

KOMPJUTERSKO PRAVO

Ljuba Slijepčević,
Pravosudna akademija
Novi Sad

Visokotehnološki kriminal u domaćim i međunarodnim propisima, s posebnim osvrtom na odredbe Krivičnog zakonika koje su stupile na snagu od 1.juna 2017. i Konvenciju Saveta Evrope o visokotehnološkom kriminalu

Uvod

Visokotehnološki kriminal je vrsta kriminala kod kojeg su informaciono-komunikacione tehnologije (IKT) objekat krivičnog dela ili sredstvo izvršenja krivičnog dela. Početkom devedesetih godina prošlog veka, u sektoru delatnosti globalne tehnologije informacija i komunikacija započeta je značajna transformacija usvajanjem tehnologija baziranih na kompjuterskim sistemima. Ove tehnologije postavile su pred organe reda širom svijeta, nove, složene izazove. Pojava i nagli porast kompjuterskog kriminala ima značajne implikacije za vlade i građane širom sveta.

INTERPOOL je organizovao prvu seminarsku obuku posvećenu suzbijanju kompjuterskog kriminaliteta 1981. godine.

Ta vrsta kriminala je u rapidnom porastu. Zbog toga je u zakonodavstvima zemalja širom sveta, pa i u Srbiji bilo neophodno inkriminisati napade na IKT, odnosno napade gde se IKT koriste kao sredstvo izvršenja krivičnog dela. Isto tako, bilo je neophodno uspostaviti specijalizovane organizacione jedinice u državnim i međunarodnim organima koje bi učestvovala u istražnom postupku, procesuiranju i suđenju za ova krivična dela.

Zakonodavna regulativa u Republici Srbiji –v isokotehnološki kriminal

Zakonodavni okvir u Republici Srbiji regulisan je sledećim zakonskim odredbama Zakon o organizaciji i nadležnosti državnih organa za borbu protiv sajber kriminala,

- Krivični zakonik,
- Zakon o odgovornosti pravnih lica za krivična dela,
- Zakonik o krivičnom postupku,
- Zakon o policiji,
- Zakon o autorskim i srodnim pravima,
- Zakon o telekomunikacijama,
- Zakon o elektronskom potpisu,
- Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine
- Pravilnik o uslovima za pružanje internet usluga i sadržaju odobrenja.

- Zakon o posebnim merama za sprečavanje vršenja krivičnih dela protiv polne slobode prema maloletnim licima
- Zakon o informacionoj bezbednosti
- Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija

Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima uređuje postupak pružanja međunarodne pravne pomoći u krivičnim stvarima u slučajevima kada ne postoji potvrđeni međunarodni ugovor, ili kada određena pitanja njime nisu uređena

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala predstavlja specifičnost Republike Srbije i primenjuje se radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela protiv bezbednosti računarskih podataka, intelektualne svojine, imovine, privrede i pravnog saobraćaja, kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj primeraka autorskih dela prelazi 2000 ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara;

krivična dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, koja se zbog načina izvršenja ili upotrebljenih sredstava mogu smatrati krivičnim delima visokotehnološkog kriminala.

Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala iz 2005. godine, osnovano je Posebno tužilaštvo za borbu protiv visokotehnološkog kriminala. Ovo tužilaštvo nadležno je za krivično gonjenje učinilaca krivičnih dela visokotehnološkog kriminala i nadležno je da postupa na celoj teritoriji Republike Srbije.

Za postupanje u predmetima visokotehnološkog kriminala nadležan je Viši sud u Beogradu za teritoriju Republike Srbije, a za odlučivanje u drugom stepenu nadležan je Apelacioni sud u Beogradu.

Takođe, odredbom Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, u okviru Ministarstva unutrašnjih poslova, obrazovana je Služba za borbu protiv visokotehnološkog kriminala koja postupa po nalogima Posebnog tužioca za visokotehnoški kriminal.

Značajnu ulogu u ovoj oblasti ima i Ministarstvo spoljne i unutrašnje trgovine i telekomunikacija, tako što doprinosi usklađivanju domaćih propisa u oblasti elektronskih komunikacija sa odgovarajućim propisima Evropske unije; preduzima mere za podsticanje istraživanja i razvoja u oblasti elektronskih komunikacija, usaradnji sa ministarstvom nadležnim za poslove razvoja i unapređenja naučnoistraživačke delatnosti;

Republička agencija za elektronske komunikacije (RATEL), osnovana Zakonom o elektronskim komunikacijama, predstavlja samostalnu organizaciju sa svojstvom pravnog lica, koja vrši javna ovlašćenja u cilju efikasnog sprovođenja utvrđene politike u oblasti elektronskih komunikacija, zaštite interesa korisnika elektronskih komunikacija i nadležna je za saradnju sa nadležnim regulatornim i stručnim telima država članica Evropske unije i

drugih država radi usaglašavanja prakse primene propisa iz oblasti elektronskih komunikacija i podsticanja konkurencije elektronskih komunikacionih mreža i usluga, unapređivanja njihovog kapaciteta

Zakon o informacionoj bezbednosti

Narodna skupština Republike Srbije usvojila je 26. januara 2016. godine Zakon o informacionoj bezbednosti („Službeni glasnik RS” broj 6/16). Ovaj zakon je prvi sistemski propis u oblasti informacione bezbednosti koji određuje mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornost pravnih lica prilikom upravljanja ovim sistemima i nadležne organe za sprovođenje mera zaštite.

Zakon je pisan u skladu sa načelima iz Strategije informacione bezbednosti EU, kao i odredbama Predloga direktive o mrežnoj i informacionoj bezbednosti EU. Predmet uređivanja prema Članu 1. ovog Zakona su mere zaštite od bezbednosnih rizika u informaciono -komunikacionim sistemima, odgovornosti pravnih lica prilikom upravljanja i korišćenja informaciono - komunikacionih sistema i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite

Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija.

Vlada Republike Srbije donela je, 30. juna 2016. godine, Uredbu o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija. Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija primenjuje se od 15. jula 2016. god.

Ovom uredbom uređuju se preventivne mere za bezbednost i zaštitu dece pri korišćenju informaciono-komunikacionih tehnologija, odnosno na internetu i postupanje u slučaju narušavanja ili ugrožavanja bezbednosti dece na internetu. Republika Srbija je prepoznala potrebu da institucionalno reaguje na znatan porast prijave štetnog i nelegalnog sadržaja na internetu koji ugrožavaju bezbednost dece, i da na taj način spreči da ovaj problem eskalira.

Uredba nalaže da Ministarstvo trgovine, turizma i telekomunikacija preduzima preventivne mere za bezbednost i zaštitu dece putem informisanja i edukacije i da uspostavi jedinstveno mesto za pružanje saveta i prijem prijave u vezi sa bezbednošću dece na internetu.

Krivični zakonik Republike Srbije

Kada je domaće zakonodavstvo u pitanju, Krivični zakonik Republike Srbije ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 i 94/2016) sadrži posebnu glavu o krivičnim delima protiv bezbednosti računarskih podataka. To su:

- Oštećenje računarskih podataka i programa (član 298.)
- Računarska sabotaža (član 299.)
- Pravljenje i unošenje računarskih virusa (član 300.)
- Računarska prevara (član 301.)
- Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (član 302.)
- Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 303.)
- Neovlašćeno korišćenje računara ili računarske mreže (član 304.)
- Pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka (član 304a).odredbe važio je do 1.juna 2017.

Krivični zakonik Srbije predviđa da su kažnjiva i druga krivična dela koja se mogu podvesti pod visokotehnoški kriminal. To su 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.

Tu spadaju i krivična dela gde se računari i računarske mreže javljaju kao sredstvo izvršenja krivičnih dela prevare, kod zloupotreba platnih kartica na Internetu, zloupotreba u oblasti elektronske trgovine i bankarstva, seksualno zlostavljanje dece na Internetu, govora mržnje na Internetu (širenje nacionalne, rasne, verske mržnje i netrpeljivosti i sl).

U ovu kategoriju spadaju i krivična dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, koja se zbog načina izvršenja ili upotrebljenih sredstava mogu smatrati krivičnim delima visokotehnoškog kriminala.

Odredbe Krivičnog zakonika važeće od 1.juna 2017

Krivična dela protiv intelektualne svojine

Član 199. Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava

Član 200. Neovlašćeno uklanjanje ili menjanje elektronske informacije o autorskom i srodnim pravima

Krivična dela protiv ustavnog uređenja i bezbednosti Republike Srbije, javnog reda i mira, imovine, pravnog saobraćaja i Krivična dela protiv ustavnog uređenja i bezbednosti Republike Srbije

Član 317 Izazivanje nacionalne, rasne i verske mržnje i netrpeljivosti

Krivična dela protiv javnog reda i mira

Član 343 Izazivanje panike i nereda

Krivična dela protiv imovine

Član 214 Iznuda

Član 215 Ucena

Krivična dela protiv pravnog saobraćaja

Član 355 Falsifikovanje isprave

Krivična dela protiv čovečnosti i drugih dobara zaštićenih međunarodnim pravom

Član 388 Trgovina ljudima

Član 223. Falsifikovanje novca (odredbe važeće DO 1. marta 2018. godine); član 241. Falsifikovanje novca (odredbe važeće OD 1. marta 2018. godine)

Član 225 Falsifikovanje i zloupotreba platnih kartica (odredbe važeće DO 1. marta 2018. godine); član 243 Falsifikovanje i zloupotreba platnih kartica (odredbe važeće OD 1. marta 2018. godine)

Krivična dela protiv sloboda i prava čoveka i građanina

Član 138 Ugrožavanje sigurnosti

Član 138a (odredbe važeće od 1. juna 2017. godine) Proganjanje

Član 143 Neovlašćeno prisluškivanje i snimanje

Član 144 Neovlašćeno fotografisanje

Član 145 Neovlašćeno objavljivanje i prikazivanje tuđeg spisa, portreta i snimka

Član 146 Neovlašćeno prikupljanje ličnih podataka

Član 153 Gonjenje za krivična dela protiv sloboda i prava čoveka i građanina

Krivična dela protiv polne slobode

Član 182a (odredbe važeće od 1. juna 2017. godine) Polno uznemiravanje

Član 184 Posredovanje u vršenju prostitucije

Član 185 (odredbe važeće do 1. juna 2017. godine) Prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju

Član 185 (odredbe važeće od 1. juna 2017. godine)

Član 185a (odredbe važeće do 1. juna 2017. godine) Navođenje maloletnog lica na prisustvovanje polnim radnjama

Član 185a (odredbe važeće od 1. juna 2017. godine) Navođenje deteta na prisustvovanje polnim radnjama

Član 185b Iskorišćavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu

Član 186 Gonjenje za krivična dela protiv polne slobode (odredbe člana 186 brišu se - izmenom 94/2016 - od 1. juna 2017. godine)

KRIVIČNA DELA PROTIV PRIVREDE-Odavanje poslovne tajne-Član 240.

Visokotehnoški kriminal u međunarodnim propisima

Generalna skupština Ujedinjenih nacija, koju čine predstavnici sve 193 svetske države, 20. decembra 2013. godine jednoglasno je usvojila Rezoluciju o pravu na privatnost u digitalnom dobu.

Evropska unija, sama ili u saradnji sa drugim međunarodnim organizacijama, već nekoliko decenija reguliše određena pitanja vezana za Internet i sajber prostor. Strategija sajber bezbednosti Evropske unije usvojena 2013. godine, predstavlja prvi sveobuhvatni akt koji je Evropska unija sačinila u ovoj oblasti.

U dokumentu se u više navrata ističe da osnovne vrednosti na kojima počiva EU moraju da se poštuju i u sajber prostoru. To znači da su postojeći međunarodni pravni akti u oblasti ljudskih prava sasvim primenljivi i u virtuelnom svetu, kao što su Međunarodna konvencija o ljudskim i političkim pravima, Evropska konvencija o ljudskim pravima i Povelja EU o osnovnim pravima.

Republika Srbija potpisnik je Konvencije o Sajber kriminalu (2009) Budimpeštanska Konvencija i Protokola uz Konvenciju o sajber kriminalu 2009 Konvencije Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja (2010)- Lozanska konvencija.

Tokom 1997. godine usvojena Direktiva Evropskog Parlamenta i Saveta o obradi podataka o ličnosti i zaštita privatnosti u telekomunikacionom sektoru“ (Directive 97/66/EC)⁹. Ipak, ključna Direktiva koja je u potpunosti posvećena zaštiti privatnosti u domenu elektronskih komunikacija je takozvana Direktiva o e-privatnosti ili pod punim nazivom „Direktiva Evropskog Parlamenta i Saveta o obradi podataka o ličnosti i zaštiti privatnosti u sektoru elektronskih komunikacija, koja je usvojena 2002. godine (Directive 2002/58/EC)¹⁰.

Zakon o potvrđivanju Konvencije o Sajber kriminalu (2009)Sl. glasnik RS, br. 19/09. je predvideo uvođenje adekvatnih instrumenata kada je reč o procesnim odredbama,kako bi se stvorila osnova za istraživanje i procesuiranje ovih krivičnih dela, ustanovljavanje brzih i efikasnih institucija i procedura međunarodne saradnje. Predviđeno je osnivanje kontakt tačke ili tački "24/7mreže" koja bi služila kao podrška policijskim i drugim organima zemalja

koje su ratifikovale Konvenciju, kao kontakt za sva obaveštenja i početna tačka za sve zahteve koji se tiču procesuiranja i istraživanja krivičnih dela visokotehnološkog kriminala.

Zakon o potvrđivanju Protokola uz Konvenciju o sajber kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema (2009) predviđa inkriminisanje akata rasističke i ksenofobične prirode počinjenih putem računarskih sistema. Njegova osnovna svrha je da se inkriminišu ponašanja koja nisu obuhvaćena Konvencijom, a koja se tiču širenja mržnje, netolerancije i netrpeljivosti prema rasnim, nacionanim, verskim i drugim grupama i zajednicama, korišćenjem računara kao sredstava komunikacije i širenja propagande.

Zakon o potvrđivanju Konvencije Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja (2010) -tzv Lozanska konvencija reguliše sprečavanje i borbu protiv seksualnog iskorišćavanja i seksualnog zlostavljanja djece, kao i zaštitu prava dece-žrtava seksualnog iskorišćavanja i seksualnog zlostavljanja, te unapređenje nacionalne i međunarodne saradnje u borbi protiv seksualnog iskorišćavanja i seksualnog zlostavljanja dece.

Konvencija o Sajber kriminalu (CETS br. 195)

Budimpeštanska Konvencija predstavlja prvi međunarodni sporazum o visokotehnološkim kriminalu koji je zaključen u cilju usklađivanja nacionalnih prava, unapređenja istražnih metoda i saradnje među državama. Konvencija o sajber kriminalu je osmišljena u cilju sprečavanja dela koja su usmerena protiv integriteta, poverljivosti i dostupnosti kompjuterskih sistema, mreža i podataka, a samim tim i sprečavanja zloupotrebe tih sistema, mreža i podataka tako što će se pokrenuti kaznene mere za takvo delovanje kao što je opisano u Konvenciji i pri čemu će se primeniti kazne za efikasnu borbu protiv krivičnih dela, i na taj način će se na unutrašnjem i međunarodnom nivou olakšati otkrivanje, istraga i gonjenje za izvršena krivična dela i omogućiti da se obezbede uslovi za brzu i pouzdanu međunarodnu saradnju.

Konvencija o Sajber kriminalu Saveta Evrope je prvi međunarodni sporazum koji reguliše materijalno pravni, procesno pravni, organizacioni i međunarodni okvir krivičnih dela koja su izvršena putem interneta i drugih računarskih mreža.

Konvencija postavlja osnovne postulate pravnih normi koje se tiču kršenja prava intelektualne svojine, računarski izvršenih prevara, zloupotreba maloletnika u pornografske svrhe itd. Ovom Konvencijom su propisane i radnje i mere, kako materijalno, tako i procesno pravne prirode, koje su usmerene ka regulisanju društveno štetnog ponašanja u ovoj oblasti i koje primenjuju savremene istražne metode prilikom otkrivanja i gonjenja izvršioca krivičnih djela, kao što su pretraga računarskih mreža i presretanje računarskih podataka, čiji je glavni cilj gonjenje izvršioca krivičnih dela i uspostavljanje zajedničke krivično-pravne

politike, koja je usmerena ka zaštiti društva od svih oblika visokotehnološkog, tj. „sajber kriminala“, posebno kroz usvajanje odgovarajućih pravnih normi i uspostavljanje saradnje.

Konvencija se sastoji iz četiri glave i to:

- Upotreba termina (I glava)
- Mjere koje trebaju da budu preduzete na domaćem nivou – materijalno i procesno pravo (II glava)
- Međunarodna saradnja (III glava)
- Završne odredbe (IV glava)

U okviru poglavlja 1, Konvencija na opšti način definiše pojmove kao što su računarski sistem, računarski podaci, pružalac usluga, podaci o saobraćaju, itd.

Imajući navedeno u vidu, Konvencija u širem smislu definiše računarski sistem kao uređaj koji se sastoji od hardvera, tj. fizičkih uređaja i softvera, tj. računarskih programa, koji se zajedno koriste za automatsko procesuiranje digitalnih podataka. Navedeni zbirni uređaj može uključiti ulazne, izlazne, kao i uređaje za pohranjivanje. U smislu Konvencije, računarsku mrežu predstavljaju dva ili više međusobno povezana računarska sistema. Međusobna povezanost može biti zemaljska, tj. putem žice ili kabla, bežična ili korišćenjem oba načina. Mreža može geografski biti ograničena na malu oblast (lokalna mreža) ili se može pružati preko velike teritorijalne oblasti (kao što su takozvane „WAN“ mreže). Ovakve mreže, takođe, mogu biti međusobno povezane na opisane načine.

Internet predstavlja globalnu mrežu koja se sastoji od mnoštva međusobno povezanih mreža koje sve koriste isti komunikacioni protokol, tj. Način komunikacije. Drugi tipovi mreža takođe postoje, bez obzira da li su ili nisu povezane na Internet i međusobno su osposobljene da komuniciraju razmenom računarskih podataka između računarskih sistema.

Pojedinačni računari ili računarski sistemi mogu biti povezani. Termin pružalac usluga, tj. „Internet service provider“, obuhvata široku kategoriju fizičkih i pravnih lica koja imaju određene uloge u odnosu na komunikaciju ili procesuiranje podataka u računarskim sistemima. Pod

ovom definicijom je jasno navedeno da kako javni, tako i privatni subjekti koji pružaju ovakvu vrstu usluga, jesu i moraju biti uključeni u krivično- pravni zakonodavni okvir zemalja potpisnica Konvencije.

Druga glave predviđa odredbe o sankcionisanju kriminala koji je izvršen pomoću računara i računarskih mreža i koji određuje 9 opštih krivičnih dela koja su podeljena u 4 različite kategorije.

Krivična dela koja su određena Konvencijom su:

1. neovlašćeni (protiv pravni) pristup
2. neovlašćeno (protiv pravno) presretanje
3. ometanje toka podataka
4. ometanje računarskog sistema

5. zloupotreba uređaja
6. falsifikovanje počinjeno pomoću računara
7. prevara izvršena pomoću računara
8. krivična dela dečije pornografije
9. krivična dela autorskih i srodnih prava.

U odjeljku 2, druge glave, koji govori o procesnim odredbama predviđaju:

1. hitno čuvanje pohranjenih podataka
2. hitno čuvanje i jelimično otkrivanje podataka o saobraćaju
3. naredbu za dostavljanje
4. pretragu i zaplenu računarskih podataka
5. prikupljanje podataka o saobraćaju u realnom vremenu
6. presretanje podataka o saobraćaju

U trećoj glavi Konvencija sadrži odredbe koje se odnose na tradicionalnei računarski povezane pravne instrumente međusobne saradnje, tj.međunarodne saradnje u krivičnom pravu, kao i pravila za izručenje.

Poglavlje govori o tradicionalnoj međunarodnoj saradnji u krivičnoj materiji

u dve situacije:

- kada ne postoji pravna osnova u vidu sporazuma, reciprociteta itd.,između strana potpisnica Konvencije, u kom slučaju se primjenjuju odredbe same Konvencije, kao i u slučajevima kada takva osnova postoji;te kada se primenjuju odredbe tih pravnih okvira uz pomoć primene same Konvencije.

Konvencija o Sajber kriminalu Savjeta Evrope (CETS 185) u svom trećem poglavlju reguliše u članovima od 23.do 35. Međunarodnu pravnu pomoć u krivičnim stvarima u oblasti tzv. „sajber kriminaliteta“. Konvencija u navedenim članovima, a posebno u uvodnim, naglašava i podvlači neophodnost proširenja međunarodne saradnje na najširi i najobuhvatniji mogući način. Konvencija kroz uspostavljanje principa međunarodne saradnje omogućava uspostavljanje intenzivne i ekstezivne međusobne saradnje država i njenih organa i pokušava da umanjii svaki negativni uticaj na brzine, ometanja i protok informacija i dokaza u međunarodnom okruženju.

Takođe, međunarodna saradnja bi trebalo da bude usmerena i da obuhvata i sva krivična dela koja se odnose na računare i računarske sisteme, kao i podatke koji su generisani od strane računara, koji su upotrebljeni ili na drugi način iskorišćeni u toku računarske komunikacije kao i prikupljanje dokaza u elektronskoj formi u vezi izvršenja krivičnih dela.U okviru regulisanja međunarodne pravne pomoći u krivičnim stvarima, a koje se odnose na borbu protiv visokotehnološkog kriminala,posebnu ulogu zauzima postojanje tzv. „24/7 mreže“ koja predstavlja mrežu tačaka kontakta među zemljama koje su ratifikovale Konvenciju I koje tačke kontakta se u najvećem broju slučajeva nalaze pri ministarstvima unutrašnjih poslova i javnim tužilaštvima, a ređe u ministarstvima pravde određenih zemalja. S tim u vezi, jasno je da ova mreža predstavlja brzi odgovor na prethodno navedenu potrebu za efektivnom borbom protiv kriminaliteta, tj. krivičnih dela koja su počinjena

korišćenjem računarskih sistema i računara, kao i efektivno prikupljanje dokaza u elektronskoj formi.

Četvrti deo Konvencije obuhvata završne odredbe potpisavanja i stupanja na snagu (pristupanje, teritorijalna primena, izjave, rezerve, rešavanje sporova, otkaz, itd.).

Direktiva 2013/40/EU

Direktiva 2013/40/EU je doneta od strane Evropskog parlamenta 20. avgusta 2013. godine i odnosi se na napade usmerene protiv informacionih sistema. Direktiva menja okvirnu odluku Saveta 2005/222/JHA i predstavlja sastavni dio tzv. „ACQUI COMMUNAUTAIRE“ – zajedničkog okvira zemalja članica Evropske Unije.

Cilj Direktive je da približi krivičnim zakonodavstvima zemalja članica Unije oblast napada protiv informacionih sistema, uspostavljanjem minimalnih pravila koji se odnose na definiciju krivičnih dela i odgovarajućih krivično-pravnih sankcija, kao i unapređenje saradnje između nadležnih organa koji uključuju pripadnike policije i drugih specijalizovanih agencija za sprovođenje zakona članica Unije, kao i nadležnih specijalizovanih agencija i tela same Evropske Unije kao što su EUROJUST, EUROPOL ili njegov Evropski centar za Sajber krajm (EC 3), kao i uključivanje u rad Evropske agencije za mrežnu i informatičku sigurnost (ENISA).

Obaveze države prema Ustavu Republike Srbije – član 194 koji navodi da su Potvrđeni međunarodni ugovori i opšteprihvaćena pravila međunarodnog prava deo su pravnog poretka Republike Srbije.

Ključne reči: Zakonodavna regulativa u Republici Srbiji -visokotehnološki kriminal, Visokotehnološki kriminal u međunarodnim propisima Generalna skupština Ujedinjenih nacija, koju čine predstavnici sve 193 svetske države, 20. decembra 2013. godine jednoglasno je usvojila Rezoluciju o pravu na privatnost u digitalnom dobu, Republika Srbija potpisnik je Konvencije o Sajber kriminalu (2009) Budimpeštanska Konvencija i Protokola uz Konvenciju o sajber kriminalu 2009 Konvencije Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja (2010)- Lozanska konvencija Direktiva 2013/40/EU je doneta od strane Evropskog parlamenta 20. avgusta 2013. godine i odnosi se na napade usmerene protiv informacionih sistema, Direktiva menja okvirnu odluku Saveta 2005/222/JHA i predstavlja sastavni dio tzv. „ACQUI COMMUNAUTAIRE“ –zajedničkog okvira zemalja članica Evropske Unije. Nadležne specijalizovane agencije i tela same Evropske Unije kao što su EUROJUST, EUROPOL ili njegov Evropski centar za Sajber krajm (EC 3), kao i uključivanje u rad Evropske agencije za mrežnu i informatičku sigurnost (ENISA).

Literatura:

1. Branko Stamenković, Saša Živanović, Bojana Paunović, Ivana Stevanović: VODIČ ZA SUDIJE I TUŽIOCE NA TEMU VISOKOTEHNOLOŠKOG KRIMINALA I ZAŠTITE MALOLETNIH LICA U REPUBLICI SRBIJI

2. Sinkovski S., Informaciona bezbednost komponenta nacionalne bezbednosti, Vojno delo, Beograd, 2/2005,

3. Akademija za diplomatiju i bezbednost – centar za strateške studije, društvo za informatiku Srbije, Agencija „ZIPA“, Informaciona Bezbednost, Beograd, 2009

4. Stevanović, I.(b) (2014) Moje pravo da budem zaštićen, Beograd: Institut za kriminološka i sociološka istraživanja.

5. Drakulić M., Drakulić R., Regulacija Interneta

Objavljeno „Advokatska kancelarija“ april 2018.

http://www.profisistem.com/propis_soft/akcija/98/advokatska_kancelarija