UDK: 343.10 (497.6)
izvorni znanstveni rad
primljen 6. ožujka 2007.

Dr. sc. Sabrina Horović,
izvanredni profesor Pravnog fakulteta Sveučilišta u Mostaru

KAZNENA DJELA PROTIV SUSTAVA ELEKTRONSKE OBRADE PODATAKA U KAZNENOM ZAKONU FBiH

Temelj inkriminacija sadržanih u glavi XXXII. „Kaznena djela protiv sustava elektronske obrade podataka" u Kaznenom zakonu Federacije Bosne i Hercegovine sadržan je u Konvenciji o kibernetičkom kriminalu iz 2001. godine. Autorica je izvršila pravnu analizu odredaba članaka 393., 394. i 395. Kaznenog zakona, koji predstavljaju kaznena djela protiv povjerljivosti, integriteta i dostupnosti kompjutorskih podataka i sustava i usporedila navedene odredbe s relevantnim odredbama čl. 2-6., 7. i 8. Konvencije Vijeća Europe. U radu su učinjeni prijedlozi de lege ferenda u pogledu postojećih inkriminacija, kao i u pogledu propisivanja novih inkriminacija, dječje pornografije na računalnom sustavu ili mreži i rasnoj i ksenofobičnoj diskriminaciji putem računalnog sustava, sukladno dodatnom Protokolu uz Konvenciju o kibernetičkom kriminalu.

1. UVOD

Kaznena djela protiv sustava elektronske obrade podataka predstavljaju novinu u Glavi XXXII. Kaznenog zakona Federacije Bosne i Hercegovine. Temelj sadržanih inkriminacija je Konvencija Vijeća Europe o kibernetičkom kriminalu, usvojena u Budimpešti 23. studenog 2001. godine, koja je stupila na snagu 1. srpnja 2004. godine.[1]

Povijest kompjutorizacije seže u daleku 1822. godinu, a naglo se razvija tijekom II. svjetskog rata. No, može se uzeti da je jednostavnim oblikom današnjeg elektroničkog računala engleskog matematičara Alana Taringa, konstruiranog još 1936., otpočela era kompjutora.[2]

Kaznena djela protiv sustava elektronske obrade podataka uobičajeno se nazivaju kompjutorskim kriminalitetom. Postoje različiti pokušaji definiranja pojma kompjutorskog ili računalnog kriminaliteta. Prema jednima, ovaj oblik kriminaliteta nije prerastao u cjelovit i jedinstven fenomen, već se unutar njega odvijaju različiti oblici kriminalnog djelovanja, uz tendenciju da ipak, pro futuro, postane dominantan. Drugi ovaj kriminalitet povezuju s posebnim stručnim znanjima ili uz kaznena djela koja se ne bi mogla počiniti bez uporabe kompjutora. Povijesno, prve kompjutorske zloporabe bile su ogra-

1) Bosna i Hercegovina još nije potpisala navedenu Konvenciju.

2) Hawkins, J. M.- Allen, R., The Oxford English Dictionary, Oxford, 1991., str. 300-301.

ničene na ovlaštene korisnike, koji su se njima služili kako bi olakšali počinjenje tradicionalnih kaznenih djela, najčešće prijevare. Razvojem komunikacijskih uređaja (modema) sedamdesetih godina prošlog stoljeća i osobnih računala, osamdesetih godina prošlog stoljeća širi se tzv. softversko piratstvo, dok s razvojem globalnog informacijsko-komunikacijskog sustava (Interneta) kompjutorski kriminalitet prerasta nacionalne granice i dobiva globalne razmjere.[3]

Kompjutorski kriminalitet bismo mogli definirati kao ukupnost kriminalnih ponašanja na određenom području i u određenom razdoblju usmjerenih protiv tajnosti, cjelovitosti i dostupnosti računalnih sustava, mreža i računalnih podataka kao i kriminalna ponašanja kojima se zlorabljuju računalni sustavi, mreže i računalni podaci.[4]

Prije zakonodavnih reformi i kaznenopravne regulacije kompjutorskog kriminala, na ovaj oblik, primjenjivale su se kaznene odredbe o krađi, prijevari, pronevjeri, poslovnoj i drugoj tajni i o zaštiti intelektualnog vlasništva. Na taj način dovodilo se u pitanje temeljno načelo zakonitosti, posebice određenost zakonskih opisa kaznenog djela i zabrana analogije. To je uvjetovalo aktivnost nacionalnih zakonodavstava, najprije u razvijenim zemljama, kao i aktivnost regionalnih[5] i međunarodnih organizacija.[6]

Konvencija o kibernetičkom kriminalu predviđa propisivanje u nacionalnom kaznenom zakonodavstvu četiri skupine kaznenih djela: kaznena djela protiv povjerljivosti, integriteta i dostupnosti kompjutorskih podataka i sustava, kaznena djela u vezi s kompjutorima, kaznena djela vezana za kompjutorski sadržaj i kaznena djela koja se odnose na kršenje autorskih i njima sličnih prava. Dodatni Protokol iz 2003. g., koji još nije stupio na snagu, propisuje i inkriminiranje rasizma i ksenofobije putem kompjutora.

Kaznena djela protiv sustava elektronske obrade podataka propisana su u glavi XXXII. Kaznenog zakona Federacije Bosne i Hercegovine i glavi XXXII. Kaznenog zakona Brčko Distrikta Bosne i Hercegovine, dok Krivični zakon Republike Srpske ova kaznena djela ne propisuje u posebnoj glavi, nego u okviru drugih glava u posebnom dijelu KZ-a. U radu će se analizirati glavne značajke pojedinih kompjutorskih kaznenih djela iz Kaznenog zakona Federacije Bosne i Hercegovine, i to: kaznenog djela „Oštećenje računalnih programa i podataka" (čl. 393. KZ FBiH i čl. 387. KZ BD BiH, koje predstavlja prema klasifikaciji iz navedene Konvencije, kazneno djelo protiv povjerljivosti, integriteta i dostupnosti kompjutorskih podataka i sustava), kazneno djelo „Računalno krivotvorenje" (čl. 394. KZ FBiH i čl. 388. KZ BD BiH) i „Računalna prijevara" (čl. 395. KZ FBiH i čl. 389. KZ BD BiH), koja predstavljaju kaznena djela u vezi s kompjutorima.

3) Prema: Dragičević, D., Kompjutorski kriminalitet i informacijski sustavi, Informatorovi priručnici, Zagreb, 2004., str. 117 - 119.

4) Definicija utvrđena na temelju teksta preambule Konvencije o kibernetičkom kriminalu u kojem stoji „da je ova Konvencija nužna radi odvraćanja od postupaka usmjerenih protiv tajnosti, cjelovitosti i dostupnosti računalnih sustava, mreža i računalnih podataka, kao i za odvraćanje od njihovih zloporaba, jer utvrđuje - na način opisan u Konvenciji – kriminalizaciju takvog ponašanja.

5) Primjerice: U okviru OECD-a, 1985. g. zemljama članicama preporučeno je koje bi namjerne radnje trebalo kriminalizirati.

6) Primjerice: Vijeće Europe je 1989, g. u Preporuci br. R(89)a utvrdilo minimalnu i opcijsku listu kompjutorskih inkriminacija, a UN su na VIII. kongresu 1990. g. u Havani, Rezolucijom, zatražili od svih država članica UN da pojačaju napore radi suzbijanja manipulacija elektroničkim računalima među koje ulazi modernizacija kaznenog prava i postupka. Više o tome: Krapac, D., Kompjutorski kriminalitet, Zagreb, 1992., str. 17. i dalje.

2. POJEDINA KAZNENA DJELA

2. 1. Oštećenje računalnih podataka i programa

Riječ je o novom kaznenom djelu iz sastava kompjutorskog kriminala.[7] Opis kaznenog djela usklađen je s odredbama članaka 2. do 6. Konvencije o kibernetičkom kriminalu. Propisivanjem ovog kaznenog djela popunjava se praznina u našem kaznenom zakonodavstvu koja je u ovom pogledu postojala i otklanja se potreba neodgovarajuće primjene postojećih tradicionalnih inkriminacija. Odredbama ovog članka pruža se znatno šira kaznenopravna zaštita sustavu elektronske obrade podataka nego što to proizlazi iz naziva članka. Težište kaznenog djela je na pravnoj zaštiti od neovlaštenog pristupa kompjutorskim sustavima, tj. „hakinga". Kaznenopravne norme koje se odnose na područje neovlaštenog pristupa kompjutorskim sustavima donesene su u većini zemalja, primjerice: u Njemačkoj (čl. 202 a. KZ-a), Francuskoj (čl. 462-2. KZ-a), Španjolskoj (čl. 256. KZ-a), Švicarskoj (čl. 143 bis KZ-a), Velikoj Britaniji (čl. 1, 2 Computer Misuse Act-a iz 1990.), itd.

Zakonodavac ne propisuje pojmove računalnih programa i računalnih podataka, zbog toga ih je potrebno tumačiti u skladu sa značenjem datim u Konvenciji. U čl. 1. toč. b. Konvencije „računalnim podacima" označava se svako iskazivanje činjenica, informacija ili koncepata u obliku prikladnom za obradu u računalnom sustavu, uključujući i program koji je u stanju prouzročiti da računalni sustav izvrši određene funkcije. Ne koristi se termin „računalni sustav" iz čl. 1. toč. a. Konvencije, koji označava svaku napravu ili skupinu međusobno spojenih ili povezanih naprava, od kojih jedna ili više njih na temelju programa automatski obrađuje podatke.

Stavak 1.

Djelo iz stavka 1. čini onaj tko ošteti, izmijeni, izbriše, uništi ili na drugi način učini neuporabljivim ili nedostupnim tuđe računalne podatke ili računalne programe. Temelj ove inkriminacije je čl. 4. Konvencije (Ometanje podataka). Opis djela je širi u odnosu na konvencijsko rješenje, jer se osim na ometanje podataka proteže i na nedopuštenu manipulaciju računalnim podacima ili programima. Modalitetima radnje počinjenja ovlaštenu se osobu ograničava ili onemogućuje u elektroničkoj obradi podataka (činjenica, informacija ili koncepata) prikladnih da elektronički sustav obavi određenu zadaću.

---

7) Oštećenje računalnih podataka i programa (Čl. 393. KZ FBiH) glasi:

(1) Tko ošteti, izmijeni, izbriše, uništi ili na drugi način učini neuporabljivim ili nepristupačnim tuđe računalne podatke ili računalne programe, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine.

(2) Tko unatoč zaštitnim mjerama neovlašteno pristupi računalnim podacima ili programima ili neovlašteno presreće njihov prijenos, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(3) Kaznom iz stavka 2. ovoga članka kaznit će se tko onemogući ili oteža rad ili korištenje računalnog sustava, računalnih podataka ili programa ili računalnu komunikaciju.

(4) Ako je kazneno djelo iz stavka 1. do 3. ovoga članka počinjeno u odnosu na računalni sustav, podatak ili program tijela vlasti, javne službe, javne ustanove ili gospodarskog društva od posebnog javnog interesa, ili je prouzročena znatna šteta, kaznit će se zakonom zatvora od tri mjeseca do pet godina.

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

(6) Posebne naprave, sredstva, računalni programi ili podaci sačinjeni, korišteni ili prilagođeni radi počinjenja kaznenih djela, kojima je kazneno djelo iz stavka 1. do 3. ovoga članka počinjeno, oduzet će se.

Radnja počinjenja djela iz stavka 1. određena je alternativno kao: oštećenje, izmjena, brisanje, uništenje ili na drugi način počinjenje neuporabljivim ili nedostupnim tuđih računalnih podataka ili programa.

Radnja oštećenja na određeni način predstavlja kompjutorsku sabotažu. Inkriminiranjem radnje oštećenja nastoji se zaštititi cjelovitost kompjutorskih podataka i programa. Ovaj oblik kaznenog djela odnosi se prema kaznenom djelu oštećenja tuđe stvari iz čl. 293. st. 1. KZ-a kao specijalno u odnosu prema općem kaznenom djelu (lex specialis derogat legi generali).

Radnja izmjene poseban je oblik kaznenog djela prijevare (čl. 294. KZ-a), jer se izravnom izmjenom ili putem programa izvode nezakonite manipulacije s obilježjima prijevare. Izmjena tuđih automatski obrađenih podataka ili računalnih programa ujedno je i njihovo kompjutorsko krivotvorenje.

Brisanje računalnih podataka ili programa je način njihova uništenja, radnja kojom se oni čine trajno neuporabljivim.

Radnja ovog oblika kaznenog djela može biti i svaka druga radnja kojom se ti podaci ili programi čine neuporabljivim ili nedostupnim. Pojam činjenja nedostupnim je širi, jer uključuje i situacije kada podaci nisu izbrisani ili oštećeni, ali im ovlašteni korisnik ne može pristupiti.

Za dovršenje kaznenog djela traži se nastupanje određene posljedice, neuporabljivost ili nedostupnost podataka ili programa.

Djelo se može počiniti samo s namjerom.

Kod ovog oblika kaznenog djela postavlja se pitanje odnosa s kaznenim djelom krađe (čl. 286. KZ-a), u slučaju krađe hardware-a (materijalna osnovica koju čini informatička tehnologija), ili pojedinih uređaja (pr. modema-naprave koja pretvara digitalne signale iz kompjutora i prenosi ih preko telefonskih linija do drugog modema koji primljeni signal ponovno pretvara u digitalni oblik). U Austriji postoji stjecaj s kaznenim djelom krađe iz par. 127. KZ-a. Istu praksu bismo i mi mogli prihvatiti i u navedenim slučajevima utvrditi stjecaj kaznenog djela iz čl. 393. st. 1. i čl. 286. KZ-a.

Stavak 2.

Kazneno djelo čini onaj tko unatoč zaštitnim mjerama neovlašteno pristupi računalnim podacima ili programima ili neovlašteno presreće njihov prijenos. Temelj ove inkriminacije je čl. 2. Konvencije (Nezakoniti pristup) i čl. 3. Konvencije (Nezakonito presretanje).

Radnja počinjenja neovlaštenog pristupa prema Objašnjenjima iz Konvencije je ulaženje u cijeli ili bilo koji dio kompjutorskog sustava (hardware, komponente, pohranjeni podaci, itd.), ali se pristupom ne smatra obično slanje e-mail poruke ili fajla.

Neovlašteni pristup postoji ne samo cjelini računalnog sustava nego i njegovu dijelu.

Neovlašteno presretanje sastoji se od svake radnje kojom se „upada" u nejavne prijenose računalnih podataka prema računalnom sustavu, iz njega ili unutar njega (uključujući i elektromagnetske emisije iz računalnog sustava koji prenosi te računalne podatke), počinjene tehničkim sredstvom (prema čl. 3. Konvencije). Prema Objašnjenjima Konvencije odredba o nezakonitom presretanju ima za cilj zaštitu prava privatnosti u pogledu prijenosa računalnih podataka.

Potrebno je da su pristup ili presretanje počinjeni neovlašteno i unatoč zaštitnim mjerama. Zakonski izraz „neovlašteno" ukazuje da je riječ o kaznenom djelu kod kojeg

je protupravnost ne samo genusni, već posebni, specijalni dio bića ovog oblika kaznenog djela. Tamo gdje postoji ovlaštenje isključena je protupravnost kaznenog djela.

Računalni podaci ili programi moraju prethodno biti posebno zaštićeni. Misli se na zaštitne mjere čiji je cilj osiguranje dostupnosti računalnih podataka ili programa samo ovlaštenim osobama. Međutim, u našim financijski i tehnički siromašnim uvjetima teško je osigurati učinkovitu tehničku, programsku i podatkovnu zaštitu. Veoma su skupa sredstva zaštite i osobe koje ih provode. Uobičajene su sljedeće metode i sredstva zaštite: fizička zaštita, provjera pristupa, pravilno postavljanje i zaštita lozinke, kriptografske metode, kerberos, vatreni zidovi, digitalni potpis, digitalni vremenski biljeg, stenografija, izdvajanje, sigurnosne kopije, zaštita od virusa i nadzor rada i korištenja računalnog i mrežnog sustava.[8]

Nekažnjivost neovlaštenog pristupa računalnim podacima ili programima bez prethodno poduzete zaštitne mjere, s obzirom na naše trenutne ekonomske i tehnološke uvjete i zbog neodređenosti i nepostojanja zakonske obveze njihovog poduzimanja, ovu inkriminaciju čine problematičnom.

Glede subjektivne strane inkriminacije, traži se samo namjerni pristup.

Budući da je djelo neovlaštenog pristupa ili presretanja često samo početak ili priprema za počinjenje nekog drugog, težeg djela, s kojim će doći u stjecaj, u nekim se zemljama inkriminira temeljno djelo hakerstva i njegovi kvalificirani oblici, tako da ukoliko i ne dođe do ostvarenja tog drugog djela, počinitelj se kažnjava za temeljno djelo hakinga, kao aktivnosti usmjerene na neovlašteni pristup, kako bi se saznali određeni podaci povjerljive naravi ili kako bi se ti podaci krivotvorili, uništili ili oštetili.[9]

Na ovom mjestu samo kao napomena o neograničenim mogućnostima novih oblika hakerske aktivnosti putem Interneta. Radi se, primjerice, o krađi identiteta, prodaji lažnih kreditnih kartica putem elektroničke mreže, korištenju tuđih osobnih kartičnih podataka i putem njih na teret njihovih vlasnika kradljivci kupuju robu, troše, dižu novac, čak prodaju ostavštinu. Jedino što je vlasnicima e-mailova za sada ostalo jest da budu vrlo oprezni pri njihovu korištenju putem Interneta.[10]

Stavak 3.

Djelo iz stavka 3. sastoji se u onemogućavanju ili otežavanju rada ili korištenja računalnog sustava, računalnih podataka ili programa, te u onemogućavanju ili otežavanju računalne komunikacije. Temelj ove inkriminacije je čl. 5. Konvencije (Ometanje sustava). Za razliku od odredbe čl. 5. Konvencije, naš zakonodavac ne navodi načine na koje se može onemogućiti ili otežati rad ili korištenje računalnog sustava, računalnih podataka ili programa ili računalna komunikacija. Članak 5. Konvencije, kao načine počinjenja, primjera radi navodi: unošenje, prenošenje, oštećenje, brisanje, mijenjanje ili prikrivanje kompjutorskih podataka, kojim se protupravno i u većem stupnju ometa funkcioniranje kompjutorskih sustava.

Radnja počinjenja je dakle neodređena, sastoji se od svakog postupka kojim se drugim osobama onemogućava ili otežava rad ili korištenje računalnog sustava, podataka ili programa ili računalne komunikacije.

---

8) O svakoj od navedenih metoda i sredstava zaštite v. Dragičević, D., op. cit., str. 78 - 92.

9) Tako, primjerice: u Sjedinjenim Američkim Državama, Eletronic Communications Privacy Act of 1986. i Computer Fraud and Abuse Act of 1984. and 1986., prema Dragičević, D., op. cit., str. 152.

10) Bačić, F., - Pavlović, Š., Komentar Kaznenog zakona, Organizator, Zagreb, 2004., str. 803.

Namjera počinitelja obuhvaća „namjerni čin ozbiljnog neovlaštenog sprječavanja funkcioniranja računalnog sustava" (čl. 5. Konvencije).

Najčešći način počinjenja ovog oblika kaznenog djela ostvaruje se slanjem spame e-mail poruka, što znači slanje neželjene, netražene poruke, slanje neželjenog elektroničkog smeća. Zbog ovakvih poruka samo tvrtke članica Europske unije godišnje gube 2,5 milijardi eura. O štetnosti spam poruka dovoljno govori podatak da više od polovice poslanih e-mailova otpada na spam.[11]

Stavak 4.

U stavku 4. propisani su kvalificirani oblici kaznenih djela iz prethodna tri stavka. Kvalificirane okolnosti su svojstvo korisnika objekta radnje ili težina posljedice. Svojstvo korisnika odnosi se na organ vlasti, javne službe ili gospodarsko društvo od posebnog javnog interesa, što mora biti obuhvaćeno namjerom počinitelja. Iz opisa kaznenog djela ne vidi se na što se odnosi šteta. Je li riječ o šteti nastaloj neposrednim gubicima prouzročenim radnjom počinjenja ili o troškovima restitucije, ili o šteti nastaloj zbog kraćeg ili duljeg nekorištenja oštećenih podataka. U ocjeni postojanja štete kao elementa bića kaznenog djela u obzir treba uzeti samo neposredno prouzročenu štetu, a ostale gubitke i štetne posljedice počinjenog djela počinitelju treba uzeti kao otegotnu okolnost. Za prouzročenje štete dovoljan je nehaj počinitelja.

Stavak 5.

Djelo iz st. 5. čini onaj tko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugom dostupne posebne naprave, sredstva, računalne programe ili računalne podatke stvorene ili prilagođene radi počinjenja kaznenog djela iz st. 1 - 3. ovog članka. Temelj ove inkriminacije nalazi se u članku 6. Konvencije (Zloporaba uređaja). U Objašnjenjima Konvencije kao razlog za ustanovljenje ovog kaznenog djela navodi se da počinjenje kaznenih djela protiv povjerljivosti, cjelovitosti i dostupnosti kompjutorskih sustava ili podataka često zahtijeva posjedovanje sredstava za pristup („hakerskog oruđa") ili druga oruđa što predstavlja jak poticaj za njihovo stjecanje u kriminalne svrhe, što onda može dovesti do stvaranja jedne vrste crnog tržišta u njihovoj proizvodnji i distribuciji.

Radnje počinjenja ovog oblika kaznenog djela su alternativno određene i radi se o radnjama koje po svojoj sadržini predstavljaju pripremanje ili pomaganje djela iz st. 1-3. ovog članka, a koje su ovim stavkom propisane kao samostalno kazneno djelo. Međutim, ako bi počinitelj radnje iz st. 5. ujedno počinio kazneno djelo iz st. 1-3., neće odgovarati za djelo iz st. 5., jer se radi o kaznenom djelu iz sastava tzv. delicta preparata.

Stavak 6.

Posebne naprave, sredstva, računalni programi ili podaci stvoreni, korišteni ili prilagođeni radi počinjenja kaznenih djela kojima je kazneno djelo iz st. 1. do 3. ovog članka počinjeno, obvezno će se oduzeti i kada nisu svojina počinitelja.

Ova odredba temelji se na primjeni sigurnosne mjere oduzimanja predmeta iz čl. 78. KZ-a.

11) Više o tome: Pavlović, Š., Spamming e-mail poruke, HLJKPP, br. 1/2004., str. 287 - 291.

2.2. Računalno krivotvorenje[12]

Temelj za ovo kazneno djelo je članak 7. Konvencije („Krivotvorenje koje je u vezi sa kompjutorima"). Prema Objašnjenjima uz Konvenciju, svrha čl. 7. je propisivanje kaznenog djela paralelnog kaznenom djelu krivotvorenja opipljivih isprava. Radi se o kaznenom djelu koje se čini uporabom kompjutorskog sustava, a objekt radnje su kompjutorski podaci, pri čemu pojmovi kompjutorskog sustava i kompjutorskih podataka imaju značenje ranije opisano u čl. 1. Konvencije. Ovim kaznenim djelom štiti se autentičnost, izvornost računalnih podataka koji imaju vrijednost za pravne odnose i pravni promet.

Stavak 1.

Djelo iz stavka 1. čini tko neovlašteno izradi, unese, izmijeni, izbriše ili učini neuporabljivim računalne podatke ili programe koji imaju vrijednost za pravne odnose s ciljem da se uporabe kao pravi ili sam uporabi takve podatke ili programe.

Radnja počinjenja alternativno je određena. Radi se o radnjama kojima se dobivaju računalni podaci ili programi koji nisu autentični, koji ne potiču od osobe koja je označena kao njihov autor, odnosno kojima se mijenja njihov izvorni oblik ili sadržaj, pri čemu je za postojanje djela nebitno je li podatak koji je, primjerice, unesen ili izbrisan, točan ili netočan. Ovako određene radnje počinjenja kaznenog djela odgovaraju radnjama izrade lažne isprave i preinačenja prave isprave kod kaznenog djela krivotvorenja isprave iz čl. 373. KZ-a.

Moderno doba obilježava elektronička pošta, elektroničko poslovanje i ostali oblici daljinskog komuniciranja. Radi zaštite podataka i dokumenata u toj razmjeni nužno je predvidjeti i kaznenopravnu zaštitu. Najprije, osiguranje osobe koja je sastavila dokument s ciljem osiguranja njezine vjerodostojnosti i zatim zaštita autentičnosti podataka u prometu, prema čl. 1. d. Konvencije, računalni podaci u vezi s komunikacijama, stvoreni pomoću računalnog sustava, koji je dio komunikacijskog lanca, koji podaci naznačuju podrijetlo komunikacije, njezino odredište, put, vrijeme, datum, veličinu, trajanje ili vrstu te usluge.

Da bi postojalo kazneno djelo, nužno je da računalni podatak ili program imaju vrijednost za pravne odnose. U opisu djela objekt radnje nije određen u skladu s Konvencijom, koja u čl. 7. sadrži računalne podatke, ali ne i programe. Naime, prema već ranije citiranom čl. 1. b. Konvencije računalni podatak uključuje i program koji je podoban prouzročiti da računalni sustav izvrši određenu funkciju. Nije, dakle, trebalo u KZ unositi i programe kao objekt radnje.

---

12) Računalno krivotvorenje (čl. 344. KZ FBiH) glasi:

(1) Tko neovlašteno izradi, unese, izmijeni, izbriše ili učini neuporabljivim računalne podatke ili programe koji imaju vrijednost za pravne odnose, s ciljem da se 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. ovoga članka počinjeno u odnosu na računalne podatke ili programe tijela, javne službe, javne ustanove ili gospodarskog društva od posebnog javnog interesa, ili je prouzročena znatna šteta, kaznit će se kaznom zatvora od tri mjeseca do pet godina.

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

(4) Posebne naprave, sredstva, računalni programi ili podaci sačinjeni, korišteni ili prilagođeni radi počinjenja kaznenih djela, kojim je počinjeno kazneno djelo iz stavka 1. ili 2. ovoga članka, oduzet će se.

Krivotvorenje se odnosi ne samo na vidljive i čitljive dokumente nego i na dokumente u digitalnom obliku, pa i bez postojanja na fizičkom mediju, već u samom postupku obrade ili prijenosa unutar mreže ili između udaljenih računalnih sustava.

Postoji samo jedno kazneno djelo ako ista osoba krivotvori, a zatim i uporabi krivotvoreni računalni podatak ili program.

Kazneno djelo je delictum communium.

Kazneno djelo se može počiniti samo s izravnom namjerom, a za postojanje djela traži se utvrđivanje posebne namjere da se računalni podatak ili program koji ima vrijednost za pravne odnose i čija se autentičnost nekom od zakonom propisanih radnji počinjenja narušava, upotrijebi kao pravi.

Kod drugog oblika kaznenog djela iz st. 1., u odnosu na okolnost da je računalni podatak ili program koji se uporabljuje krivotvoren, dovoljna je i eventualna namjera.

Kazneni zakon Njemačke ima dva kaznena djela, krivotvorenje podataka s dokaznom snagom u par. 269.[13], čiji je smisao inkriminacije zaštita sigurnosti i pouzdanosti pravnog prometa i podataka (elektroničkih dokumenata) u prometu i kazneno djelo mijenjanje podataka iz par. 303. a[14], koje se sastoji u protupravnom brisanju, zatajivanju, činjenju neuporabljivim ili mijenjanju podataka. Ovo kazneno djelo važno je ne samo zbog neposrednih manipulacija na podacima, odnosno s podacima, već i mogućnosti da se primijeni i na slučajeve kada do modifikacije ili brisanja podataka dođe kao rezultat djelovanja malicioznih programa koji imaju za cilj da takve izmjene naprave ili pak onemoguće njihovo korištenje.

S namjerom da se elektroničkim dokumentima pruži ista pravna zaštita kao i onima na papiru, neke zemlje kao, primjerice, već navedena Njemačka, Francuska, Finska, Norveška, itd., donijele su nove zakonske odredbe o krivotvorenju kojima se napušta nužnost vizualnog zapažanja.[15]

Stavak 2.

U stavku 2. propisan je kvalificirani oblik kaznenog djela iz stavka 1. ovog članka. Kvalificirani oblik će postojati ako je djelo iz stavka 1. počinjeno u odnosu na računalne podatke ili programe tijela javne službe, javne ustanove ili gospodarskog društva od posebnog javnog interesa, ili je prouzročena znatna šteta. Kvalificirane okolnosti su svojstvo korisnika objekta radnje ili težina posljedice. Posebice se zaštićuju podaci ili programi određenih tijela, javnih službi, javnih ustanova ili gospodarskih društava od posebnog javnog interesa. Ovo kazneno djelo može se počiniti i u slučaju kad je djelom iz st. 1. prouzročena znatna šteta.

Počinitelj može biti bilo tko.

---

13) Par. 269. KZ Njemačke glasi:

(1) Tko prijevarno u pravnom prometu tako načini ili promijeni podatke važne za dokazivanje da oni kod njihovog očitovanja predstavljaju lažnu ili krivotvorenu ispravu, ili tako pripravljene ili izmijenjene podatke upotrijebi, kaznit će se kaznom zatvora do pet godina ili novčanom kaznom.

(2) Kažnjiv je i pokušaj.

(3) Odgovarajuće se primjenjuje stavak 3. članka 267. (Krivotvorenje isprava).

14) Par. 303. a. glasi:

(1) Tko protupravno podatke (iz članka 202a. st.2.) izbriše, zataji, učini neupotrebljivima ili izmijeni, kaznit će se kaznom zatvora do dvije godine ili novčanom kaznom.

(2) Kažnjiv je i pokušaj.

15) Čl. 269, 271, 273, 274, 348. KZ-a Njemačke, čl. 462-5. i 462-6. KZ-a Francuske, pog. 33. čl. 1-6. KZ-a Finske., čl. 509 - 4. i 509 - 5. KZ-a Norveške.

Djelo je namjerno. Namjera obuhvaća svijest i znanje o korisniku računalnih podataka, odnosno da se djelom prouzroči znatna šteta. Za voljni element nužno je postojanje posebne namjere, pa se djelo može počiniti samo s izravnom namjerom.

Stavak 3.

U odredbi stavka 3. inkriminira se svaka neovlaštena izrada, nabavka, prodaja, posjedovanje ili činjenje drugom dostupnim posebnih naprava, sredstava, računalnih programa ili računalnih podataka stvorenih ili prilagođenih radi počinjenja kaznenog djela iz st. 1. i 2. ovog članka.

Ovdje, kao i kod kaznenog djela iz čl. 393. st. 5. zakonodavac nastoji osigurati kaznenopravnu intervenciju u ranijoj fazi, prije počinjenja nekog drugog kaznenog djela (iz st. 1. i 2. ovog članka). Kazneno djelo je nesamostalno (delictum preparatum) u slučaju kad njegov počinitelj ostvari djelo iz st. 1. ili st. 2. Djelo je i formalni delikt, iscrpljuje se samom, alternativno određenom, radnjom počinjenja,

Kazneno djelo je namjerno, a namjera obuhvaća svijest o poduzimanju jedne ili više radnji počinjenja, s ciljem da se stvore uvjeti ili mogućnosti za kasnije počinjenje djela iz st. 1. ili 2. ovog članka.

Stavak 4.

Predmeti namijenjeni za počinjenje kaznenog djela iz st. 1. ili 2. (instrumenta sceleris) obvezno se oduzimaju, neovisno o njihovu vlasništvu, a u smislu odredbe čl. 78. KZ-a.

2. 3. Računalna prijevara

Temelj za ovo kazneno djelo je članak 8. Konvencije (Prijevara u vezi s kompjutorom).[16] Prema Objašnjenjima Konvencije, svrha ovog članka je kriminalizacija bilo kakve neprikladne manipulacije tijekom postupka obrade podataka s namjerom da se prouzroči nezakoniti prijenos imovine.

Stavak 1.

Radnja počinjenja temeljnog oblika kaznenog djela računalne prijevare je neovlašteno utjecanje na ishod elektronske obrade podataka, neovlaštenim unošenjem, oštećenjem, izmjenom, prikrivanjem računalnog podatka ili programa ili na drugi način utjecanjem na ishod elektronske obrade podataka i to s ciljem da se sebi ili drugome pribavi protupravna imovinska korist i time drugom prouzroči imovinska šteta.

Usporedbom opisa dispozicije st. 1. čl. 395. KZ-a i čl. 8. Konvencije uočava se da je opis djela iz st. 1. ovog članka nepotpun i neprecizan. U čl. 8. Konvencije određeni

16) Računalna prijevara (Članak 395. KZ-a) glasi:

(1) Tko neovlašteno unese, ošteti, izmijeni ili prikrije računalni podatak ili program ili na drugi način utječe na ishod elektronske obrade podataka s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist i time drugome prouzroči imovinsku štetu, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

(2) Ako je kaznenim djelom iz stavka 1. ovoga članka pribavljena imovinska korist koja prelazi 10.000 KM, počinitelj će se kazniti kaznom zatvora od dvije do deset godina.

(3) Ako je kaznenim djelom iz stavka 1. ovoga članka pribavljena imovinska korist koja prelazi 50.000 KM, počinitelj će se kazniti kaznom zatvora od dvije do dvanaest godina.

(4) Tko kazneno djelo iz stavka 1. ovoga članka počini samo s ciljem da drugoga ošteti, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

su bitni elementi inkriminacije. Stranama potpisnicama Konvencije sugerira se usvajanje zakonskih mjera kojima će se u unutarnjem zakonodavstvu kaznenopravno sankcionirati „namjerni čin neovlaštenog uzrokovanja štete na imovini drugog". Djelo se po Konvenciji može počiniti „bilo kakvim unošenjem, mijenjanjem, brisanjem ili činjenjem neuporabljivim računalnih podataka" ili „bilo kakvim ometanjem funkcioniranja računalnog sustava".

Alternativno su u st. 1. čl. 395. KZ-a propisane sljedeće djelatnosti: unošenje, kao upisivanje, snimanje, unos novog podatka, s tim da takva promjena mora u bitnoj mjeri utjecati na sadržinu postojećeg računalnog sustava. Oštećenje je privremeno, djelomično, kratkotrajno onesposobljavanje funkcioniranja računalnog sustava kroz izazivanje kvarova na pojedinim dijelovima, vezama ili sklopovima, pri čemu se prvobitna funkcionalnost i uporabljivost može vratiti zamjenom pokidanog dijela novim dijelom ili njegovom popravkom. Izmjena je brisanje postojećih podataka ili njihovo prepravljanje, krivotvorenje, preinačenje na bilo koji način. Prikrivanje je sklanjanje nekog od podataka (onog koji ima bitan značaj) i njegovo činjenje nedostupnim zauvijek ili za određeno vrijeme ostalim korisnicima računalnih sustava. Prikrivanje postoji kada se ne unese kakav podatak od strane osobe koja je bila obvezna na njegovo unošenje u računalni sustav. To može biti i bilo koja druga radnja podobna i dovoljna da u značajnijoj mjeri utječe na ishod sustava elektronske obrade podataka.[17] Temeljna primjedba ovakvoj dispoziciji je u tome što se u obilježje djela unosi i „svaki drugi način" njegova počinjenja, čime se ugrožava pravno načelo određenosti opisa kaznenog djela (nullum crimen sine lege, nulla poena sine lege certa).

Od kaznenog djela prijevare iz čl. 294. KZ-a, ovo kazneno djelo razlikuje se u tome što počinitelj, time što „izmijeni tuđe računalne podatke ili računalne programe", ne dovodi „nekoga" (fizičku osobu)"u zabludu ili ga održava u zabludi", a niti je djelom iz ovog članka taj drugi doveden u položaj da „na štetu svoje ili tuđe imovine nešto učini ili ne učini".

Objekt kaznenog djela su tuđi računalni podaci ili računalni programi. Trebalo je po ugledu na čl. 8. Konvencije u opis djela umjesto „računalni podaci ili računalni programi", unijeti izraze „računalni podaci ili računalni sustavi", sukladno njihovom značenju utvrđenom u čl. 1. Konvencije. Iz ovog razloga, opravdano je pitanje nije li inkriminacija iz čl. 395. st. 1. nepotpuna, jer u sebi ne uključuje računalnu prijevaru bilo kojom radnjom ometanja funkcioniranja računalnog sustava.

Da bi radnje iz st. 1. ovog članka predstavljale radnje počinjenja kaznenog djela, potrebno je da su poduzete s ciljem da se sebi ili drugom pribavi protupravna imovinska korist, a za postojanje dovršenog kaznenog djela nije nužno da je taj cilj i ostvaren.

Posljedica djela je prouzročenje imovinske štete drugom. Pojam imovinske koristi i štete uzima se u istom značenju kao i kod kaznenog djela prijevare iz čl. 294. KZ-a.

I ovdje u opisu djela postoji nelogičnost; s jedne strane za njegovo ostvarenje dovoljno je utvrditi da se ono čini iz koristoljubivih pobuda, dakle korist i ne mora biti ostvarena, a s druge strane, da bi djelo postojalo, nužno je da je drugome prouzročena šteta. Taj drugi dio je suvišan.

Kazneno djelo može se počiniti samo s namjerom, pri čemu se traži specijalna namjera, dok je za prouzročenje štete drugom dovoljan nehaj.

17) Petrović, B.- Jovašević, D., Krivično pravo II, Pravni fakultet Univerzitet u Sarajevu, 2005., str. 326-327.

Stavak 2. i 3.

U stavku 2. i 3. propisani su teži oblici temeljnog kaznenog djela i oni su kvalificirani isključivo visinom pribavljene protupravne imovinske koristi. Oni postoje ako je počinjenjem kaznenog djela iz st. 1. pribavljena imovinska korist koja prelazi 10.000 KM (st. 2.), odnosno 50.000 KM (st. 3.). Riječ je o djelima kvalificiranim težom posljedicom, pa se za njih odgovara ako se posljedica može pripisati nehaju počinitelja, ali je moguće da ova korist bude obuhvaćena i njegovom namjerom.

Stavak 4.

Ovo djelo počini tko kazneno djelo iz stavka 1. počini samo s ciljem da drugog ošteti. Razlika između st. 1. i 4. samo je u motivu počinjenja kaznenog djela. Kod djela iz st. 1. motiv se sastoji u pribavljanju protupravne imovinske koristi, dok počinitelj djelo iz st. 4. čini s ciljem oštećenja drugoga. Kazneno djelo iz st. 4. je lakši oblik kaznenog djela iz st. 1., a privilegirajuća okolnost je cilj s kojim je poduzeta radnja počinjenja. I ovaj oblik kaznenog djela može se počiniti samo s izravnom namjerom.

Iako je riječ o posebnom obliku kaznenog djela prijevare, zakonodavac ovu vrstu prijevare smatra težom od one iz čl. 294. KZ-a. To proizlazi kako iz propisanih kazni za temeljni oblik kaznenog djela (za prijevaru je to zatvor do tri godine, a za računalnu prijevaru, zatvor od šest mjeseci do pet godina), tako i iz visine pribavljene koristi kod kvalificiranih oblika (kod prijevare prelazi 30.000 KM, kod računalne prijevare prelazi 50.000 KM).

3. ZAKLJUČAK

Propisivanje kaznenih djela protiv sustava elektronske obrade podataka posljedica je razvitka informacijskih tehnologija, širenja njihove primjene u svim sferama života i s tim povezanim sve učestalijim i opasnijim napadima na sustav elektronske obrade podataka, bilo da su ti napadi poduzeti kako bi se narušila sigurnost, pouzdanost i dostupnost računalnih podataka ili programa, odnosno onemogućio ili otežao rad ili korištenje računalnih sustava, programa, podataka ili komunikacija ili kako bi se uz pomoć računalnih sustava, podataka ili programa, odnosno njihovom zloporabom postigli neki drugi protupravni ciljevi.[18] Zaštita od kompjutorskog kriminaliteta postaje važnom funkcijom društva, jer se sa svakom inovacijom javljaju nove zloporabe počinjene na kompjutorima ili uz njihovu pomoć. Susrećemo se na svim lokalnim, nacionalnim i regionalnim razinama i na svjetskim razinama. Tome puno prdonosi digitalni oblik dostupnih podataka i informacija, a isto tako da se kaznena djela mogu počiniti daljinskim pristupom, korištenjem, upravljanjem i manipuliranjem podacima. Pogoduje im, također, okolnost da se u istim pojavama i procesima nalazi i prepleće dopušteno i nezakonito, a učinci se postižu istim sredstvima i podjednakim metodama i postupcima koji se koriste u svakodnevnom radu i korištenju informatičke tehnologije. Trebalo je vremena da se u razvijenim sredinama uvidi kako je društvena štetnost od kompjutorskih zloporaba takva da je riječ o postupcima kojima se ugrožavaju „elementarne vrijednosti društvenog i pravnog poretka, koje su nužne za zajednički život, pa je prijeko potrebno da se njihova zaštita osigura sredstvima kaznenog prava, njegovim sankcijama kao naj-

18) Tako: Komentari kaznenih zakona Bosne i Hercegovine, Knjiga II, Sarajevo, 2005., str. 1279.

težim društvenim prinudnim mjerama", što je dovelo i do zaključka „da je takva mjera nužna i da je samo ona adekvatan odgovor na jedno ponašanje pojedinca koje društvo ne može tolerirati i za koje ponašanje neki drugi lakši oblik pravnog reagiranja ne bi odgovarao".[19]

Nova informatička tehnologija, uz sve svoje prednosti, omogućila je, s jedne strane, da se tradicionalne kaznenopravne povrede (primjerice: krađe, oštećenja, prijevare, krivotvorenja) čine na potpuno nov i bitno drukčiji način nego ranije, dok je, s druge strane, donijela i nove oblike kompjutorskog kriminala kojima se više ne ugrožavaju već tradicionalni objekti kaznenopravne zaštite, već također i nova netjelesna dobra, kao što su kompjutorski podaci i kompjutorski programi. Pojedini autori smatraju da se kod „kompjutorskog kriminala" jednom „savršenom zločinu suprotstavlja nesavršeno kazneno pravo"[20]. Da bi se riješilo postojeće stanje i popunile pravne praznine, umjesto proširenja opisa postojećih kaznenih djela (što bi bilo u kontradiktornosti s načelom zakonitosti i zabranom analogije in malam partem u kaznenom zakonodavstvu) mnoge su zemlje, među kojima je i Bosna i Hercegovina, donijele posebne kaznenopravne odredbe u borbi protiv kompjutorskog kriminala. Ova kaznena djela, kako je uvodno utvrđeno, propisana su u glavi XXXII. KZ FBiH i glavi XXXII. KZ BD BiH, kao i u okviru pojedinih glava KZ RS.

Zajednička obilježja ove Glave kaznenih djela su: Objekt zaštite je određen kao sigurnost računalnih podataka ili informacijskog sustava u cjelini ili njegovog pojedinog dijela, Počinjenje kaznenog djela uz pomoć ili uporabu kompjutora, Posebnost počiniteljevih radnji kojima se osigurava pristup kompjutorskom sustavu, proširuje taj pristup kako bi mogao dalje djelovati, poduzima druge radnje ovisno o svojim namjerama (pribaviti, izmijeniti, uništiti podatke ili programe, itd.) i ukloniti dokaze o poduzetim radnjama, Posebnost znanja i specijalizacija na strani počinitelja ovih kaznenih djela (tako, primjerice, Jedinica za borbu protiv kompjutorskog kriminala FBiH, razlikuje pet skupina počinitelja ovih kaznenih djela: čisti hakeri, unutrašnji hakeri, hakeri kriminalci, hakeri industrijski špijuni, hakeri u funkciji stranih obavještajnih službi)[21], Namjera počinitelja kao subjektivni element koja se ogleda u namjeri pribavljanja za sebe ili drugog kakve koristi ili nanošenja kakve štete drugoj fizičkoj ili pravnoj osobi, Ova kaznena djela, nadalje, čine se prikriveno, s većom ili manjom razlikom između radnje počinjenja i posljedice i ostaju neotkrivena sve dok oštećenik ne pretrpi štetu u računalnim podacima ili sustavu.

U radu su obrađena obilježja kaznenih djela: oštećenje računalnih podataka i programa iz čl. 393. KZ F BiH, računalno krivotvorenje iz čl. 394. KZ F BiH i računalna prijevara iz čl. 395. KZ F BiH. Izvršena je usporedba s odredbama Konvencije o kibernetičkom kriminalu iz 2001. g. koja je stupila na snagu 2004. g. Učinjeni su određeni prijedlozi de lege ferenda, ukazano je na razgraničenja u pogledu odnosa s drugim kaznenim djelima iz KZ FBiH. Naziv kaznenog djela iz čl. 393. KZ FBiH, radi usuglašavanja s Konvencijom, trebalo bi izmijeniti u „Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava, a sadašnji nelogični raspored stavaka 1. i 2. čl. 393. trebalo bi zamijeniti tako da st. 2. bude stavak 1., a stavak 1. postane stavak 2. ovog članka. Riječ je o dva potpuno odvojena nedopuštena ponašanja.

19) Bačić, F., Kazneno pravo, Opći dio, Informator, Zagreb, 1995. str. 90.

20) Tako, Krapac, D., Kompjutorski kriminalitet, Zagreb, 1992. str. 39.

21) Više o tome, Dragičević, D., op. cit. str. 72 - 76.

U glavi XXXII. KZ FBiH propisana su još kaznena djela: „Ometanje rada sustava i mreže elektronske obrade podataka" (čl. 396.), kojim se štite nesmetani rad sustava i elektronske obrade podataka, kazneno djelo „Neovlašteni pristup zaštićenom sustavu i mreži elektronske obrade podataka" (čl. 397.), kojim se štiti sigurnost sustava i elektronske obrade podataka i kazneno djelo „Računalna sabotaža" (čl. 398.), kojim se štite računalni sustavi i normalno odvijanje postupaka računalne obrade podataka u određenim subjektima od postupaka poduzetih s ciljem onemogućavanja ili znatnog ometanja njihovog rada. Navedena kaznena djela predstavljaju kaznena djela protiv povjerljivosti, integriteta i dostupnosti kompjutorskih podataka i sustava.

Iako Bosna i Hercegovina još nije potpisala Konvenciju o kibernetičkom kriminalu, naše je kazneno zakonodavstvo u većoj mjeri usklađeno s odredbama ove Konvencije. De lege ferenda trebalo bi propisati kazneno djelo „Dječja pornografija na računalnom sustavu ili mreži" i proširiti zakonski opis kaznenog djela „Povreda ravnopravnosti čovjeka i građanina" iz čl. 177 KZ-a, posebnim stavkom o djelu rasne i ksenofobične naravi počinjenim putem računalnog sustava.

Određene izmjene trebalo bi izvršiti i u Zakonu o kaznenom postupku kako bi se stvorile pretpostavke za uspostavljanje tehničkog sustava nadzora i presretanja komunikacija u slučajevima predviđenim zakonom.

Međutim, neprekidne promjene zahtijevaju stalno preispitivanje postojećeg stanja i prilagodbe u kibernetičkom prostoru. Zbog toga samo implementiranje međunarodnih kaznenopravnih odredbi iz Konvencije u našem zakonodavstvu nije dovoljan jamac informacijske sigurnosti i zaštite od kompjutorskog kriminala. Kaznena djela kompjutorskog kriminala u velikom broju su transnacionalnog karaktera i upravo zbog toga međunarodnopravna usklađenost, suradnja i pomoć pri otkrivanju i progonu počinitelja temeljni je preduvjet uspješne borbe protiv kompjutorskog kriminala. Zbog toga u skoroj budućnosti može se očekivati da će broj država koje će ratificirati i implementirati Konvenciju o kibernetičkom kriminalu u nacionalnim zakonodavstvima biti daleko veći.

Pri tome, kaznenopravna zaštita koja jest i ostaje iznimno važno sredstvo u borbi protiv kompjutorskog kriminala, ne smije biti prepuštena sama sebi, niti smije biti jedini odgovor društva na zloporabe. Ona mora biti podjednako praćena i podržavana drugim društvenim mjerama, zahvatima i aktivnostima koje će odvraćati potencijalne počinitelje, omogućavati sprječavanje kriminalnih radnji i njihovo brzo otkrivanje. Tako će se postići da kaznenopravna zaštita i pretjerana kriminalizacija, pored sprječavanja nepoželjnog, ne sputava nesmetano funkcioniranje, korištenje i stalni razvitak informacijskih sustava i informacijskog društva.

CRIMINAL ACTS AGAINST THE ELECTRONIC SYSTEM OF DATA PROCESSING IN PENAL CODE OF THE FEDERATION OF BOSNIA AND HERZEGOVINA

Summary

The ground for the incriminations comprised in chapter XXXII "Criminal Acts against the Electronic System of Data Processing" in Penal Code of the Federation of Bosnia and Herzegovina is set in the Convention on Cybernetic Crime from the year 2001. Author has made a legal analysis of provisions under Articles 393, 394 and 395 of the Penal Code which provide for criminal acts against confidentiality, integrity and availability of computer data and systems and has compared them with the respective provisions under Articles 2-6, 7 and 8 of the Convention of Council of Europe. In the paper, several *de lege ferenda* prepositions were made in respect to existing incriminations, as well as in respect to enactment for new incriminations, child pornography in computer system or computer network, and racial and xenophobic discrimination through computer system, pursuant to the additional Protocol of the Convention on Cyber Crime.