Kriminalističke teme
Časopis za kriminalistiku, kriminologiju i sigurnosne studije
Godište XII, Broj 3-4, 2012. str. 243-254
ISSN 1512-5505

INKRIMINIRANJE NEKIH KAZNENIH DJELA IZ PODRUČJA RAČUNALNOG KRIMINALITETA U REPUBLICI HRVATSKOJ

Stručni rad

INCRIMINATION OF SOME CRIMINAL ACTS OF COMPUTER CRIMINALITY IN REPUBLIC OF CROATIA

Proffesional paper

Siniša FRANJIĆ

Sažetak

Nagla ekspanzija modernih računalnih i digitalnih tehnologija donijela je niz društveno neprihvatljivih ponašanja koja je potrebno adekvatno regulirati (ili inkriminirati) kako bi počinitelji, nakon provedenoga pravosudnog postupka, mogli biti sankcionirani. Konvencija o kibernetičkom kriminalu i Dodatni protokol konvencije o kibernetičkom kriminalu dokumenti su Vijeća Europe koji opisuju računalna kaznena djela. Budući da Republika Hrvatska želi postati članica Europske unije, u svoj je Kazneni zakon ugradila odredbe spomenutih dokumenata Vijeća Europe.

Ključne riječi

Konvencija o kibernetičkom kriminalu, Kazneni zakon, Računalni kriminalitet, Internet

Abstract

Abrupt widening modern computer and digital technologies are bring many social unacceptable behaviorals which must be adequately approbate in national legislative. Convention on cybercrime and Additional Protocol to the Convention on cybercrime is documents of Council of Europe whose described computer criminal acts. As Republic of Croatia wish to be a part of European Union, in Croatian Criminal law are be incorporated provisions of Convention of cybercrime and Additional Protocol to the Convention on cybercrime.

Key words

Convention on cybercrime, Criminal law, Computer criminality, Internet.

1. Hrvatska kaznenopravna regulativa računalnog kriminaliteta

Informatička revolucija donijela je nove oblike društveno neprihvatljivog ponašanja koje je na odgovarajući način trebalo kriminalizirati. Zakonom o izmjenama i dopunama Kaznenog zakona [1], koji je stupio na snagu 1. listopada 2004. godine, u hrvatski pravni sustav implementirane su odredbe Konvencije o kibernetičkom kriminalu [2] i Dodatnog protokola [3] te Konvencije. Time je Republika Hrvatska kriminalizirala čitav niz društveno neprihvatljivih ponašanja vezanih uz računala i informacijske sustave, a opisi nekih postojećih kaznenih djela su usavršeni i upotpunjeni. Ovdje svakako treba istaknuti da na nekim opisanim situacijama neprihvatljivih ponašanja treba dodatno poraditi jer neka od ponuđenih rješenja nisu upotpunjena.

Konvencija o kibernetičkom kriminalu se sastoji od četiri poglavlja i to: Pojmovi, Mjere koje treba poduzeti na nacionalnoj razini, Međunarodna suradnja i Završne odredbe.

Dodatni protokol Konvencije o kibernetičkom kriminalu također ima četiri poglavlja i to: Zajedničke odredbe, Mjere koje se poduzimaju na nacionalnoj razini, Odnos između Konvencije i ovog Protokola i Završne odredbe.

1. 1. Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa i sustava [4]

Članak opisuje nezakoniti pristup i njime se kaže kako Zakon štiti samo onaj sustav koji ima zaštitne mjere. Ako se isti bude nezaštićen, neće se ostvariti elementi kaznenog djela.

Članak 223.

»(1) Tko unatoč zaštitnim mjerama neovlašteno pristupi računalnom sustavu, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine.

(2) Tko s ciljem onemogući ili oteža rad ili korištenje računalnih podataka ili programa, računalnog sustava ili računalnu komunikaciju, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

---

[1] Zakon o izmjenama i dopunama Kaznenog zakona – NN – 105/2004.
[2] Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu – NN – MU 9/2002.
[3] Zakon o potvrđivanju dodatnog protokola uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava – NN – MU 4/2008.
[4] Kazneni zakon – NN 110/97.; 27/98.; 50/2000.; 51/2001.; 111/2003.; 190/2003.; 105/2004.; 84/2005.; 71/2006.; 110/2007.; 152/2008.; 57/2011.

(3) Kaznom iz stavka 2. ovoga članka kaznit će se tko neovlašteno ošteti, izmijeni, izbriše, uništi ili na drugi način učini neuporabljivim ili nedostupnim tuđe računalne podatke ili programe.

(4) Kaznom iz stavka 2. ovoga članka kaznit će se tko presretne ili snimi nejavni prijenos računalnih podatka koji mu nisu namijenjeni prema računalnom sustavu, iz njega ili unutar njega, uključujući i elektromagnetske emisije računalnog sustava koji prenosi te podatke, ili tko omogući nepozvanoj osobi da se upozna s takvim podacima.

(5) Ako je kazneno djelo iz stavka 1., 2., 3. ili 4. ovoga članka počinjeno u odnosu na računalni podatak, program ili sustav tijela državne vlasti, javne ustanove ili trgovačkog društva od posebnoga javnog interesa, ili je prouzročena znatna šteta, počinitelj će se kazniti kaznom zatvora od tri mjeseca do pet godina.

(6) Tko neovlašteno izrađuje, nabavlja, uvozi, raspačava, prodaje, posjeduje ili čini drugome dostupne posebne naprave, sredstva, računalne podatke ili programe stvorene ili prilagođene za činjenje kaznenog djela iz stavka 1., 2., 3. ili 4. ovoga članka, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(7) Posebne naprave, sredstva, računalni podaci ili programi stvoreni, korišteni ili prilagođeni za činjenje kaznenih djela, a kojima je počinjeno kazneno djelo iz stavka 1., 2., 3. ili 4. ovoga članka oduzet će se.

(8) Za pokušaj kaznenog djela iz stavka 1., 2., 3. ili 4. ovoga članka počinitelj će se kazniti.

Člankom 223., stavak 1, opisano je ponašanje koje se odnosi na nezakoniti pristup. Njime se određuje da Zakon štiti samo onaj sustav koji ima zaštitne mjere. Ako se sustav ostavi potpuno otvorenim i nezaštićenim, odnosno ako računalo bude potpuno dostupno, neće se ostvariti elementi kaznenog djela [5].

U stavku 2. istog članka opisano je ponašanje koje se odnosi na ometanje sustava. U praksi su česti slučajevi koji se ovim stavkom inkriminiraju. Važan element ovdje jest namjera što znači da se oslobađa odgovornosti onaj tko, na primjer, nepažnjom isključi ključna računala davatelja internet usluga i dovede do prekida komunikacije. Ovdje je važno istaknuti da se upravo ovdje može pronaći jedna od specifičnosti u s vezi računalnog kriminala. Napadač može pustiti u distribuciju crva koji će se proširiti na tisuće drugih računala, koja će onda, bez znanja svojih rabitelja, sudjelovati u napadu. To bi značilo da postoji mogućnost uporabe tuđe

[5] Šimundić, Slavko; Franjić, Siniša: «Računalni kriminalitet», Pravni fakultet Sveučilišta u Splitu, Split, 2009., str. 95. i 96.

infrastrukture u počinjenju kaznenog djela bez ikakvog znanja vlasnika ili osoba koje rabe tu infrastrukturu. Oni ne mogu kazneno biti odgovorni za zlouporabu svoje opreme, ali će posredno biti njome pogođeni usporavanjem „zaraženih" računala i opterećivanjem njihovih mrežnih veza.

Stavak 3. opisuje ometanje podataka čime se taj oblik imovine štiti slično kao što se štite materijalne stvari. Računalni podaci u digitalnom obliku danas sve češće predstavljaju iznimno važnu imovinu. Štete koje nastanu oštećivanjem, izmjenjivanjem, brisanjem ili uništavanjem tuđih podataka mogu biti goleme.

Stavak 4. opisuje nezakonito presretanje kojim se traži sankcioniranje neovlaštenog presretanja nejavnih prijenosa računalnih podataka prema informacijskom sustavu, iz njega ili unutar njega (uključujući elektromagnetske emisije koje se nalaze u informacijskom sustavu i same računalne podatke) koje je počinjeno tehničkim sredstvom. Drugim riječima, to bi značilo da se ovim stavkom izričito zabranjuje prisluškivanje bežičnog prijenosa podataka te prisluškivanje žičanog prijenosa koje je moguće izvesti bez izravnog priključenja na telekomunikacijsku liniju.

Stavak 5. uvodi kvalificirani oblik ovoga kaznenog djela kada je objekt radnje računalni podatak, program ili sustav tijela državne vlasti, javne ustanove ili trgovačkog društva od posebnoga javnog interesa, ili je prouzročena znatna šteta, a što opravdano predviđa i težu propisanu kaznu. Ovdje se, kao mogući problem, može pojaviti određivanje „znatne štete".

Cilj kaznenopravne zaštite iz stavka 6. jest sprečavanje stvaranja i širenja tržišta naprava i u praksi vrlo čestih specijaliziranih programa za počinjenje kaznenih djela opisanih u stavcima 1., 2., 3. i 4. Inkriminacija tih kaznenih djela često se može provesti uz pomoć legalnih naprava i legalnih programa i tu se mogu pojaviti dodatni problemi.

Stavak 8. kaže da Konvencija o kibernetičkom kriminalu u svom članku 11. stavak 2. traži da države potpisnice propišu kažnjavanje i za pokušaj kaznenih djela iz ovog članka, trebalo je izričito propisati i kaznu za pokušaj.

1. 2. Računalno krivotvorenje [6]

Računalni podaci i programi su u svakodnevnoj upotrebi, a svaka njihova prerada, izmjena, brisanje, kopiranje, daljnja distribucija i sl., također se smatraju kaznenim djelima.

[6] Kazneni zakon – NN 110/97.; 27/98.; 50/2000.; 51/2001.; 111/2003.; 190/2003.; 105/2004.; 84/2005.; 71/2006.; 110/2007.; 152/2008.; 57/2011.

Članak 223.a

(1) Tko neovlašteno izradi, unese, izmijeni, izbriše ili učini neuporabljivim računalne podatke ili programe koji imaju vrijednost za pravne odnose, u namjeri da se oni uporabe kao pravi ili sam uporabi takve podatke ili programe, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(2) Ako je kazneno djelo iz stavka 1. počinjeno u odnosu na računalne podatke ili programe tijela državne vlasti, javne ustanove ili trgovačkog društva od posebnog javnog interesa, ili je prouzročena znatna šteta, počinitelj će se kazniti kaznom zatvora od tri mjeseca do pet godina.

(3) Kaznom iz stavka 1. ovoga članka kaznit će se tko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugome dostupne posebne naprave, sredstva, računalne podatke ili programe stvorene ili prilagođene za činjenje kaznenog djela iz stavka 1. ili 2. ovoga članka.

(4) Posebne naprave, sredstva, računalni podaci ili programi stvoreni, korišteni ili prilagođeni za činjenje kaznenih djela, a kojima je počinjeno kazneno djelo iz stavka 1. ili 2. ovoga članka oduzet će se.

(5) Za pokušaj kaznenog djela iz stavka 1. i 3. ovoga članka počinitelj će se kazniti.

Stavak 1. kaže kako se u suvremenom gospodarskom poslovanju te u poslovanju javne uprave i drugih pravnih osoba sve češće koriste digitalne baze podataka te kako se brojne evidencije vode isključivo u elektroničkom obliku [7]. Mnoge od tih baza podataka imaju iznimnu vrijednost, a njihova izmjena, uništavanje ili brisanje čine takve podatke neuporabljivima. Oni mogu prouzročiti velike štete i predstavljaju veliku društvenu opasnost.

Stavak 2. implicira uvođenje kvalificiranog oblika kaznenog djela [8], a ovdje se također može pojaviti problem određivanja velike štete.

Stavci 3., 4. i 5. su poprilično jasni.

[7] Šimundić, Slavko; Franjić, Siniša: Op. cit., str. 98.
[8] Kvalifikatorne okolnosti mogu se odnositi na modalitete radnje, svojstvo počinitelja ili objekta radnje, pobude, težinu posljedice i sl.

1. 3. Računalna prijevara [9]

Prijevare se mogu počiniti i uz pomoć suvremene računalne tehnologije, a posljedica je prouzročenje štete drugome.

Članak 224.a

(1) Tko s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, koristi, izmijeni, izbriše ili na drugi način učini neuporabljivim računalne podatke ili programe, ili onemogući ili oteža rad ili korištenje računalnog sustava ili programa i na taj način prouzroči štetu drugome, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

(2) Tko kazneno djelo iz stavka 1. počini samo s ciljem da drugoga ošteti, kaznit će se kaznom zatvora od tri mjeseca do tri godine.

(3) Tko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugome dostupne posebne naprave, sredstva, računalne podatke ili programe stvorene ili prilagođene za činjenje kaznenog djela iz stavka 1. ili 2. ovoga članka, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(4) Posebne naprave, sredstva, računalni podaci ili programi stvoreni, korišteni ili prilagođeni za činjenje kaznenih djela, a kojima je počinjeno kazneno djelo iz stavka 1. ili 2. ovoga članka oduzet će se.

(5) Za pokušaj kaznenog djela iz stavka 2. i 3. ovoga članka počinitelj će se kazniti.

Stavak 1. kaže kako je ovdje bitan element pribavljanje protupravne imovinske koristi, a posljedica je prouzročenje štete drugome [10]. Pod ovim kaznenim djelom moći će se pronaći razni oblici upada u računalne sustave sa svrhom promjene stanja na bankovnim računima, računalne prijevare s kreditnim karticama, plaćanja lažnim brojevima kreditnih kartica itd. Tu također mogu spadati razne blokade računalnih sustava kako bi se onemogućila provjera valjanosti kartica, brisanje loše kreditne povijesti itd.

Stavak 3. kaže da se ovdje radi o privilegiranom obliku kaznenog djela [11]. Posljedica je i ovdje prouzročenje štete drugome, ali je cilj počinitelja da ošteti drugoga,

---

[9] Kazneni zakon – NN 110/97.; 27/98.; 50/2000.; 51/2001.; 111/2003.; 190/2003.; 105/2004.; 84/2005.; 71/2006.; 110/2007.; 152/2008.; 57/2011.

[10] Vojković, Goran; Štambuk-Sunjić, Marija: „Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske“, Zbornik radova Pravnog fakulteta u Splitu, 1/2006.

[11] Poput kvalifikatornih, i privilegirajuće se okolnosti mogu odnositi na modalitete radnje, svojstvo počinitelja ili objekta radnje, pobude, težinu posljedice itd. Za privilegirane oblike su propisane blaže

odnosno cilj nije stjecanje protupravne imovinske koristi. Određenu sličnu štetu čine kaznena djela iz članka 223. pa bi se u praksi moglo dogoditi da dođe do nedoumica pod koje kazneno djelo svrstati određeno ponašanje.

1. 4. Dječja pornografija na računalnom sustavu ili mreži [12]

Na žalost, postoje ljudi koji se bave i ovime.

Članak 197.a

(1) Tko pomoću računalnog sustava ili mreže proizvodi, nudi, distribuira, pribavlja za sebe ili drugoga, ili tko u računalnom sustavu ili na medijima za pohranu računalnih podataka posjeduje pornografske sadržaje koji prikazuju djecu ili maloljetnike u seksualnom eksplicitnom ponašanju ili koji su fokusirani na njihove spolne organe, kaznit će se kaznom zatvora od jedne do deset godina.

(2) Tko djetetu, posredstvom računalnog sustava, mreže ili medija za pohranu računalnih podataka učini pristupačnim slike, audiovizualne sadržaje ili druge predmete pornografskog sadržaja, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(3) Posebne naprave, sredstva, računalni programi ili podaci korišteni ili prilagođeni za počinjenje kaznenog djela iz stavka 1. i 2. ovoga članka oduzet će se.

Kazneni zakon Republike Hrvatske je u svome izvornom tekstu iz 1997. godine poznavao kaznena djela „iskorištavanje djece ili maloljetnih osoba za pornografiju“ i „upoznavanje djece s pornografijom“. Zbog širenja dječje i maloljetničke pornografije putem interneta, bilo je potrebno propisati posebnu inkriminaciju s primjerenom kaznom, što je i učinjeno [13].

Bitan element ove inkriminacije jest činjenje pristupačnim djeci fotografija, audiovizualnih sadržaja ili drugih predmeta pornografskog sadržaja putem računalnog sustava, mreže i medija za pohranu računalnih podataka kao što su diskete, CD-ovi, DVD-ovi itd. Pornografski sadržaji danas su dostupni na internetu, a mediji za pohranjivanje podataka mogu se kupiti na gotovo svakom koraku. Kod kupnje medija može se provjeriti dob kupca, no, surfanje internetom je, u pravilu, anonimno. Tu se postavlja pitanje što učiniti da bi se djeci onemogućio pristup internet stranicama s pornografskim sadržajima i, za sada, ne postoji nekakav zadovoljavajući odgovor na to pitanje.

---

kazne
[12] Kazneni zakon – NN 110/97.; 27/98.; 50/2000.; 51/2001.; 111/2003.; 190/2003.; 105/2004.; 84/2005.; 71/2006.; 110/2007.; 152/2008.; 57/2011.
[13] Šimundić, Slavko; Franjić, Siniša: Op. cit., str. 99. i 100.

U svakom slučaju, uspješno se može primijeniti odredba iz stavka 2. ovog članka na slučajeve izravnog nuđenja djeci pornografskih sadržaja. No, što učiniti kada djeca sama surfaju internetom u potrazi za takvim sadržajima lažno se predstavljajući punoljetnima predstavlja dodatni problem. On se može riješiti uvođenjem odgovarajućih standarda na međunarodnoj razini.

1.5. Rasna i druga diskriminacija [14]

Internet je kao masovni medij izuzetno pogodan i za objavljivanje društveno neprihvatljivih ponašanja vezanih za rasnu i druge vrste diskriminacija. Potpisnici Konvencije o kibernetičkom kriminalu i njezinoga dodatnog Protokola su se obvezali sprečavati takve inkriminacije.

Članak 174.

(1) Tko na temelju razlike u rasi, vjeri, jeziku, političkom ili drugom uvjerenju, imovini, rođenju, naobrazbi, društvenom položaju ili drugim osobinama, spolu, boji kože, nacionalnosti ili etničkome podrijetlu krši temeljna ljudska prava i slobode priznate od međunarodne zajednice, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

(2) Kaznom iz stavka 1. ovoga članka kaznit će se tko progoni organizacije ili pojedince zbog njihova zalaganja za ravnopravnost ljudi.

(3) Tko u cilju širenja rasne, vjerske, spolne, nacionalne, etničke mržnje ili mržnje po osnovi boje kože ili spolnog opredjeljenja, ili drugih osobina, ili u cilju omalovažavanja, javno iznese ili pronese zamisli o nadmoćnosti ili podčinjenosti jedne rase, etničke ili vjerske zajednice, spola, nacije ili zamisli o nadmoćnosti ili podčinjenosti po osnovi boje kože ili spolnog opredjeljenja, ili drugih osobina, kaznit će se kaznom zatvora od tri mjeseca do tri godine.

(4) Tko s ciljem iz stavka 3. ovoga članka putem računalnog sustava raspačava ili na drugi način učini dostupnim javnosti materijale kojima se poriče, znatnije umanjuje, odobrava ili opravdava kazneno djelo genocida ili zločina protiv čovječnosti, kaznit će se kaznom zatvora od šest mjeseci do tri godine.

Ovdje se opisuje ponašanje iz članka 6. Dodatnog protokola Konvencije o kibernetičkom kriminalu kojim se traži sankcioniranje distribucije ili dostupnosti javnosti putem računalnog ili nekog sličnog sustava onih materijala koji poriču, znatnije umanjuju, odobravaju ili opravdavaju djela koja predstavljaju genocid ili

[14] Kazneni zakon – NN 110/97.; 27/98.; 50/2000.; 51/2001.; 111/2003.; 190/2003.; 105/2004.; 84/2005.; 71/2006.; 110/2007.; 152/2008.; 57/2011.

zločin protiv čovječnosti onako kako je to definirano u međunarodnom pravu i priznato kao takvo putem konačnih i obvezujućih odluka Međunarodnoga vojnog suda uspostavljenog Londonskim sporazumom 8. kolovoza 1945. godine ili bilo kojega drugog međunarodnog suda uspostavljenog putem relevantnih međunarodnih dokumenata čiju jurisdikciju ta stranka priznaje. To znači da Dodatni protokol izričito propisuje kako se inkriminiranje odnosi na nacističke zločine počinjene tijekom Drugoga svjetskog rata i na zločine počinjenje, na primjer, u bivšoj Jugoslaviji i u Ruandi za koje postoje relevantni međunarodni sudovi.

Internet je kao novi masovni medij iznimno pogodan za publiciranje najrazličitijih vrsta najrazličitijih materijala. Pojedinci, a i neke organizacije, su ga vrlo brzo počeli zlouporabljavati javno publicirajući društveno neprihvatljive stavove među kojima se nalaze poricanje, znatnije umanjivanje, odobravanje ili opravdavanje kaznenih djela genocida ili zločina protiv čovječnosti.

Budući da je Hrvatska bila poprište brojnih tragičnih događaja tijekom XX. stoljeća, ovdje opisani zločini imaju svoje mjesto u hrvatskom Kaznenom zakonu.

2. «Novi» Kazneni zakon

Od 01. siječnja 2013. godine, u Republici Hrvatskoj primjenjivat će se «novi» Kazneni zakon [15] koji, za razliku od prethodnog, ima posebnu glavu u kojoj su propisana kaznena djela iz područja računalnog kriminaliteta. To je Glava dvadeset i peta koja nosi naziv «Kaznena djela protiv računalnih sustava, programa i podataka. Ona predviđa sljedeća kaznena djela: Neovlašteni pristup, Ometanje rada računalnog sustava, Oštećenje računalnih podataka, Neovlašteno presretanje računalnih podataka, Računalno krivotvorenje, Računalna prijevara, Zloporaba naprava i Teška kaznena djela protiv računalnih sustava, programa i podataka. U «novom» Kaznenom zakonu predviđena su još neka kaznena djela koja se mogu počiniti uz pomoć računala i računalne tehnologije, ali se ista nalaze u drugim glavama.

«Novi» Kazneni zakon nije donio ništa novo što se tiče kaznenih djela iz područja računalnog kriminaliteta, osim što su u Glavi XXV. opisana pojedina kaznena djela i to na način da su iz «starog» Kaznenog zakona preneseni opisi stavaka pojedinih inkriminacija i tako su nastali opisi navedenih kaznenih djela. Svakako treba istaknuti da se opisi kaznenih djela dječje pornografije i rasne diskriminacije također nalaze u «novom» Kaznenom zakonu, ali u drugim glavama, što je, u svakom slučaju, pogrešno jer tim kaznenim djelima svakako nije mjesto negdje drugdje, nego u ovoj glavi Kaznenog zakona iz prostog razloga što se ona danas uglavnom čine posredstvom moderne računalne tehnologije. Pogrešno je i to što su

[15] Kazneni zakon – NN 125/2011.; 144/2012.

nazivi kaznenih djela drugačije navedeni pa će to zasigurno stvarati određene poteškoće tijelima koja se bave njihovim suzbijanjem.

3. Perspektiva i budućnost informatike u policiji

Razvoj moderne informacijske tehnologije, posebice računala, snažno je utjecao na mnoge djelatnosti. Razvojem novih tehnoloških dostignuća, širenjem područja primjene i primjene novih znanstvenih spoznaja, računalo postaje nužno svakodnevno pomagalo u životu i radu većine ljudi. Na nekim područjima to jest sadašnjost, a na nekima bliska budućnost, pa tako i u Ministarstvu unutarnjih poslova Republike Hrvatske. Nažalost, razvojem modernih informacijskih tehnologija, razvijaju se njezine brojne zlouporabe, kao i zlouporabe u kojima je moderna informacijska tehnologija samo tek sredstvo izvršenja kaznenih djela. Budući da se moderna informacijska tehnologija razvija praktički svakodnevno koja također praktički svakodnevno donosi brojne nove izazove, policijski službenici moraju biti spremni za njih. Ulaganje u njihovu dodatnu izobrazbu te u nove informacijske tehnologije omogućit će sprečavanje računalnog kriminaliteta u fazi nastanka pojedinoga kaznenog djela. Drugim riječima, policija mora biti spremna za izazove koje donosi moderno doba.

4. Zaključak

Informacijski sustav je skup definiranih pravila, praktičnih iskustava i metoda rada kod kojih ljudi ili grupe ljudi trebaju raditi na unošenju datih podataka u računalo i koji će obraditi informaciju tako da pruži sve potrebite specifikacije što će pojedincima omogućiti da se odluče u konkretnim poslovnim situacijama. Svakako treba posebno istaknuti da na funkcioniranje i kvalitetu svakoga informacijskog sustava bitno utječe nekoliko čimbenika i to: pristup izgradnji informacijskog sustava, koncepcija njegove izgradnje, tehničke osnove i koncepcija upravljanja njihovom izgradnjom i funkcioniranjem. I tu sada dolazimo do problema na kojega ukazuje ovaj rad, a to je zlouporaba moderne informacijske tehnologije. Ona je vrlo jednostavna i njome je lako upravljati pa je zbog toga doživjela naglu rasprostranjenost diljem svijeta. Budući da ista, dakle, ne predstavlja nekakav poseban problem, mnogi pojedinci uspješno su njome ovladali. S obzirom da, s jedne strane, na internetu postoji mnoštvo specijaliziranih stranica koje objavljuju novosti isključivo iz područja ovladavanja modernim informacijskim tehnologijama, s druge strane se javlja akumulacija znanja što znači da se javno, u elektroničkom obliku, prezentiraju sva trenutačna tehničko-tehnološka dostignuća iz najrazličitijih znanstvenih i neznanstvenih područja. Akumulacija znanja katkada zna biti potpomognuta objavljivanjem knjiga iz istih područja u kojima se također nudi nešto novo. Znanstvenici i drugi stručnjaci sva svoja istraživanja provode i objavljuju njihove rezultate s jednim isključivim ciljem, a to je dobrobit čovječanstva. Međutim, tu se vrlo brzo počinje javljati računalni kriminalitet jer se u toj priči upravo ovdje pojavljuju oni koji žele na brz i lak način doći do zarade ne suzdržavajući se ni od čega. Razvojem moderne informacijske tehnologije, nažalost,

razvija se i njezina zlouporaba. Drugim riječima, računalna revolucija donijela je nove oblike društveno neprihvatljivih ponašanja koje je na odgovarajući način trebalo sankcionirati što je i učinjeno Kaznenim zakonom Republike Hrvatske i u nekoliko navrata Zakonom o izmjenama i dopunama Kaznenog zakona Republike Hrvatske. Inkriminaciji kaznenih djela iz područja računalnog kriminaliteta prethodilo je prihvaćanje Konvencije o kibernetičkom kriminalu koju je Republika Hrvatska potpisala 2001. godine. No, svakako treba istaknuti da je najveći problem u ovom području taj što je počiniteljima kaznenih djela vrlo teško ući u trag. Uspješno suzbijanje kaznenih djela iz područja računalnog kriminaliteta može provesti jedino dobro obučena i dobro opremljena policija. To je jedan od najvažnijih elemenata u cjelokupnoj politici suzbijanja kriminaliteta uopće, a ovaj rad, analizom kaznenopravnih odredbi, ima za cilj doprinijeti boljem razumijevanju i izobrazbi svih onih koji se nalaze na liniji reagiranja na ova protupravna ponašanja. Potrebno je pooštriti sankcioniranje kaznenih djela iz područja računalnog kriminaliteta pa će politika njegova suzbijanja znatnije doći do izražaja. Počiniteljima i potencijalnim počiniteljima na taj bi se način poslala poruka da sankcioniranje računalnog kriminaliteta ima smisla.

LITERATURA:

1) Kazneni zakon – NN 110/97.; 27/98.; 50/2000.; 51/2001.; 111/2003.; 190/2003.; 105/2004.; 84/2005.; 71/2006.; 110/2007.; 152/2008.; 57/2011.
2) Zakon o izmjenama i dopunama Kaznenog zakona – NN – 105/2004.
3) Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu – NN – MU 9/2002.
4) Zakon o potvrđivanju dodatnog protokola uz Konvenciju o kibernetičkom kriminalu o inkrimininiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava – NN – MU 4/2008.
5) Šimundić, Slavko; Franjić, Siniša: «Računalni kriminalitet», Pravni fakultet Sveučilišta u Splitu, Split, 2009.
6) Vojković, Goran; Štambuk-Sunjić, Marija: „Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske“, Zbornik radova Pravnog fakulteta u Splitu, 1/2006.
7) Kazneni zakon – NN 125/2011.; 144/2012.

Biografija

Siniša Franjić rođen je u Osijeku 09. siječnja 1969. godine. Osnovnu i obje srednje škole završio je u Osijeku, a diplomirao je na Pravnom fakultetu Sveučilišta u Splitu. U suautorstvu s prof. dr. sc. Slavkom Šimundićem, napisao je knjigu «Računalni kriminalitet» koja ima status sveučilišnog udžbenika - UDK 343.533:004>(075.8); ISBN 978-953-6102-01-9, nekoliko znanstvenih članaka iz područja računalnog kriminaliteta i dvije skripte: «Komunikacije i komunikacijske vještine» (2010.) i «Ekonomska politika» (2011.)