikrivene istražne tehnike u cilju rasvetljavanja i uspešne borbe protiv najtežih oblika kriminala. Odredbama zakona o ljudskim pravima iz 1998. godine, britanskim sudovima omogućeno je da direktno primenjuju odredbe Evropske konvencije. Iako je reč o državi bitno različite pravne tradicije od nas, zakonodavstvo i praksa britanskog pravosuđa ipak predstavljaju značajan izvor za poređenje.

3.1.3. Kompjuterski kriminal u zakonodavstvu Nemačke

Među prvima u svetu, Nemci su 1970. godine u pokrajini Hessen doneli Zakon o zaštiti podataka. Međutim, tek u savezni Zakon o zaštiti podataka iz 1977. godine unesene su krivičnopravne sankcije na području zaštite automatske obrade podataka. Iako Nemački krivični zakonik, iz 1978. godine, ne poznaje kompjuterska krivična dela, to ne znači da ta protivpravna, nedopuštena ponašanja nisu inkriminisana. Naime, u Nemačkoj je 1988. godine donet poseban Krivični zakon za suzbijanje privrednog kriminaliteta, koji predviđa niz kompjuterskih krivičnih dela i to: krađu podataka, kompjutersku špijunažu, kompjutersku prevaru, falsifikovanje podataka, obmanu u pravnom prometu pri obradi podataka, promenu podataka, kao i kompjutersku sabotažu. Pored pomenutih pravnih izvora svakako treba pomenuti i Zakon o autorskim delima. Što se sudova tiče, nemački sudovi imaju značajno iskustvo u rešavanju slučajeva vezanih za kompjuterski kriminal. Kada je reč o primeni istražne tehnike kompjuterskog sravnjivanja podataka, uređena je saveznim pokrajinskim zakonima, kao i članom 98. a-c nemačkog Zakona o krivičnom postupku. Njima su precizirani uslovi automatizovanog pretraživanja identifikacionih podataka osoba, kao i njihovih karakterističnih fizičkih ili psihičkih osobina, a koji upućuju na učinioce tačno određenih krivičnih dela da bi se isključio broj osumnjičenih ili suzio krug osoba koje bi mogle doći u obzir kao potencijalni izvršioci.

3.1.4. Kompjuterski kriminal u zakonodavstvu Austrije

Sve do 1987. godine austrijsko krivično zakonodavstvo nije sadržavalo posebne odredbe u pogledu kompjuterskog kriminala, već je jedini propis u kojem su bile sadržane odredbe koje su se odnosile na kompjuterske zloupotrebe bio Zakon o zaštiti podataka. Zaštita pružena ovim propisom odnosila se samo na lične podatke građana, dok drugi kompjuterski podaci nisu uživali nikakvu zaštitu. Takvo neodrživo stanje dovelo je do reforme krivičnog zakonodavstva, pa je 1988. godine, na predlog austrijskog ministarstva pravde, predložena dopuna zakonodavstva. U tom smislu je predlagano da se u Krivični zakon (*StrafGesetzbuch, StGB*) uvedu nova krivična dela, kao što su oštećenje podataka, kompjuterska prevara, falsifikovanje, krađa vremena. Na osnovu lepeze krivičnih dela koja su uvedena u austrijsko zakonodavstvo može se primetiti da su austrijski i nemački stručnjaci sarađivali, budući da su obe zemlje otprilike u isto vreme, na sličan način, razmatrale reformu krivičnog zakonodavstva u pogledu obuhvatanja krivičnih dela kompjuterskog kriminala. Međutim, predlog je samo delimično prihvaćen, tako da su u konačnu novelu *StrafGesetzbucha* unesena samo krivična dela oštećenja podataka (čl.126 StGB) i zloupotreba obrade podataka (čl.148 StGB). Tako je novi Krivični zakon stupio na snagu 1988. godine.

3.1.5. *Kompjuterski kriminal u zakonodavstvu Francuske*

Poput drugih zemalja kontinentalnog pravnog sistema, francusko krivično zakonodavstvo je koncentrisano oko pisanog zakonika, donesenog od strane predstavničkog tela (*Code Penale*). Krivična dela kompjuterskog kriminala sadržana u francuskom Krivičnom zakonu su neovlašćeno pribavljanje podataka, neovlašćeno pristupanje, menjanje sadržaja, brisanje ili oštećenje podataka, ometanje normalnog rada kompjutera, prevara i falsifikovanje. Reč je o zemlji koja ima snažnu zakonodavnu aktivnost i koja je uvek među prvim sankcionisala uticaj novih tehnologija. Prikupljanje, informatička obrada i korišćenje podataka, za potrebe stvaranja različitih baza podataka, uređeno je posebnim Zakonom o zaštiti podataka iz 1978. godine. Odredbama ovog zakona uređena je obaveza svih korisnika banaka podataka, bili oni državni organi ili privatna lica, da se za svako otvaranje nove banke podataka moraju obratiti pismenim zahtevom za odobrenje državnoj Komisiji za informatiku i slobode građana, koja je ovlašćena da se brine o informacijskom samoodređivanju građana.

<i>SAD</i>	<i>Velika Britanija</i>	<i>Nemačka</i>	<i>Austrija</i>	<i>Francuska</i>	<i>SRBIJA</i>
Zakon o kompjuterskim prevarama i zloupotrebama	Zakonik o zloupotrebi kompjutera				
Zakon o privatnosti elektronskih komunikacija					
Zakon o elektronskoj špijunaži					
Zakon o iskorenjivanju računarskih virusa					
Zakon o prevenciji dečje pornografije					
Zakon o borbi protiv terorizma					
	Zakon o zaštiti podataka	Zakon o zaštiti podataka	Zakon o zaštiti podataka	Zakon o zaštiti podataka	Zakon o zaštiti podataka o ličnosti
	Zakon o krađi				
	Zakon o falsifikovanju i krivotvorenju				
	Zakon o zaštiti autorskih i srodnih prava	Zakon o autorskim delima			Zakon o autorskim i srodnim pravima
		Krivični zakon za suzbijanje privrednog kriminaliteta	Krivični zakon	Krivični zakon	Krivični zakon

Tabela 2. Pregled zakona koji regulišu kompjuterski kriminal u pojedinim zemljama

4. ZAKLJUČAK

Glavni doprinos ovog rada je komparativna analiza zakonske regulative i pravosudne prakse kompjuterskog kriminala u Republici Srbiji i nekim relevantnim zemljama. Ova analiza je pokazala da u odnosu na te zemlje, u Republici Srbiji nedostaje više zakona i regulativa. Stoga, rad stavlja akcenat na akte koje bi trebalo doneti i time obogatiti naš

pravosudni sistem. U nekim elementima Republika Srbija je bolje pravno regulisala borbu protiv kompjuterskog kriminala od većine zemalja u okruženju. Na primer, Udruženje sudskih veštaka u informacionim tehnologijama je organizovano u Srbiji, a slične nevladine organizacije nema ni u jednoj državi u našem okruženju, pa i šire.

Sa aspekta našeg zakonodavstva, usvajanjem Zakona o izmenama i dopunama Krivičnog zakona Republike Srbije, u sistem krivičnog prava uvedeno je sedam računarskih krivičnih dela, koji su za cilj imali bezbednost računarskih podataka. Kasnije donet Krivični zakon Republike Srbije, koji je stupio na snagu januara 2006. godine, predstavlja pomak u sankcionisanju kriminalnih dela u odnosu na prethodni, ali još uvek nedovoljno adekvatno rešenje. 18. marta 2009. godine Skupština Republike Srbije usvojila je odgovarajući set zakona iz oblasti visokotehnološkog kriminala i time osnažila zakonodavstvo u borbi protiv ove široko rasprostranjene pojave. Time je i naša zemlja učinila pomak, mada je neophodno, pored postojećih, doneti još čitav set zakona u cilju efikasnog suzbijanja tog krivičnog dela. Nesumnjivo najbolje rešenje bi bilo delimično prezentiranje procedura, definicija i nomenklatura od strane međunarodnih organizacija koje su ovu oblast već uredile. Takođe, najjednostavnije bi bilo prihvatanje stranih sertifikata kao validnih, te bi na taj način verovatnija bila upotreba stranog već postojećeg i nekompromitovanog kadra, koji bi na verodostojan i profesionalan način mogao da pokaže put i posluži kao odličan primer domaćem pravosuđu i organima gonjenja u procesuiranju slučajeva uz pomoć digitalne forenzike.

U Republici Srbiji postoji posebno odeljenje za borbu protiv VTK u sastavu Okružnog javnog tužilaštva u Beogradu, kao i odsek za suzbijanje kompjuterskog kriminala koji je sistematizovan u okviru Službe za borbu protiv organizovanog kriminala Uprave kriminalističke policije (SBPOK). Međutim, mana postojećih organa ogleda se u nedostatku adekvatnih profesionalnih kadrova u datoj oblasti. I dok Sjedinjene Američke Države raspolažu brojnim inovacijama, poput *Virtual Digital Evidence Lab*, otvorene od strane Nacionalnog instituta pravde, u našoj zemlji nema čak ni fizičkih laboratorija za ispitivanje digitalnih dokaza.

Ostaje nada da će primena zakonskih rešenja u velikoj meri suzbiti i preduprediti brojna protivpravna postupanja u odnosu na računar. Nesporno je da bez suočavanja sa kriminalom kao realnom, rasprostranjenom pojavom, bez preduzimanja koordiniranih aktivnosti zakonodavca i pravosudnih organa, s jedne strane, i stručnjaka za računarske tehnologije, s druge, nema načina za njegovo suzbijanje.

5. LITERATURA

- 1) Akademija za diplomatiju i bezbednost – centar za strateške studije, društvo za informatiku Srbije, Agencija „ZIPA“, *Informaciona Bezbednost*, Beograd, 2009
- 2) Cleetus, J., *Computer Forensics – Law and Privacy*, http://novalam.com/files/computer_forensics/Computer%20Forensics%20-%20Law%20and%20Privacy.ppt, 2008.
- 3) Krivični zakonik, “Službeni glasnik Republike Srbije”, br. 85/05, 29.IX 2005.
- 4) Milosavljević, M., Grubor, G., *Digitalna forenzika računarskog sistema*, Univerzitet Singidunum, 2008.

- 5) Mocas, S., *Topics in Computer Science Introduction to Digital Forensics*, Washington State University, 2009
- 6) Petrović R. S., *Kompjuterski kriminal*, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, 2001.
- 7) Zakon o autorskim i srodnim pravima, „Službeni list SCG” br. 61/04, 22.XII 2004.
- 8) Zakonik o krivičnom postupku, „Službeni glasnik Republike Srbije” br.46/06, 25.V 2006.
- 9) Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, „Službeni glasnik Republike Srbije” br. 61/05, 15.VII 2005.
- 10) Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine, „Službeni glasnik Republike Srbije”, br.47/06, 25.V 2006.
- 11) Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, „Službeni glasnik Republike Srbije”, br.19/09, 18.III 2009.
- 12) Zakon o sprečavanju pranja novca i finansiranja terorizma, „Službeni glasnik Republike Srbije” br.20/09, 18.III 2009.

COMPARATIVE ANALYSIS OF COMPUTER CRIME IN OUR AND SOME FOREIGN LEGAL SYSTEMS

Dipl. pravnik, Vanesa Polić, master diplomac, Univerzitet Singidunum

vanesapolic@gmail.com

Abstract

In this piece of work an approach to resolve computer crime problems from the legal point of view is made. It is written by a goal to enable law makers and the other experts to cope with the numbers of computer misuse and new kind of criminal. A founded and stable system of law with a strong law regulation is needed to mitigate this phenomenon. This system could contribute to ICT security from different kind of misuse and strengthen confidence to the legal system and ICT experts could introduced new security technologies and methods, knowing these are covered by law. This paper is based on a state in our law system, methods and regulations, but also on a review of foreign legal systems and their approach to resolve this serious and dispersed type of criminal. Purpose is to help the judiciary and the institutions that have emphasis on the fight against computer crime.

Key words: Computer crime, law maker, law system, law regulation, ICT security, judiciary