Zbornik
Instituta za kriminološka i
sociološka istraživanja
2007 / Vol. XXVI / 1-2 / 265-291

Originalni naučni rad
UDK: 341.48:[343.533::004

MEĐUNARODNI STANDARDI U SUPROTSTAVLJANJU KOMPJUTERSKOM (CYBER) KRIMINALU I NJIHOVA PRIMENA U SRBIJI

Borko Lepojević*
Ministarstvu odbrane Republike Srbije, Beograd

Marina Kovačević Lepojević**
Institut za kriminološka i sociološka istraživanja, Beograd

Savremene uslove života karakteriše pojava novih, složenijih oblika kriminala, koji postaju sve izraženiji i zahtevaju adekvatnu reakciju društva radi sprečavanja i ublažavanja posledica nastalih izvršenjem krivičnog dela. Kompjuterski (cyber) kriminal je kao savremen oblik kriminaliteta prepoznat i aktuelizovan u protekle dve decenije od strane različitih međunarodnih i nacionalnih institucija i organizacija. Ovaj rad ima za cilj da odredi pojam i oblike cyber kriminala, da da pregled međunarodne legislative kao osnove za adekvatnu regulaciju cyber kriminala na nadnacionalnom nivou, kao i da prikaže pravni okvir za regulaciju cyber kriminala u Srbi-

* Email: borko.lepojevic@mod.gov.yu
* *Email: marina_kov@yahoo.com

ji. Konvencijom o cyber kriminalu Saveta Evrope iz 2001. godine postavljena je osnova za adekvatnu regulaciju cyber kriminala. Pored Saveta Evrope, značajni međunarodni faktori u suprotstavljanju cyber kriminalu su: Evropska Unija, grupa G8, Ujedinjene Nacije, kao i: Svetska organizacija za zaštitu intelektualne svojine (WIPO), Svetska Trgovinska Organizacija (APEC), Svetska unija za telekomunikacije (ITU) i drugi. Srbija je 2005. godine potpisala Konvenciju o cyber kriminalu, dok njena ratifiikacija predstoji. Domaće zakonodavstvo je u značajnoj meri prilagođeno preporukama koje proizilaze iz Konvencije, dok su u cilju adekvatne implementacije stvorena odgovarajuća tela poput Posebnog tužilaštva za visokotehnološki kriminal, Posebnog odeljenja MUP-a za borbu protiv visokotehnološkog kriminala i drugih.

KLJUČNE REČI: kompjuterski (cyber) kriminal / internet / legislativa / Evropa / Srbija

UVOD

Razvoj informaciono-komunikacionih tehnologija u drugoj polovini XX i početkom XXI veka je imao snažan uticaj na sve tokove života savremenog čoveka. Informaciono društvo je postalo imperativ moderne civilizacije, nešto ka čemu se teži. Internet, kao globalna mreža računarskih sistema danas predstavlja medij preko koga se realizuju servisi elektronskog poslovanja (e-bussiness) i elektronske vlade (e-government). U tom virtuelnom prostoru koji koriste milijarde ljudi i u kome se razmenjuju ogromne količine informacija, javljaju se novi, složeni oblici kriminaliteta. Krivična dela se tako vrše u nematerijalnom prostoru, takozvanom *cyber* prostoru, korišćenjem nekonvencionalnih sredstava za izvršenje, odnosno računara. Ekonomski gubici prouzrokovani kompjuterskim kriminalitetom u SAD-u se za 2006. godinu procenjuju na 52, 5% miliona $ (Gordon, L. A., Loeb, M., Lucyshyn, W., Richardson, R., 2006: 3). Za cyber kriminal državne granice ne postoje, pa samim tim efikasna borba protiv ove

vrste kriminala zahteva međunarodnu saradnju i jedan sasvim nov i nekonvencionalan pristup. U cilju suprotstavljanja cyber kriminalu, udružuju se mnoga nacionalna zakonodavstva i međunarodne organizacije, privatni sektor kao i nevladine organizacije, sve u cilju prevencije i ublažavanja negativnih posledica.

Značajnu ulogu u međunarodnoj regulaciji cyber kriminala imaju: Evropska Unija, Savet Evrope, grupa G8, Ujedinjene Nacije, kao i organizacije koje su se ovim problemom bavile posredno, kao što su Svetska organizacija za zaštitu intelektualne svojine (WIPO), Svetska Trgovinska Organizacija (WTO) i druge. Konvencijom o cyber kriminalu Saveta Evrope iz 2001. godine postavljeni su temelji svetskoj borbi protiv visokotehnološkog kriminala i otvorene mogućnosti za adekvatniji odgovor na pojavu kompjuterskog kriminala. Veliki doprinos u borbi protiv kompjuterskog kriminala daju Industrijski sektor za proizvodnju informaciono-komunikacione opreme i Internet-servis-provajderi (ISP), koji bi trebalo da obezbede sisteme za praćenje elektronskog saobraćaja i povećaju sigurnost informacije u cyber prostoru. Razvijene zemlje su pokrenule brojne inicijative za razvoj pravne regulative i osposobljavanje policije i pravosuđa za efikasno suprotstavljanje cyber kriminalu. Primeri ovakvih napora su programi Inicijativa za elektronsku jugoistočnu Evropu, Plan za sigurniji internet, PACO program u našoj zemlji i drugi.

Krivični Zakonik Republike Srbije je dopunjen krivičnim delima iz oblasti visokotehnološkog kriminala, doneti su Zakon o elektonskom potpisu, Zakon o nadležnostima i organizaciji državnih organa za borbu protiv visokotehnološkog kriminala, Zakon o autorskom i srodnim pravima. Srbija je 2005. godine potpisala Konvenciju o cyber kriminalu Saveta Evrope, dok njena ratifikacija predstoji. Februaru 2007. godine formirano je Posebno tužilaštvo za visokotehnološki kriminal, dok se još uvek radi na formiranju Posebne službe u MUP-u namenjene za borbu protiv visokotehnološkog kriminala.

POJAM I OBLICI CYBER KRIMINALA

Da bi se razumeo pojam *cyber kriminal* potrebno je prvo odrediti prostor u kome on egzistira, a to je *cyber prostor*. Termin *cyber prostor,* po prvi put se sreće kod Vilijama Džibsona u naučno-fantastičnoj noveli *Neuromanser* (1984), pri čemu ga je autor upotrebio da prikaže nematerijalni prostor nezamislive kompleksnosti u kome računarski podaci putuju kao delići svetlosti. Danas se pod cyber prostorom podrazumeva vrsta "zajednice" sačinjene od mreže kompjutera, u kojoj se elementi tradicionalnog društva nalaze u obliku bajtova i bitova, ili prostor koji kreiraju kompjuterske mreže, odnosno globalna informaciona infrastruktura kroz koju se vrši masovna komunikacija i u kojoj istovremeno koegzistiraju virtuelno i realno (Drakulić, M., Drakulić, R., 2005: 2)

Bilo koja dva računara, odnosno, informaciono – komunikaciona uređaja, koja su povezana žičnim ili bežičnim spojem čine delić cyber prostora. Internet, kao globalna svetska mreža daje cyber prostoru globalnu karakteristiku, odnosno omogućava vezu između bilo koje dve tačke na planeti kroz cyber prostor.

Stanfordski naučno-istraživački istitut (SRI) je za potrebe Ministarstva pravde SAD izdao priručnik o kompjuterskom kriminalu u kome je data prva definicija komjuterskog kriminala pri čemu se pod kompjuterskim kriminalitetom podrazumeva *krivično delo za čije je uspešno procesuiranje potrebno poznavanje kompjuterske tehnologije*[1]. U Preporuci Saveta Evrope 1989. godine definisani su prekršaji vezani za informacione tehnologije (IT), kao *prekršaji, u čijem procesuiranju istražni organi moraju obezbediti pristup podacima obrađenim u kompjuterskim sistemima ili transmitovanim od strane računarskih sistema, ili drugih sistema za obradu elektronskih podataka*[2]. Na X Kongresu Ujedinjenih Nacija[3] u aktu *Kriminal vezan za kompjuterske*

[1] Harmonization on national legal approaches on cybercrime, ITU, WSIS Thematic meeting on Cyber security, Geneve, jun 2005 http://www.itu.int/osg/spu/forum/intgov04/contributions/itu-workshop-feb-04-internet-governance-background.pdf
[2] Recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe on 13 September 1989 and Report by the European Committee on Crime Problems: Computer-related crime. See http://cm.coe.int/ta/rec/1989/89r9.htm
[3] 10th United Nations Congress on the Prevention of Crime and the treatment of Offenders, www.oun.org

mreže kompjuterski kriminal se definiše kao *bilo koji oblik kriminala koji se može izvršavati sa kompjuterskim sistemima i mrežama, u kompjuterskim sistemima i mrežama ili protiv kompjuterskih sistema i mreža.* Konvencijom Saveta Evrope[4] o cyber kriminalu prvi put je zvanično upotrebljen termin cyber kriminal, pod kojim se podrazumeva *svaka aktivnost usmerena protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka, kompjuterskih sistema i kompjuterskih mreža kao i zloupotreba kompjuterskih podataka, sistema i mreža*. U skladu sa ovim tumačenjem cyber kriminal podrazumeva raznovrsne kriminalne aktivnosti uključujući napade na kompjuterske podatke i sisteme, napade vezane za računare, sadržaje ili intelektualnu svojinu.

U domaćoj literaturi pod cyber kriminalom (internet kriminal, e-kriminal, visokotehnološki kriminal, on-line kriminal) podrazumeva se oblik kriminalnog ponašanja u cyber prostoru, kao okruženju, u kome se računarske mreže mogu naći kao cilj, sredstvo, dokaz i /ili simbol ili okruženje izvršenja krivičnog dela (Drakulić, M., Drakulić, R., 2005: 2)

Po Konvenciji[5] o cyber kriminalu se u odnosu na kriterijum povrede cyber prostora izdvajaju sledeći oblici cyber kriminala:

- dela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema

U ovu grupu dela ubrajaju se: nezakoniti pristup, presretanje, uplitanje u podatke ili sisteme, zloupotreba uređaja, programa i šifara (neovlašćena proizvodnja, prodaja, uvoz i distribucija)

- dela vezana za kompjutere

U ovu grupu dela ubrajaju se falsifikovanje i krađa kompjuterskih podataka.

- dela vezana za sadržaje

---

[4] CoE - Convention on Cyber crime (2001) http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc
[5] CoE - Convention on Cybercrime (2001) http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc

Najčešći sadržaj koji se pojavljuje u ovoj grupi je pornografija i to maloletnička odnosno dečija pornografija, pri čemu se vrši posedovanje, distribucija, transmisija, čuvanje ili činjenje dostupnim i raspoloživim pornografskih materijala, njihova proizvodnja radi distribucije i obrade u kompjuterskom sistemu.

- dela vezana za kršenje autorskih i srodnih prava

Dela iz ove grupe tiču se neautorizovanog reprodukovanja i distribucije što se direktno nadovezuje na mogućnost zaštite autorskih prava (Berska i Rimska konvencija) i intelektualne svojine od strane svetske organizacije za intelektualnu svojinu (WIPO).

U zavisnosti od tipa kriminaliteta, koji je počinjen posredstvom računara, oblici cyber kriminala mogu se podeliti u sledeće grupe (Drakulić, M., Drakulić, R., 2005: 4)

- Politički cyber kriminalitet

Pod političkim cyber kriminalitetom podrazumevamo cyber špijunažu, haking, cyber sabotažu, cyber terorizam i cyber ratovanje.

- Ekonomski cyber kriminalitet

U ekonomski cyber kriminalitet spadaju cyber prevare, haking, krađa internet usluga i vremena, piratstvo softvera, mikročipova i baza podataka, cyber industrijska špijunaža, prevare na internet aukcijama (neisporučivanje proizvoda, lažna prezentacija proizvoda, lažna procena, nadgrađivanje cene proizvoda, udruživanje radi postizanja veće cene, trgovina robom sa crnog tržišta, višestruke ličnosti).

- Proizvodnja i distribucija nedozvoljenih i štetnih sadržaja (dečija pornografija, pedofilija, verske sekte, širenje rasističkih, nacističkih i sličnih ideja i stavova, zloupotreba žena i dece).

- Manipulacija zabranjenim proizvodima, supstancama i robama (drogom, ljudskim organima, oružje).

- Povrede cyber privatnosti

Povreda cyber privatnosti podrazumeva nadgledanje e-pošte, spam, "phishing", prisluškivanje, snimanje "pričaonica", praćenje e-konferencija, prikačinjanje i analiza "kukija" (*cookies*, eng).

Zbornik IKSI, 1-2/2007 – B. Lepojević, M. Kovačevi-Lepojević „Međunarodni standardi u suprotstavljanju kompjuterskom (cyber) kriminalu i njihova primena u Srbiji", (str. 265-291)

MEĐUNARODNA LEGISLATIVA CYBER KRIMINALA

Prva inicijativa za borbu protiv kompjuterskog kriminala pokrenuta je od strane Operacionog komiteta američkog Senata u ferbuaru 1977. godine, gde se po prvi put predlaže razvoj legislative koja se tiče kompjuterskog kriminala.

Evropska Unija je bila inicijator i vodeći nosilac međunarodne inicijative za borbu protiv visoko-tehnološkog, odnosno cyber kriminala. U periodu od 1998. do 2002. godine Evropska Unija je donela brojna dokumenta u cilju formiranja pravnog okvira za regulaciju visoko-tehnološkog kriminala, bezbednijeg cyber prostora kao i uspostavljanja bolje međunarodne kooperacije u cilju efikasnije borbe protiv cyber kriminala. Takođe, kroz mnogobrojne aktivnosti EU je definisala praktične akcije u cilju sprovođenja legislative. Studija o pravnim aspektima kompjuterskog kriminala u informacionom društvu[1] je dala značajan doprinos u određenju pojma cyber kriminala kao višeg oblika kompjuterskog kriminala. Na sastanku Evropskog Saveta[7] u Lisabonu, marta 2000. godine, pred Evropsku Uniju postavljeni su ambiciozni cilljevi u smislu tranzicije postojeće EU ekonomije, u dinamičnu i konkurentnu ekonomiju u cilju povećanja razvoja, otvaranja novih i boljih radnih mesta i kvalitetnijih socijalnih programa, u kojoj bi informaciono - komunikacione tehnologije trebalo da odigraju ključnu ulogu. U skladu sa tim ciljevima data je direktiva da se ispitaju mogućnosti nove Evropske ekonomije u kombinaciji sa internetom. Kao posledica ove direktive, sa zadatkom obezbeđivanja ciljeva sa Lisabonskog sastanka[8] juna iste godine donet je Akcioni

---

[1] Urlich Sieber *Legal Aspects of Computer-related Crime in the Information Society – COMCRIME Study*, dostupno na stranici http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc

[7] Evropski Savet,t.j. Savet Ministara Evropske Unije, nikako ne bi trebalo mešati sa Savetom Evrope, jer Evropski Savet (European Council) predstavlja najviše telo u okviru EU dok Savet Evrope predstavlja organizaciju koja, iako su njeni članovi zemlje članice EU (kao i mnoge zemlje van EU), nije telo Evropske Unije

[8] Lisabonska strategija EU, dostupno na stranici http://europa.eu/scadplus/glossary/lisbon_strategy_en.htm

plan elektronske[9] Evrope (*eEurope Action Plan*), koji pored ostalog insistira na povećanju stepena bezbednosti na mreži, sa akcentom na privatni sektor koji se bavi proizvodnjom mrežnog softvera i hardvera, kao i na poboljšavanju saradnje između nacionalnih tela za borbu protiv cyber kriminala. Direktiva o elektronskom poslovanju iz 2000. godine (*E-commerce directive*) posebno reguliše problem zloupotreba u e-trgovini na internetu. Savet donosi Odluku o sprečavanju dečije pornografije na internetu 2000. godine[10] kao i Strategiju EU za novi Milenijum[11]. Na predlog Evropskog parlamenta 2001. godine donet je akt pod nazivom *Obezbeđivanje sigurnijeg Informacionog društva kroz povećanje sigurnosti informacione infrastrukture i borbu protiv kriminala vezanog za kompjutere*[12]. Od 2001. godine, inicijativu za borbu protiv cyber kriminala, na međunarodnom nivou, preuzima Savet Evrope, dok Evropska Unija ostaje bitan činilac na ovom polju. Od mnogobrojnih akata donetih posle 2001. godine mogu se izdvojiti Predlog[13] za pravni okvir odlučivanja vezanog za napade na informacione sisteme donet 2002. godine, gde je izvršena definicija i klasifikacija vrsta napada na informacione sisteme i predložen zakonski okvir, i doneta Odluka[14] vezana za borbu protiv spam-a, spyware-a i malicioznih softvera.

Kada je praktična implementacija zakonskih rešenja u pitanju, Evropska Unija je ostala dosledna i to ne samo u oblasti svoje nadležnosti već je intenzivnim međunarodnim aktivnostima inicirala

---

[9] eEurope Action Plan 2002 http://europa.eu.int/information_society/eeurope/2002/action_plan/pdf/actionplan_en.pdf

[10] Council Decision of 29 May 2000 to combat child pornography on the Internet http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:138:0001:0004:EN:PDF

[11] European strategy for the beginning of the new Millennium, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:124:0001:0033:EN:PDF

[12] Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/ce072/ce07220020321en03230329.pdf

[13] Proposal for a Council Framework Decision on attacks against information systems http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf

[14] Council Decission on fighting spam, spyware and malicious software http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:EN:PDF

praktične poteze i drugih zemalja van Unije. Sve zemlje članice EU na svom nivou osnovale su specijalne jedinice policije za borbu protiv visoko-tehnološkog kriminala[15]. Primeri ovakvih jedinica su britanska Jedinica[16] za visokotehnološki kriminal - NHTCU (*National High Tech Crime Unit*), kao i Jedinica za tehnologije u okviru nemačke[17] federalne policije. Takođe, u skladu sa direktivama Odluke Saveta o sprečavanju dečije pornografije na Internetu i Konvencije za borbu protiv cyber kriminala, između zemalja članica EU uspostavljena je 24/7 veza između specijalizovanih tela država članica za borbu protiv dečije pornografije na internetu i cyber kriminala uopšte. Na inicijativu UNESCO-a vezanom za sigurniji internet za decu (poznatiji pod nazivim "elektronske stražarske kule"), EU od 1999. godine finansira Program za sigurniji internet[18], čija je treća faza u toku (treća faza traje od 2005. do 2008. godine), a koji ima za cilj borbu protiv nelegalnih sadržaja, promociju sigurnijeg cyber okruženja i podizanje svesti ljudi kada je internet u pitanju. Jedan od prioriteta ovog programa je formiranje call centara ("vrućih linija") u zemljama članicama, koje bi služile za prijavu nedozvoljenih i štetnih sadržaja na internetu. Pored "vrućih linija" zemalja članica EU, program obuhvata i centre za prijavu nedozvoljenih i štetnih internet sadržaja u SAD-u, Brazilu, Kanadi, Taivanu, Južnoj Koreji i Australiji. Evropska Komisija je od 1. juna 2005. godine započela program pod nazivom „Evropsko informaciono društvo za rast i zaposlenje"[19], koji predstavlja sveobuhvatnu strategiju razvoja evropskog informacionog društva do 2010 godine, u okviru koje su adresirani svi mogući izazovi i pravci razvoja informacionog društva i medija sektora EU. Ovaj program promoviše otvorenu i konkurentnu digitalnu ekonomiju u kojoj

---

[15] Nacionalne jedinice za borbu protiv cyber kriminala http://www.4law.co.il/6.html
[16] Britanska Jedinica za visokotehnološki kriminal *(National High Tech Crime Unit)* http://www.nhtcu.org/
[17] Nemačka federalna policija, Jedinica za tehnologiju http://www.bka.de/kriminalwissenschaften/forschung/ki23.htm
[18] EU Program za sigurniji internet http://www.europa.eu.int/information_society/activities/sip/index_en.htm
[19] EU Program "i2010 Evropsko informaciono društvo za rast i zaposlenje" http://ec.europa.eu/information_society/eeurope/i2010/introduction/index_en.htm

informaciono-komunikacione tehnologije predstavljaju bitan faktor. Program ima 3 glavna principa:

- Stvaranje jedinstvenog evropskog informacionog prostora, koje promoviše otvoreno i konkurentno interno tržište za informaciono društvo i medija servise
- Promovisanje i ohrabrivanje investicija u inovacije i razvoj informaciono-komunikacione tehnologije
- Pospešivanje boljih javnih servisa i kvaliteta života kroz upotrebu informaciono-komunikacione tehnologije

Od druge polovine 70-tih godina, deo aktivnosti **Saveta Evrope** bio je usmeren na prepoznavanje i definisanje visokotehnološkog kriminala kao oblika kriminalne aktivnosti, kao i usaglašavanje zakonske regulacije ove vrste kriminala u zemljama članicama. U Preporuci[21] 1989. godine definisani su sledeći oblici kriminaliteta: kompjuterska prevara, kompjutersko falsifikovanje, šteta naneta kompjuterskim sistemima ili programima, kompjuterska sabotaža, neovlašćeni pristup, neovlašćena presretanja, neovlašćena reprodukcija zaštićenih kompjuterskih programa i topografskih materijala. Takođe, u ovoj Preporuci Saveta date su dodatne smernice koje bi trebalo imati u vidu pri donošenju novih zakona u zemljama članicama. Preporuka je dopunjena 1995. godine u kojoj je dato 18 principa predstavljenih u 8 poglavlja: pronalaženje i obezbeđivanje (autentičnosti) dokaza, tehničko nadgledanje, obaveza saradnje sa istražnim organima, elektronski dokaz, korišćenje enkripcije, istraživanje, statistika, obuka i međunarodna saradnja. Kao rezultat višegodišnjih aktivnosti Saveta na ovom planu 2001. godine doneta je **Konvencija o cyber kriminalu**[20], dokument koji se uzima za osnov svetske savremene legislative koja reguliše pitanja cyber kriminala, čije su potpisnice, pored zemalja članica, SAD, Kanada, Japan i mnoge druge

[21] Recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe on 13 September 1989 and Report by the European Committee on Crime Problems: Computer-related crime. See http://cm.coe.int/ta/rec/1989/89r9.htm
[20] CoE - Convention on Cybercrime, november 20001
http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc

neevropske zemlje. Sve aktivnosti Saveta Evrope na polju borbe protiv visokotehnološkog kriminala objedinjene su u Konvenciji[22] o cyber kriminalu iz 2001. godine koju su do sada potpisale 53 zemlje, a kojom su uspostavljeni temelji međunarodnoj pravnoj regulaciji cyber kriminala. Konvencija o cyber kriminalu se sastoji iz četiri dela. U prvom delu definisani su ključni termini kao što su računarski sistem, kompjuterski podatak, servis-provajder i tako dalje. Drugi deo definiše mere koje su nacionalna zakonodavstva dužna da preduzmu u cilju donošenja zakonske regulative koja će pokriti krivična dela iz oblasti cyber kriminala. U ovom delu su definisani oblici cyber kriminala koje je potrebno zakonski regulisati i oni se dele na 4 grupe dela:

- dela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema – njih čine nezakoniti pristup, presretanje, uplitanje u podatke ili sisteme, korišćenje uređaja, programa, lozinki (proizvodnja, prodaja, uvoz, distribucija)
- dela vezana za kompjutere – kod kojih su falsifikovanje i krađe najtipičniji oblici napada
- dela vezana za sadržaje – dečija pornografija je najčešći sadržaj koji se pojavljuje u ovoj grupi obuhvatajući posedovanje, distribuciju, transmisiju, čuvanje ili činjenje dostupnim i raspoloživim ovih materijala, njihova proizvodnja radi distribucije i obrada u kompjuterskom sistemu ili na nosiocu podataka
- dela vezana za kršenje autorskih i srodnih prava obuhvataju
- neovlašćeno reprodukovanje i distribuciju zaštićenih dela (zakonima o intelektualnoj svojini i autorskom pravu) gde se kao sredstvo izvršenja javljaju kompjuterski sistemi

U ovom delu Konvencije, data je preporuka nacionalnim zakonodavstvima da definišu odgovarajuće procedure u cilju adekvatnog krivičnog postupka pri procesuiranju ovih krivičnih dela.

---

[22] Konvencija o cyber kriminalu – Zemlje potpisnice i status akta u svakoj http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=2/5/2007&CL=ENG

Takođe se traži da definišu nadležna tela (sudove) na određenim delovima svoje teritorije, u čijoj će nadležnosti biti procesuiranje krivičnih dela iz oblasti cyber kriminala. Treći deo konvencije definiše međunarodnu saradnju, gde su pored opštih principa međunarodne saradnje po ovoj krivičnoj materiji, definisani i principi ekstradicije počinilaca, generalni principi međusobne saradnje kao i principi međusobne saradnje u odsustvu adekvatnih međunarodnih ugovora. U ovom delu naglašena je obaveza svake države potpisnice da obezbedi odgovarajuće telo (*point of contact*), dostupno 24 časa 7 dana u nedelji, za kontakt i saradnju po pitanju cyber kriminala sa sličnim telima u drugim državama. Četvrti deo Konvencije sadrži završne odredbe koje se tiču pravnih aspekata konvencije: datuma otvaranja za potpis, načina stupanja na snagu, potencijalnih zemalja potpisnica i druge. Konvencija o cyber kriminalu dopunjena je 2003. godine Dodatnim protokolom[23] o kriminalizaciji dela ksenofobične ili rasističke prirode počinjenih kroz kompjuterske sisteme.

Većina zemalja potpisnica je do sada razvila odgovarajuću legislativu vezanu za procesuiranje dela iz oblasti visokotehnološkog kriminala, kao i odgovarajuća specijalizovana tela. Primer takvih tela su: u Belgiji FCCU (Federal Computer Crime Unit), u Danskoj čak postoje dva specijalizovana tela - ITSU (Information Technology Support Unit) i NCFU (National Computer Forensics Unit), SEFTI u Francuskoj (Service d'Enquête sur les Fraudes aux Technologies de l'Information) i druga. Konvenciju o cyber kriminalu do februara 2006 potpisale su 53 zemlje od kojih je u 18 zemalja (uključujući SAD) Konvencija stupila na snagu. U preostalim zemljama potpisnicama (uključujući i Srbiju) Konvencija o cyber kriminalu čeka ratifikaciju Skupštine. Savet Evrope finansirao je i finansira mnogobrojne projekte u zemljama u razvoju. Primer takvog

[23] Dodatni protokol Konvenciji o cyber kriminalu vezan za dela ksenofobije ili rasisma počinjena kroz kompjuterske sisteme (Additional protocol to the convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems), dostupno na internet stranici http://conventions.coe.int/Treaty/en/Treaties/Word/189.doc

projekta je PACO[24] projekat koji se trenutno sprovodi Srbiji. Cilj ovog projekta je borba protiv ekonomskog kriminala. Tri glavna cilja ovog projekta su:

- Reforma pravosuđa
- Učvršćivanje sistema za borbu protiv pranja novca i protiv finansiranja terorista
- Poboljšanje detekcije i prevencija cyber kriminala

U okviru aktivnosti za realizaciju trećeg cilja projekta održavaju se radionice i tematski sastanci širom Srbije, na kojima se okupljaju razni akteri, domaći i oni akreditovani od strane Saveta, diskutujući o temi cyber krimala, sve sa ciljem da naša zemlja u bliskoj budućnosti osposobi svoje institucije za efikasno suprotstavljanje visokotehnološkom kriminalu. Dobar deo ovih tematskih sastanaka i radionica posvećen je animiranju zakonodavne vlasti u Srbiji da ratifikuje Konvenciju o cyber kriminalu. U januaru 2007. godine organizovana je studijska poseta srpske delegacije Jedinici za borbu protiv visokotehnološkog kriminala Velike Britanije (NHTCU), koja je u okviru britanske Agencije za borbu protiv ozbiljnog organizovanog kriminala (SOCA).

G-8, grupa koju čini osam najrazvijenijih zemalja sveta, dala je snažan doprinos u svetskoj borbi protiv cyber kriminala. Međutim, taj značaj se ne ogleda toliko u pravnoj regulaciji visokotehnološkog kriminala, koliko u iniciranju i implementaciji praktičnih rešenja i uspostavljanju efikasnije međunarodne saradnje u borbi protiv visoko-tehnološkog kriminala, pa i cyber kriminala. Na sastanku ministara pravde i policije G-8 u Vašingtonu, posvećenom cyber-kriminalu, definisano je deset principa[25] za borbu protiv cyber kriminala, i to su:

1. Ne sme biti sigurnog mesta (*safe-heaven*, eng) na svetu za one koji zloupotrebljavaju informacione tehnologije

---

[24] PACO Projekat u Srbiji (*Project against economic crime*)
http://www.jp.coe.int/CEAD/JP/Default.asp?ProgrammeID=84&SA=1#TopOfList
[25] 10 Principa i Akcioni Plan G-8 za borbu protiv Cyber kriminala, Washington D.C. 1997
http://www.usdoj.gov/criminal/cybercrime/g82004/97Communique.pdf

2. Saradnja u istražnom postupku mora postojati između svih zemalja nezavisno od toga gde je pričinjena šteta
3. Policija mora imati adekvatnu obuku i opremu da bi se suprotstavlljala visokotehnološkom kriminalu
4. Pravosuđa zemalja moraju zaštiti poverljivost, integritet i dostupnost podataka i sistema od neovlašćenog pristupa i obezbediti kažnjavanje svake zloupotrebe
5. Pravosuđa zemalja moraju omogućiti očuvanje podataka i brz pristup istima, što je često od presudnog značaja za uspešnu istragu
6. Principi međusobne pomoći među zemljama moraju obezbediti brzo prikupljanje i razmenu podataka u slučajevima međunarodnog visoko-tehnološkog kriminala
7. Elektronski pristup organa policije jedne države podacima sa otvorenim kodom (*open-source*, eng) koji se nalaze na teritoriji druge države ne zahteva dozvolu za pristup države na čijoj se teritoriji podaci nalaze
8. Forenzički standardi za sakupljanje i autentifikaciju računarskih podataka moraju biti razvijeni i implementirani na nivou svih država.
9. Informacioni i telekomunikacioni sistemi moraju omogućiti prevenciju i detektovanje zloupotreba mreže, i moraju u sebi sadržati sisteme za praćenje ovakvih napada i prikupljanje podataka.
10. Aktivnosti na ovom polju moraju biti koordinisane da bi se izbegla bilo kakva redundansa i dupliranje posla.

Sa namerom da podrži ovih 10 principa definisan je akcioni plan G-8 za suprotstavljanje visoko-tehnološkom kriminalu, koji predstavlja direktive za praktičnu implementaciju navedenih principa. Oktobra 1999. godine na sastanku ministara pravde i policije G-8 u Moskvi, posvećenom visokotehnološkom kriminalu i finansijskim aspektima transnacionalnog kriminala, donet je akt pod nazivom *Principi*

transgraničnog (međunarodnog) pristupa skladištenim kompjuterskim podacima[26], u kome su razrađeni principi ubrzane međusobne saradnje država po pitanjima očuvanja i pristupa podacima. Naglašena je potreba za unapređivanjem legislative zemalja članica G-8, koja bi bila neophodna za uspešno procesuiranje krivičnih dela iz oblasti visoko-tehnološkog kriminala kao i potreba za sprečavanjem zloupotreba interneta u smislu napada na bankarske elektronske sisteme i "rasturanje" štetnih sadržaja kao što je dečija pornografija. Istaknut je i značaj saradnje sa industrijskim sektorom koji bi trebalo da obezbedi mehanizme za prevenciju i detekciju napada i mehanizme za efikasno i brzo sakupljanje elektronskih dokaza, kao i potreba za širenjem 24/7 mreže za međunarodnu saradnju u realnom vremenu po pitanjima cyber kriminala, kao neophodnog sistema za efikasnu borbu protiv visoko-tehnološkog kriminala, kao oblikom transnacionalnog kriminala. U saopštenju sa sastanka u Milanu februara 2001[27] još jednom se naglašava značaj efikasne borbe protiv visokotehnološkog kriminala, naročito dečije pornografije, i daje podrška svim institucijama i telima koje su u okviru G-8 (Lyon grupa) i van G-8 (podrška Savetu Evrope u istrajnosti na izradi Konvencije za borbu protiv cyber-kriminala, podrška japanskoj inicijativi za održavanje drugog svetskog samita o zaštiti prava deteta u smislu borbe protiv dečije pornografije na internetu, itd.). Takođe se u ovom saopštenju, daje direktiva ekspertima G-8 da razmotre mogućnost formiranja baze podataka G-8 (koja bi bila u nadležnosti Italije u smislu održavanja) vezanoj za krivična dela iz oblasti dečije pornografije na internetu. Sastanak ministara pravde i policije u Mont Tremblant-u (Kanada) u maju 2002. godine, bio je vrlo plodan po broju donetih akata, od kojih su po pitanju suprotstavljanja visokotehnološkom kriminalu, najbitniji: Preporuke za praćenje mrežnih komunikacija preko nacionalnih granica u cilju pomoći pri procesuiranju krivičnih

---

[26] Principi trans-graničnog pristupa skladištenim računarskim podacima, G-8, Moskva, Oktobar 1999, http://www.usdoj.gov/criminal/cybercrime/g82004/99TransborderAccessPrinciples.pdf

[27] Saopštenje sa sastanka ministara pravde i policije u Milanu, februar 2001 http://www.g8.utoronto.ca/adhoc/justice2001.htm

dela iz oblasti terorizma i drugih; Prinicipi dostupnosti podataka važnih za očuvanje javne bezbednosti; Lista za očuvanje podataka; i Izjava G-8 po pitanju regulisanja zaštite podataka. Cilj ovih dokumenata su: poboljšanje saradnje među državama, u smislu omogućavanja međunarodnog praćenja i nadzora elektronskog saobraćaja, razvoj odgovarajuće legislative na nacionalnom nivou, koja bi omogućila istražnim organima da zatraže elektronske podatke (e-mail-ove lične podatke korisnika) od provajdera kada to istražni postupak zahteva i definisanje procedura koje omogućavaju nepovredivost autentičnosti elektronskih podataka koji su od značaja u istražnom postupku. Jedno od najznačajnih doprinosa G-8 u svetskoj borbi protiv cyber-kriminala jeste formiranje 24/7 mreža za kontakt i saradnju iz oblasti cyber kriminala, čiji je idejni tvorac i glavni implementor bila podgrupa za visokotehnološki kriminal Lyon grupe. Ova mreža danas broji preko 40 zemalja članica i predstavlja osnov međunarodne saradnje u borbi protiv cyber kriminala. Aktivnosti grupe najrazvijenijih zemalja sveta po pitanju visokotehnološkog kriminala postoje svake godine, jer je borba protiv ovog kriminala jedna od ključnih tema sastanaka ministara na godišnjem samitu G-8.

Ujedinjene Nacije su kroz nekoliko rezolucija Generalne Skpštine istakle problem visoko-tehnološkog kriminala, izraživši svoju zabrinutost vezanu za zloupotrebu informaciono-komunikacionih tehnologija i naglasivši potrebu za sigurnijim cyber prostorom. Mnoga tela u okviru UN sprovela su značajna istraživanja ove problematike i inicirala dijalog u određenim oblastima kao što su zaštita od spam-a i sigurnost informacije u cyber prostru i slično. Na VIII Kongresu UN posvećenom kriminalu, održanom u Havani 1990. godine UN su usvojile Rezoluciju o regulaciji kompjuterskog kriminala. Na temu *Razvoj informacija i telekomunikacija u kontekstu međunarodne bezbednosti* Generalna skupšina UN je donela 6 rezolucija [9]: 53/70 od 04.12.1998, 54/49 od 01.12.1999, 55/28 od 20.11.2000, 56/19 od 29.11.2001, 57/53 od 22.11.2002 i 58/32 od 18.12.2003. U njima je istaknuta mogućnost zloupotrebe informaciono-komunikacionih tehnologija u svrhe suprotne principima UN, pa je stoga potrebno da sve zemlje sprovedu mere u ovoj oblasti u cilju prevencije i smanjenja štete nastale ovim

zloupotrebama. Takođe je odobreno stvaranje posebne UN ekspertske grupe koja bi podrobnije ispitala oblast zloupotreba informaciono-komunikacionih tehnologija. U drugoj grupi rezolucija donetih 2000 (56/43 od 04.12) i 2001(56/121 od 19.12), pod nazivom *Borba protiv kriminalnih zloupotreba informacionih tehnologija*[28] date su preporuke državama za suprotstavljanje novim oblicima kriminala. Prvi korak UN u implementaciji odredaba protiv cyber kriminala je bio stvaranje ekspertske grupe od 15 članova, sa namerom da detaljno ispita oblast zloupotreba IKT i Generalnoj Skupštini predoči dalje perspektive rešavanja ovog problema. Na poslednja četiri UN kongresa posvećena prevenciji kriminala i tretmanu počinilaca jedna od tema je bio je i cyber kriminal.

OSTALI MEĐUNARODNI FAKTORI REGULACIJE CYBER KRIMINALA

Pored Evropske Unije, Saveta Evrope, grupe G-8 i Ujedinjenih Nacija, doprinos u regulaciji cyber kriminala daju i Svetska organizacija za zaštitu intelektualne svojine (WIPO), Svetska Trgovinska Organizacija (WTO), Azijsko-Pacifička organizacija za ekonomsku saradnju (APEC), Svetska unija za telekomunikacije (ITU), Organizacija za ekonomsku saradnju i razvoj (OECD) i Komonvelt.

Svetska trgovinska organizacija je istakla problem cyber kriminala, a posebno zloupotrebu interneta u elektronskoj trgovini. Na Konferenciji[29] APEC-a u Meksiku 2002. godine prihvaćena je inicijativa za razvoj grupe zakona za suprotstavljanje visokotehnološkom kriminalu, koji će se primenjivati u okviru organizacije i koji će biti u skladu sa Rezolucijom UN 55/63 iz 2000. godine i Konvencijom o cyber kriminalu Saveta Evrope iz 2001. godine. Još 1983. godine OECD je

[28] Harmonization on national legal approaches on cybercrime, ITU, WSIS Thematic meeting on Cyber security, Geneve, jun 2005 http://www.itu.int/osg/spu/forum/intgov04/contributions/itu-workshop-feb-04-internet-governance-background.pdf

[29] Harmonization on national legal approaches on cybercrime, ITU, WSIS Thematic meeting on Cyber security, Geneve, jun 2005 http://www.itu.int/osg/spu/forum/intgov04/contributions/itu-workshop-feb-04-internet-governance-background.pdf

prepoznala zloupotrebu računarskih sistema i mreža kao kriminalnu aktivnost u sve većoj ekspanziji i oformila ekspertski komitet sa ciljem da istraži ovu oblast i da predlog za dopunu pravnih sistema u cilju efikasnog procesuiranja krivičnih dela visokotehnološkog kriminala. ITU je u saradnji sa UN dala doprinos kroz iniciranje Svetskog samita o informacionom društvu, kao i zalaganje na usaglašavanju državnih regulacija, insistiranje na efikasnijoj međunarodnoj saradnji i dijalogu sa industrijskim sektorom u cilju razvoja sigurnijeg cyber prostora. Zemlje članice Komonvelta su 2002. godine pokušale da usklade svoje zakone po pitanju regulacije cyber kriminala kroz dokument *Krivična dela vezana za kompjutere* koji ima sličan okvir kao i Konvencija o cyber kriminalu Saveta Evrope. Treba istaći doprinos akademskih ustanova i istraživačkih tela, kao što je Virzburški Univerzitet u Nemačkoj i Stanford Univezitet koji ulažu značajne napore u borbi protiv cyber-kriminala.

PRAVNI OKVIR ZA REGULACIJU CYBER KRIMINALA U SRBIJI

Cyber kriminal je na teritoriji Srbije dugo imao "sigurno utočište" (*safe-heaven,* eng), odakle se najčešće delovalo, dok se šteta pričinjavala u drugim delovima sveta. Početak regulacije cyber kriminala započinje 2005. godine kada je Srbija potpisala Konvenciju o cyber kriminalu, dok se ratifikacija ovog dokumenta od strane Skupštine Srbije još čeka. Krivičnim Zakonikom iz 2005. godine predviđena su krivična dela protiv bezbednosti računarskih podataka, krivična dela protiv intelektualne svojine i krivična dela vezana za dečiju pornografiju. Zakonom o organizovanju i nadležnostima državnih organa za borbu protiv visokotehnološkog kriminala, predviđeno je formiranje posebnih policijskih, sudskih organa i organa tužilaštva. Početak implementacije donete legislative je nastupio godinu dana nakon potpisivanja Konvencije o cyber kriminalu. U Prvom Okružnom sudu u Beogradu formirano je Posebno odeljenje za borbu protiv visokotehnološkog kriminala, dok je marta 2007. godine formirano Posebno tužilaštvo i imenovan prvi Posebni tužilac

U Krivičnom Zakoniku Republike Srbije, u glavi XXVII navode se dela iz oblasti cyber kriminala, pod nazivom "Krivična dela protiv bezbednosti računarskih podataka"[30] u čiju grupu spadaju: oštećenje računarskih podataka i programa, računarska sabotaža, pravljenje i unošenje računarskih virusa, računarska prevara, neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka, sprečavanje i ograničavanje pristupa javnoj računarskoj mreži i neovlašćeno korišćenje računara ili računarske mreže. Najstrožije je sankcionisana računarska prevara u cilju sticanja protivpravne imovinske koristi, sa zakonskim maksimumom zaprećene kazne od 10 godina zatvora, kao i računarska sabotaža za koju ne postoji opcija plaćanja novčane kazne, dok je zakonski masksimum za zatvorsku kaznu 5 godina. Glava XX tretira krivična dela protiv intelektualne svojine. U članu 199, stavovima 1. i 2., zatvorskom kaznom do tri godine kažnjava se neovlašćeno objavljivanje, snimanje, umnožavanje, ili na drugi način javno saopštavanje u celini ili delimično autorskog dela, interpretacije, fonograma, videograma, emisije, računarskog programa ili baze podataka. Istom kaznom se kažnjava onaj koji, u cilju stavljanja u promet, drži umnožene ili neovlašćeno stavljene u promet primerke autorskog dela. Ukoliko se ovo krivično delo vrši u cilju pribavljanja imovinske koristi za sebe ili drugog, može biti izrečena zetvorska kazna u trajanju do pet godina. Član 185, u glavi XVIII, odnosi se na krivična dela prikazivanja pornografskog materijala i iskorišćavanja dece za pornografiju. U stavu 1. navodi se da se *svako ko detetu proda, prikaže ili na drugi način učini dostupnim tekstove, slike, audio-vizuelne ili druge predmete pornografske sadržine ili mu prikaže pornografsku predstavu može kazniti novčanom kaznom ili kaznom zatvora u trajanju do 6 meseci.* Iskorišćavanje deteta za proizvodnju pornografskih materijala (stav 2.) u bilo kom obliku kažnjava se zatvorom od 6 meseci do 5 godina, a prodaja, elektronsko ili bilo kakvo drugo izlaganje, t.j., činjenje dostupnim materijala nastalih na ovaj način (našin iz stava 2.) dodatno se kažnjava zatvorskom kaznom

[30] Krivični zakonik Republike Srbije http://www.parlament.sr.gov.yu/content/cir/akta/akta_detalji.asp?Id=285&t=Z

do dve godine. Samo posedovanje materijala sa dečijom pornografijom u bilo kom obliku (slike, audio i video zapisi) po ovom članu nije kažnjivo i po mnogima predstavlja nedostatak u domaćoj regulaciji kriminala vezanog za dečiju pornografiju.

Zakon o organizovanju i nadležnostima državnih organa za borbu protiv visoko- tehnološkog kriminala[31] donet je kao jedan korak u sprovođenju principa Konvencije o cyber kriminalu Saveta Evrope, po kojem bi svaka zemlja potpisnica Konvencije trebalo da formira specijalizovana tela u sudstvu i organima unutrašnjih poslova u cilju suprotstavljanja visokotehnološkom kriminalu, pod kojim se u smislu ovog zakona podrazumeva vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku. Zakon je stupio na snagu 15. jula 2005. godine. Pomenuti Zakon predviđa formiranje Odeljenja za borbu protiv visokotehnološkog kriminala u okviru Okružnog javnog tužilaštva u Beogradu, pod nazivom "Posebno tužilaštvo". Radom posebnog tužilaštva rukovodi Posebni tužilac, koga imenuje Republički javni tužilac iz redova javnih tužilaca i zamenika javnih tužilaca na mandat od 4 godine, uz mogućnost ponovnog postavljenja. U okviru MUP predviđa se formiranje Službe za borbu protiv visokotehnološkog kriminala, koja bi bila nadležna za unutrašnje poslove iz oblasti visokotehnološkog kriminala. Služba bi postupala po zahtevu Posebnog tužioca u skladu sa zakonom. Zakon takođe predviđa formiranje Veća za borbu protiv visokotehnološkog kriminala za postupanje u predmetima krivičnih dela iz ove oblasti. Sudije u Veće raspoređuje Predsednik Okružnog suda u Beogradu, iz redova sudija tog suda, i uz njihovu saglasnost. Prostorije i uslove za rad Posebnog tužilaštva i Veća obezbeđuje Ministarstvo pravde, a sredstva za rad Posebnog tužilaštva, Službe i Veća obezbeđuju se iz budžeta Republike Srbije.

---

[31] Zakon o organizovanju i nadležnostima državnih organa za borbu protiv visoko-tehnološkog kriminala http://www.parlament.sr.gov.yu/content/cir/akta/akta_detalji.asp?Id=233&t=Z

Cyber kriminal se posredno može regulisati i Zakonom o patentima, Zakonom o autorskom i srodnim pravima i Zakonom o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine. U članu 5 našeg Zakona o patentima[32], izrađenog u skladu sa Evropskom konvencijom o patentima[33], gde se definišu patentibilni proizvodi, kaže se da se ne mogu patentirati: otkrića, naučne metode i matematičke metode, estecke kreacije, planovi, pravila i postupci za obavljanje intelektualnih delatnosti, za igranje igara ili za obavljanje poslova, programi računara i prikazivanje informacija. Ipak, iako se prema važećim zakonima kod nas i u EU računarski program ne može proglasiti patentom (ovo je moguće u Japanu i SAD), Evropska Organizacija za patente (EPO) ipak ostavlja prostora za selektivnu primenu ovog pravila, u slučajevima kada računarski program ima vidljiv "tehnički efekat" i rešava tehnički problem na nov i ne-očigledan način (npr. programi koji kontrolišu automatizovane procese u industriji)[34]. Obzirom da se ne mogu patentirati, računarski programi se kod naš štite autorskim pravom. Po domaćem Zakonu o autorskom i srodnim pravima[35], autorskim delom smatra se računarski program u bilo kom obliku njegovog izražavanja, uključujući i pripremni materijal za njegovu izradu. Zakonom o posebnim ovlašćenjima[36] radi efikasnije zaštite prava intelektualne svojine, koji je na snazi od 25.maja 2006. godine, određuju se posebna ovlašćenja organa državne uprave u smislu zaštite prava intelektualne svojine, u skladu sa važećim propisima kojima se uređuje pravo intelektualne svojine. U članu 11. ovog zakona pridodata je nadležnost Ministarstvu finansija, da preko poreskih inspektora i poreske policije, utvrđuje da li

---

[32] Zakon o patentima
http://www.yupat.sv.gov.yu/pdf/ser/propisi/patenti/patenti_zakon.pdf

[33] Evropska konvencija o patentima http://www.european-patent-office.org/legal/epc/e/ma1.html#CVN

[34] Evropska kancelarija za patente – Stav o patentiranju računarskih programa i poslovnih metoda http://www.european-patent-office.org/news/pressrel/2000_08_18_e.htm

[35] Zakon o autorskom i srodnim pravima http://www.yupat.sv.gov.yu/pdf/ser/propisi/autorsko/autorsko_zakon.pdf

[36] Zakonom o posebnim ovlašćenjima radi efikasnije zaštite prava intelektualne svojine http://www.parlament.sr.gov.yu/content/cir/akta/akta_detalji.asp?Id=359&t=Z

postoji povreda prava intelektualne svojine, naročito prava na računarske programe i baze podataka. Novčane kazne za povredu prava intelektualne svojine na autorska dela koja uključuju i računarske programe i baze podataka kreću se od 100.000 do 3.000.000 dinara.

Elektronski potpis potvrđuje identitet pošiljaoca poruke kao i autentičnost i integritet elektronskih dokumenata. Jedinstven za pošiljaoca i za poruku koja se šalje, elektronski potpis se može verifikovati i ne može se poreći. Druga važna prednost koju elektronski potpis pruža je to što on osigurava da su učesnici u transakciji upravo oni za koje se predstavljaju. Za razliku od pravog potpisa pisanog rukom, elektronski potpisi ne samo da identifikuju pošiljaoca elektronske poruke već i osiguravaju da se sadržaj poruke ne menja u toku prenosa. Domaći Zakon o elektronskom potpisu[37] na snazi je od 21. decembra 2004. godine. Osnovni ciljevi Zakona su u zakonskom izjednačavanju u pravnom sistemu pisane i elektronske forme dokumenta, odnosno elektronskog i svojeručnog potpisa. Osnovno zakonsko opredeljenje je da kvalifikovan elektronski potpis, formiran u skladu sa zakonom, u odnosu na podatke u elektronskom obliku ima istu pravnu snagu kao svojeručni potpis odnosno svojeručni potpis i pečat u odnosu na podatke u papirnom obliku i da je prihvatljiv kao dokaz u pravnim poslovima. Neposredni cilj zakona je da reguluše tehničke postupke i faze koje se izvode prilikom generisanja sertifikata i njihove distribucije tako da elektronski potpis postane pravosnažan dokaz u sudu. Zakon dozvoljava upotrebu elektronskog i kvalifikovanog elektronskog potpisa. Te dve kategorije potpisa razlikuju se po pravnom dejstvu koje imaju u pravnom prometu. U skladu sa odredbama zakona samo kvalifikovani elektronski potpis proizvodi pravno dejstvo kao svojeručni potpis. Definisani su uslovi koji treba da zadovoljava kvalifikovani elektronski potpis kao potpis koji garantuje identitet potpisnika i integritet elektronskog dokumenta, prihvatljivost kvalifikovanog elektronskog potpisa kao dokaznog

[37] Zakon o elektronskom potpisu http://www.parlament.sr.gov.yu/content/cir/akta/akta_detalji.asp?Id=190&t=Z

materijala u pravnim poslovima, osobine koje moraju da poseduju sredstva za formiranje kvalifikovanog elektronskog potpisa kako bi se obezbedila sigurnost i pouzdana zaštita od falsifikovanja, kao i osobine koje treba da poseduju sredstva za proveru kvalifikovanog elektronskog potpisa kako bi se pouzdano utvrdila autentičnost korisnika i bilo koja izmene u podacima.

Uredbom[38] o obezbeđivanju i zaštiti informacionih sistema državnih organa objavljenoj u Službenom glasniku SRS, broj 41 1990. godine utvrđene su mere obezbeđenja i zaštite informacionih sistema (IS) državnih organa zasnovanih na primeni računara, kao i način njihovog sprovođenja. Navedeno je da mere mogu biti organizacione i tehničke i bliže je određeno na šta se one odnose. Pored osnovnih odredbi ostala poglavlja Uredbe sadrže mere obezbeđivanja i zaštite: pri projektovanju IS (u okviru svake projektne celine), pri operativnom radu IS, mere zaštite podataka, mere obezbeđivanja i zaštite prostorija u kojima je smeštena računarska oprema, mere obezbeđivanja i zaštite računarske opreme, mere zaštite programske podrške, mere zaštite u računarskim mrežama i ostali uslovi za uspešno funkcionisanje IS.

Sve zemlje članice EU, kao i zemlje kandidati, izradile su nacionalne strategije razvoja informacionog društva. Zemlje jugoisočne Evrope, po ugledu na inicijativu EU, pokrenule su sopstvenu inicijativu, u okviru Pakta za stabilnost jugoistočne Evrope, pod nazivom "Elektronska jugoistočna Evropa", sa ciljem da odgovore na izazove koje donosi razvoj informacionog društva, iskoriste sve potencijale koje pruža moderna IKT i povećaju mogućnost integracije svojih privreda u svetsko tržište. Na konferenciji *Telekomunikacije za razvoj* koja je održana u Beogradu 29. oktobra 2002. godine, zemlje jugoistočne Evrope (Albanija, Bosna i Hercegovina, Hrvatska, BJR Makedonija, Moldavija, Srbija i Crna Gora) prihvatile su i potpisale međunarodni sporazum „Agenda e-JIE za razvoj informacionog društva" (Agenda e-JIE)[39], kao osnovni dokument za razvoj informacionog društva u ovom

[38] Strategija razvoja informacionog društva Republike Srbije http://www.dis.org.yu/www1/nauka_strategija_id.pdf
[39] Inicijativa za elektronsku jugoistoičnu Evropu http://www.eseeinitiative.org/

regionu. Ovaj sporazum je u skladu s akcionim planovima e-Evropa 2002 i 2005 i planom e-Evropa za zemlje kandidate i predstavlja potvrdu spremnosti zemalja jugoistočne Evrope da rade na razvoju informacionog društva u skladu s razvojnim procesima IT u Evropi. Ovaj dokument su takođe prihvatile zemlje članice Procesa saradnje u jugoistočnoj Evropi (SEECP) marta 2003. godine na samitu održanom u Beogradu. Strategija razvoja informacionog društva u Srbiji[40] usvojena u oktobru 2006. godine sa ciljem da se:

- unapredi stanje u oblasti informaciono-komunikacionih tehnologija (IKT)
- razjasne uloge, izgradi partnerstvo između privatnog i javnog sektora i olakša učešće svih ključnih aktera, uključujući i nevladine organizacije (NVO)
- usmeri postojeća oskudna sredstva na korišćenje IKT za nacionalne prioritete i pomogne utvrđivanje dinamike dopunskih ulaganja
- upotpuni uticaj tržišta, promoviše društvene promene, omogući lokalnu inicijativu, osigura zajedničko učenje i omogući širenje uspešnih rešenja,
- ukaže na posebne potrebe i snagu važnih delova IKT industrije za izvoz i konkuretnost privrede,
- preusmeri nacionalni sistem inovacija da zadovolji suštinske i dugoročne tehnološke zahteve, IKT (kao tehnologije opšte namene),
- ukaže na propuste u koordinaciji, istraži mrežne efekte i obezbedi dopunskaulaganja za korišćenje IKT kao infrastrukture koja osposobljava i pruža potrebne usluge

U glavi 4. koja se tiče zakonskog okvira informacionaog društa, naglašena je potreba za zakonodavstvom koje će omogućiti

[40] Strategija razvoja informacionog društva Republike Srbije http://www.dis.org.yu/www1/nauka_strategija_id.pdf

bezbednu razmenu informacija na internetu, zaštitu ličnih podataka i privatnosti, prenos informacija kroz međunarodne sisteme, kriptografsku zaštitu i zaštitu korisnika od uvredljivog, nezakonitog i neželjenog internet sadržaja. Preporuka je da bi novi zakoni morali da pruže zaštitu od terorizma, pranja novca, zaštitu intelektualnih prava, kao i propise koji regulišu internet sadržaj. Za kupovinu i prodaju putem interneta trebalo bi obezbediti odgovarajući pravni okvir. Istaknuta je potreba za ratifikacijom Konvencije o cyber kriminalu Saveta Evrope, kao bitnog koraka na putu ka usklađivanju domaćeg uređenja sa EU regulativom, a radi sprečavanja zloupotreba u oblasti informaciono-komunikacionih tehnologija. Ratifikacija ovog dokumenta predstavlja jedan od 5 prioriteta državne politike po Agendi za razvoj informacionog društva u jugoistočnoj Evropi u cilju bržeg razvoja informacionog društva u zemlji i regionu.

LITERATURA:

(1) CoE - *Convention on Cyber crime* (2001) http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc

(2) Drakulić, M., Drakulić, R. (2005) *Cyber kriminal*, Fakultet organizacionih nauka, www.bos.org.y/cepit/drustvo/sk/cyberkriminal

(3) *Europe Action Plan* 2002 http://europa.eu.int/information_society/eeurope/2002/action_plan/pdf/actionplan_en.pdf

(4) *Evropska konvencija o patentima* http://www.european-patent-office.org/legal/epc/e/ma1.html#CVN

(5) *European strategy for the beginning of the new Millennium*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:124:0001:0033:EN:PDF

(6) *EU Program za sigurniji internet* http://www.europa.eu.int/information_society/activities/sip/index_en.htm

(7) Gordon, L. A., Loeb, M., Lucyshyn, W., Richardson, R., (2006) *Computer Crime and Security Survey,* FBI/SCI http://americas.utimaco.com/encryption/fbi_csi_2006_p3.html

(8) *Konvencija o cyber kriminalu – Zemlje potpisnice i status akta u svakoj* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=2/5/2007&CL=ENG

(9) *Krivični zakonik Republike Srbije* http://www.parlament.sr.gov.yu/content/cir/akta/akta_detalji.asp?Id=285&t=Z

(10) *Lisabonska strategija EU,* dostupno na stranici http://europa.eu/scadplus/glossary/lisbon_strategy_en.htm

(11) *Recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe on 13 September 1989 and Report by the European Committee on Crime Problems: Computer-related crime,* http://cm.coe.int/ta/rec/1989/89r9.htm

(12) *Strategija razvoja informacionog društva Republike Srbije* http://www.dis.org.yu/www1/nauka_strategija_id.pdf

(13) *Zakon o organizovanju i nadležnostima državnih organa za borbu protiv visoko- tehnološkog kriminala* http://www.parlament.sr.gov.yu/content/cir/akta/akta_detalji.asp?Id=233&t=Z

(14) *Zakon o patentima* http://www.yupat.sv.gov.yu/pdf/ser/propisi/patenti/patenti_zakon.pdf

(15) *Zakon o autorskom i srodnim pravima* http://www.yupat.sv.gov.yu/pdf/ser/propisi/autorsko/autorsko_zakon.pdf

(16) *Zakonom o posebnim ovlašćenjima radi efikasnije zaštite prava intelektualne svojine* http://www.parlament.sr.gov.yu/content/cir/akta/akta_detalji.asp?Id=359&t=Z

(17) *Zakon o elektronskom potpisu* http://www.parlament.sr.gov.yu/content/cir/akta/akta_detalji.asp?Id=190&t=Z

Zbornik IKSI, 1-2/2007 – B. Lepojević, M. Kovačevi-Lepojević „Međunarodni standardi u suprotstavljanju kompjuterskom (cyber) kriminalu i njihova primena u Srbiji”, (str. 265-291)

INTERNATIONAL STANDARDS ON HIGH-TECH (CYBER) CRIME AND THEIR IMPLEMENTATION IN SERBIA

Contemporary life conditions are followed with new, complex tipes of crime, demanding propriate society reaction in order to prevent or diminish consequences caused by thiese new types of crime. High-tech (cyber) crime has been recognized as criminal behavior and placed into a focus of many national and internationl institutions and organizations in passed two decades. This paper is aimed to determine the term and forms of the cyber crime, as well as to give a preview of international legislation, as a base of propriate adressing of cybercrime. Cybercrime convention presented in 2001 by Council of Europe, stands as pillar combating the cybercrime. Besides CoE, significant contribution combaiting cybercrime gave international actors such as European Union, G8, UN, WIPO, ITU and WTO. Serbia signed Cybercrime convention in 2005, but ratification of this document hasn't been done yet. Domestic legislation has been already adopted to the Convention recomendations, as well as institutions for cybercrime's legislative implementation like Speciall prosecution for high-tech crime, Ministry of Interrior speciall dept. for combating high-tech crime and others.

*KEY WORDS**:** high-tech (cyber) crime / interne / legislation / Europe / Serbia*