Mr. se. Goran Vojković
Marija Štambuk-Sunjić,
asistent Pravnog fakulteta u Splitu

KONVENCIJA O KIBERNETIČKOM KRIMINALU I KAZNENI ZAKON REPUBLIKE HRVATSKE

UDK: 343.791 (497.5)
Primljeno: 01. 10. 2005.
Izvorni znanstevni članak

Računalna revolucija donijela je nove oblike društveno neprihvatljivog ponašanja koje je trebalo na odgovarajući način kriminalizirati. Izmjenom i dopunom Kaznenog zakona Republike Hrvatske koja je stupila na snagu 1. listopada 2004. u hrvatski pravni sustav implementirane su odredbe Konvencije o kibernetičkom kriminalu i Dodatnog protokola te Konvencije. Time je Republika Hrvatska kriminalizirala čitav niz društveno neprihvatljivih ponašanja vezanih uz računala i računalne mreže, a opisi nekih postojećih kaznenih djela vezanih uz računala i računalne mreže upotpunjeni su i usavršeni.

Članak navodi i detaljno obrazlaže cyber-kaznena djela unesena u hrvatski Kazneni zakon temeljem Konvencije o kibernetičkom kriminalu i Dodatnog protokola te analizira njihove specifičnosti.

1. UVOD

Računalna revolucija koja se zahuktala osamdesetih i posebno devedesetih godina prošlog stoljeća te širenje globalne svjetske računalne mreže - Interneta donijeli su (kao i gotovo svako novo tehnološko dostignuće) nove oblike društveno neprihvatljivih ponašanja, a koje je trebalo na odgovarajući način kriminalizirati.

Pokazalo se, međutim, kako nacionalna zakonodavstva više nisu dostatna za djelotvorno reguliranje sve većeg broja novih društvenih odnosa koji traže pravnu regulaciju. Naime, suvremeni svijet, povijesno gledano, spada u postmodernu eru, čija je bitna specifičnost da svi ozbiljni problemi društva postaju globalni (za razliku od modernog društva čije je bitno obilježje bilo nacionalno).

Niti kroz povijest, a niti u današnjim danima, nijedan normativni sustav nije uspio do kraja obuhvatiti sve relevantne društvene odnose, a to su u pravu oni odnosi koji su "važni za opstanak i dobrobit društva, koji sadrže snažne sukobe interesa i koji su izvanjski kontrolabilni"[1]. Postavlja se pitanje kada neke društvene odnose postaje opravdano pravno regulirati. U svakom pravnom sustavu postoje, naime, područja u pravnim prazninama.

S obzirom da se računala i računalne mreže danas mogu iskoristiti za izvođenje velikog broja potpuno neprihvatljivih i društveno iznimno opasnih ponašanja, bilo je potrebno žurno neka ponašanja kriminalizirati. U razdoblju modernog društva kriminalizacija nekog ponašanja odvijala se u tri faze:

[1] Visković, Nikola: *Teorija države i prava,* Zagreb, 2001. str. 233.

- Prva traje 5-10 godina i to je faza pravne regulacije, tj. izrade, iščitavanja i izglasavanja zakona.
- Nakon toga nastupa drugi period, a to je period tzv. sudskog eksperimentiranja. To je jako važno razdoblje u kojem se ispituje hoće li norme zaživjeti u društvu ili će ostati mrtvo slovo na papiru.
- Konačno dolazi i do treće faze, u kojoj se sada na osnovi iskustva provedbe zakona u praksi pristupa ponovno normativnosti i popunjava se ili mijenja zakonski tekst.

U današnjoj postmodernoj eri, brzina (odn. sporost) kriminaliziranja koja se do prije koju godinu smatrala "normalnom" jednostavno je daleko od prihvatljive. U suzbijanju novih oblika društveno neprihvatljivih ponašanja međunarodna zajednica treba djelovati koordinirano i to u dva smjera:

- brzim donošenjem odgovarajućih ujednačenih kaznenih propisa u što više država, kako bi se izbjegla mogućnost vršenja kaznenih djela iz zemlje koja nema odgovarajuće propise,
- međunarodnom suradnjom nacionalnih policija.

Sto se tiče međunarodne policijske suradnje, ona je danas prema podacima koje redovno pratimo u tisku veoma intenzivna, posebno na području razbijanja lanaca za distribuciju dječje pornografije.

Ostaje problem izjednačavanja kaznenih zakonodavstava. Jedan od ključnih događanja na tom planu je stupanje na snagu Konvencije o kibernetičkom kriminalu[2] (dalje: Konvencija) kojom se regulira potreba vođenja zajedničke kaznene politike u sferi borbe protiv računalnog kriminala. Republika Hrvatska je ratificirala Konvenciju te njene odredbe unijela u svoj Kazneni zakon[3] (dalje: KZ) donošenjem Zakona o izmjenama i dopunama kaznenog zakona[4] (dalje: Zakon o izmjenama i dopunama KZ-a), a koji je stupio na snagu 1. listopada 2004. godine.

2. KORIŠTENJE POJMA CYBER-KRIMINAL I KIBERNETIČKI KRIMINAL

Svakako smatramo potrebnim navesti kako je u Republici Hrvatskoj napravljena mala terminološka zbrka lošim prijevodom Konvencije - engleski naziv *Convention on Cybercrime* preveden je kao *Konvencija o kibernetičkom kriminalu,* mada riječ kibernetika, engl. *cybernetics*[5] nije istoznačnica riječi *cyber*\ Kibernetiku bi najkraće mogli definirati kao "sustavno proučavanje komunikacije i upravljanja u organizacijama svih vrsta"[6], a za cyber još ne postoje precizne definicije, no Rječnik stranih riječi navodi daje *cyber* prvi element u riječima koji označava što vezano uz svijet prividne stvarnosti koji nastaje pomoću kompjutera.[7] Također navedimo kako za termin *cyber* još ne postoji odgovarajući prijevod na hrvatski jezik.

"Narodne novine — Međunarodni ugovori", br. 9/02.

[3] "Narodne novine", br. 110/97, 28/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04 i 84/105.

[4] Narodne novine", br. 105/04.

[5] Riječ kibernetika (engl. Cvbernetics, fran. Cybernetique, njem. Kvbernetik) potječe iz grčkog kvbernetikg: kormilarska vještina = kvbernetes: kormilar.

[6] Deutsch, Karl W.: *The Nerves of Government: Mođels ofPolitical Communication and Control,* 2nd ed.. New York, 1966., str. 76.

[7] Anić, Vladimir — Goldstein, Ivo: *Rječnik stranih riječi,* Zagreb, 2004.

Stoga smatramo kako je termin "kibernetički kriminal" pogrešan prijevod. A kako nama najrazumljiviji termin "računalni kriminal" ne obuhvaća sve oblike društveno neprihvatljivog ponašanja koje regulira Konvencija (prema Konvenciji, računalna kaznena djela tvore grupu u koje ulaze računalno krivotvorenje i računalna prijevara); smatramo da tu grupu kaznenih djela treba jednostavno zvati *cyber-kriminal,* odnosno *cyber-kaznena djela.*

Termin kibernetika treba ostaviti tamo gdje spada - kao naziv za znanost o upravljanju i vezi, a koja spada u grupu tzv. sustavnih znanosti.

Svakako želimo naglasiti da pod pojam cyber-kaznena djela treba svrstavati samo kaznena djela kod kojih je uporaba računala ili računalne mreže bitna za biće kaznenog djela,[8] a ne sva kaznena djela u kojima se na neki način kao sredstvo izvršenja pojavljuje računalo s pripadnom perifernom opremom. Tako primjerice kazneno djelo krivotvorenja novca *nije* računalno kazneno djelo bez obzira da li se počinitelj prilikom krivotvorenja novca služio računalom - bit tog kaznenog djela je izrada lažnog novca ili preinačenje pravog novca s ciljem da ga stavi u optjecaj, a računalo (uključujući skener i pisač) se tu pojavljuju samo kao tehničko sredstvo za lakše počinjenje kaznenog djela.

3. KONVENCIJA O KIBERNETIČKOM KRIMINALU

Konvencija o kibernetičkom kriminalu predstavlja oblik međunarodnog ugovora. Međunarodni ugovori važan su izvor međunarodnog prava kojim se uređuju međusobni odnosi između subjekata međunarodnog prava.[9] No, u međunarodnom pravu naziv "ugovor" upotrebljava se u generičkom smislu koji označava sve međunarodne akte ove vrste.[10]

U doktrini se smatra da ugovori predstavljaju najsvečanije i najvažnije sporazume, najčešće političke, dok konvencije predstavljaju više specijalne (tehničke) sporazume, a upotrebljavaju se i kada treba postaviti samo pravna pravila.

Konvenciju o kibernetičkom kriminalu donijelo je Vijeće Europe[11] 23. studenoga 2001. godine,[12] a stupila je na snagu 1. srpnja 2004. godine. Konvenciju je potpisalo 38 država (među njima i nečlanice Vijeća Europe: Kanada, Japan, Južna Afrika i Sjedinjene Države), a ratificiralo ju je 11 država: Albanija, Bugarska, Cipar,

---

[8] Biće kaznenog djela jest ono što je tipično za neko kazneno djelo, po čemu se ono razlikuje od drugih kaznenih djela. To je skup svih obilježja nekog kaznenog djela. Vidi opširnije: Horvatić, Željko - Novoselec, Petar: *Kazneno pravo — opći dio,* Zagreb, 2001. str. 170.-173.

[9] Različite su definicije međunarodnog ugovora, tako npr.: "Dvostrani pravni poslovi međunarodnog prava nazivaju se međunarodnim ugovorima." - Andrassv, Juraj: *Međunarodno pravo,* VI. izd., Zagreb, 1976., str. 319.; "Međunarodni se ugovor sastoji u suglasnosti dvaju ili više subjekata međunarodnog prava s ciljem da postigne određeni učinak po međunarodnom pravu, stvarajući odnos prava i dužnosti između njegovih stranaka." — Degan, Vladimir-Đuro: *Međunarodno pravo,* Rijeka, 2000., str. 121. Opširnije: *Bečka konvencija o pravu ugovora između država i međunarodnih organizacija ili između međunarodnih organizacija* iz 1986. godine, "Narodne Novine - Međunarodni ugovori", br. 1/94.

[10] Vijeće Europe osnovano je 1949. godine s ciljem uspostavljanja uskih veza među državama članicama, ostvarivanja načela koja su njihova zajednička baština i unapređivanja njihovog gospodarskog i socijalnog napretka. Vijeće Europe ne donosi propise koji su izravno obvezujući u državama članicama, već samo priprema ugovore koje države članice moraju ratificirati.

[11] Brojni vrijedni podaci o konvencijama Vijeća Europe dostupni su na Internet adresi: http://conventions.coe.int.

Danska, Estonija, Hrvatska, Luksemburg, Mađarska, Makedonija, Rumunjska i Slovenija.[13] Vidljivo je da među državama koje su ratificirale konvenciju još uvijek nema velikih tehnološki razvijenih država, a upravo će o njima ovisiti uspjeh konvencije na globalnoj razini. I dok se činjenica kako su većina europskih država koje su ratificirale Konvenciju nove članice EU ili zemlje kandidati može opravdati time kako te države upravo zbog približavanja EU imaju prilično zahuktan i brz zakonodavni mehanizam - nedostatak ratificiranja od strane SAD-a ima političku pozadinu. Iako je još 17. studenoga 2003. predsjednik Bush proslijedio Konvenciju Senatu s prijedlogom da se ratificira, zbog brojnih prosvjeda pojedinaca i nekih udruga koji smatraju da Konvencija krši ustavna prava američkih građana te da se njene odredbe mogu zloporabiti - do ratificiranja još nije došlo. Izvršna vlast u SAD i dalje drži kako Konvenciju treba ratificirati - tako primjerice Ministarstvo pravde na posebnoj Internet stranici opsežno obrazlaže povijest i svrhu Konvencije.

Ova Konvencija spada u krug takozvanih okvirnih konvencija - njene odredbe nisu izravno primjenjive, tako da bi ih svaka država trebala implementirati u vlastito zakonodavstvo.

4. DODATNI PROTOKOL UZ KONVENCIJU O KIBERNETIČKOM KRIMINALU O KRIMINALIZACIJI AKATA RASIZMA I KSENOFOBIJE POČINJENIH PUTEM RAČUNALNIH SUSTAVA

Dodatni protokol uz Konvenciju o kibernetičkom kriminalu o kriminalizaciji akata rasizma i ksenofobije počinjenih putem računalnih sustava (dalje: Dodatni protokol) donijelo je Vijeće Europe 28. siječnja 2003. godine. Do sada ga je potpisalo 28 država, ali su ga ratificirale samo četiri: Albanija, Cipar, Danska i Slovenija.[15] Treba napomenuti kako su SAD izjavile da ne namjeravaju ratificirati Dodatni protokol,[16] što će svakako bitno otežati njegovo globalno prihvaćanje.

Dodatni protokol zahtijeva, od zemalja sudionica, kriminalizaciju širenja rasističkih i ksenofobnih sadržaja putem računalnih sustava, kao i rasističko i ksenofobno obojane prijetnje i uvrede, te negiranje holokausta i ostalih genocida.

Zanimljivo je da Republika Hrvatska - mada još nije ratificirala Dodatni protokol (potpisala gaje 26. ožujka 2003.) - u svoje kazneno zakonodavstvo unijela jednu odredbu koja je izravno povezana s Protokolom - čl. 194 st 4. KZ-a (v. infra 5.5). Dakle, došlo je do primjene još uvijek neratificiranog Dodatnog protokola.

Postavlja se pitanje pravne snage takvog međunarodnog dokumenta koji nije ratificiran (za ovaj tip međunarodnog ugovora ratifikacija je, sukladno Ustavu Republike Hrvatske, uvjet njegovog stupanja na snagu)[17], a određene odredbe već su integrirane u zakon koji je na snazi.

---

[13] Stanje na dan 3. srpnja 2005.

[14] Vidi: http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm (03. 07. 2005.).

[15] Stanje na dan 3. srpnja 2005.

[16] "Sjedinjene Države ne vjeruju kako će konačna verzija Protokola biti sukladna ustavnim jamstvima. Stoga, Sjedinjenje države obavještavaju Vijeće Europe o tome kako neće postati stranka Protokola." - http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm (03. 07. 2005.)

[17] Prema čl. 139. st. 1. Ustava Republike Hrvatske ("Narodne novine" br. 56/90, 135/97, 8/98 - pročišćeni tekst, 113/00, 124/00 - pročišćeni tekst, 28/01, 41/01 - pročišćeni tekst), Hrvatski sabor potvrđuje međunarodne ugovore koji traže donošenje ili izmjenu zakona, međunarodne ugovore vojne i političke naravi i međunarodne ugovore koji financijski obvezuju Republiku Hrvatsku.

Moguće načine izražavanja pristanka država da budu vezane ugovorom gdje se ističe načelo slobodne dispozicije stranaka naglašava članak 11. Bečke konvencije o pravu međunarodnih ugovora iz 1969. godine[18] (u daljnjem tekstu BK 69): "Pristanak države da bude vezana ugovorom može biti izražen potpisivanjem, razmjenom isprava koje čine ugovor, ratifikacijom, prihvatom, odobrenjem ili pristupom, ili na bilo koji drugi ugovoreni način."

Potpisivanje je faza u donošenju međunarodnih ugovora koja, po pravilu, dolazi poslije završenih pregovora, kada je utvrđen konačni tekst ugovora, a sastoji se od toga što predstavnici država stavljaju svoje potpise na kraju teksta ugovora. U novijoj praksi država, međutim, i samo potpisivanje ugovora jest vrlo čest način izražavanja pristanka posebno kod dvostranih ugovora.

Pravnici su kroz povijest različito tumačili posljedice potpisanog, a još neratificiranog ugovora. Neki su isticali da "potpis moralno obvezuje vladu" (Hoijer), drugi su u njemu vidjeli "obećanje na obvezivanje" (Fauchille) dok je Cavare naglašavao faktičku vrijednost potpisivanja jer "njime završava delikatna faza pregovaranja u kojoj je ugovor ispitan sa svih stajališta i trebali bi postojati jaki motivi da se odbije ratifikacija".[19] No, u međunarodnoj literaturi naglašavalo se ponekad i pravno djelovanje neratificiranog ugovora. U prvom redu dolazi primjedba da ugovor može stupiti na snagu i potpisivanjem (bez obzira na to da li se i pored toga traži naknadna ratifikacija ili ne), ako se ugovornice suglase o tome. Cavare ističe i pravno djelovanje onih ugovora čija ratifikacija gubi svoj značaj jer se pojavljuje pošto je ugovor već izvršen.[20]

Ipak, velik broj mnogostranih ugovora predviđa ratifikaciju kao pristanak države da bude vezana ugovorom. Prema članku 14. BK 69. pristanak države da bude vezana ugovorom izražava se ratifikacijom: ako ugovor predviđa da se pristanak izrazi ratifikacijom; ako se na drugi način ustanovi da su se države pregovarateljice sporazumjele da će ratifikacija biti nužna; ako je predstavnik te države potpisao ugovor uz rezervu ratifikacije; ili ako namjera te države da potpiše ugovor uz rezervu ratifikacije proistječe iz punomoći njezina predstavnika ili je izražena tijekom pregovora.

Postoji međutim obveza poštivanja predmeta i cilja ugovora i prije njegova stupanja na snagu. To pravilo jasno ističe i sama BK 69, u članku 18.[21] Naime, vremenom je potpis pod rezervom ratifikacije postao "prvi korak" ka konačnom pristanku države. Zanimljivo je razmišljanje Lorda Me Naira: "Mada potpisan ugovor kojemu je potrebna i ratifikacija ne može stupiti na snagu dok se ne razmijene

---

[18] "Narodne Novine — Međunarodni ugovori", br. 16/93.

[19] Hoijer, O., *Les Traits Internationaia* t. I., Pariš 1928.pp.7; Fauchille, P, *Traite đe đroit international public* t. I. 3, Pariš 1926. pp.305; Cavare, L, *Le droit internationalpublicpositif,* t. II, Pariš 1951., pp. 59-84. — sve citirano prema Bartoš, Milan: *Međunarodno javno pravo — Ugovorno pravo,* Beograd, 1986., str. 204.-214.

[20] Bartoš, Milan: *Međunarodno javno pravo — Ugovorno pravo,* op. cit, str. 63.

[21] Cl. 18. BK 69 propisuje kako se država mora suzdržati od čina koji bi osujetili predmet i svrhu ugovora: ako je potpisala ugovor ili razmijenila isprave koje čine ugovor uz rezervu ratifikacije, prihvata ili odobrenja, sve dok jasno ne očituje namjeru da ne postane stranka tog ugovora; ili ako je *izrazila,* svoj pristanak da bude vezana ugovorom, u razdoblju prije stupanja ugovora na snagu i pod uvjetom da se to stupanje na snagu neopravdano ne odgodi.

ili ne deponiraju ratifikacije, ne smije se pretpostavljati daje potpis do ratifikacije bez ikakvog učinka. Postoji velika količina materijala (...) koji pokazuje da su države koje su potpisale ugovor pod rezervom ratifikacije prihvatile određena ograničenja svojih sloboda u vremenu koje prethodi njegovom stupanju na snagu."[22]

Stvarna situacija nastala u Republici Hrvatskoj činjenicom da je Dodatni protokol potpisan i primijenjen, po našem mišljenju mijenja pravnu narav ratifikacije - ona postaje neka vrst deklaratornog akta, jer je obveza koja iz nje proizlazi već realizirana. Naravno, ovo sve ne oslobađa Republiku Hrvatsku potrebe da se Dodatni protokol ratificira, pri čemu glavni razlog ratifikacije više nije implementacija normi Dodatnog protokola u nacionalno pravo, već stvaranje čiste i jasne pravne situacije.

5. NOVA KAZNENA DJELA

5.1. Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa i sustava - čl. 223 KZ.

Zakonom o izmjenama i dopunama KZ-a u potpunosti je promijenjen naslov i tekst čl. 223. KZ-a koji je regulirao oštećenje i uporabu tuđih podataka.

Tko unatoč zaštitnim mjerama neovlašteno pristupi računalnom sustavu, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine [čl. 223. st. l.J.

Ovim stavkom inkriminirano je ponašanje iz čl. 2. Konvencije - nezakoniti pristup. Ono što je za primjenu ovog članka u praksi veoma bitno jest formulacija "tko unatoč zaštitnim mjerama neovlašteno pristupi...", a kojom se određuje kako zakon štiti samo onaj sustav koji ima zaštitne mjere! Ukoliko se sustav ostavi potpuno otvorenim i nezaštićenim, dakle računalo potpuno dostupno ili npr. bežična računalna mreža na koju je moguće spajanje bez ikakve provjere, neće se ispuniti elementi za postojanje kaznenog djela.

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 [čl. 223. st. 2.J.

U pitanju je inkriminiranje ponašanja iz čl. 5. Konvencije - ometanje sustava.

U praksi su već brojni slučajevi koji se ovim stavkom inkriminiraju. Različitim tehnološkim postupcima se vrši "napad" na određeno računalo - najčešće generiranjem enormnog broja pristupa određenom računalu koje je spojeno na Internet.[23] Ovakvi napadi mogu blokirati Internet promet cijele države

---

[22] McNair, A.: *The Law ofTreaties,* London 1961., str.199., citirano prema Crnić Grotić, Vesna: *Pravo međunarodnih ugovora,* Rijeka, 2002., str. 33.-34.

[23] Među najpoznatijima je takozvani DDoS napad - tako je u travnju 2001. hrvatski Internet prostor bio gotovo blokiran snažnim napadima izvana. Hrvatsko Nacionalno središte za računalnu sigurnosti - CERT je objavilo na svojim web-stranicama 21. travnja 2001.: "Oko 18h počeo je jedan od do sada najvećih DDoS napada na hrvatski Internet prostor. Radi se o distribuiranom napadu uskraćivanja usluga, koji se sastoji u slanju velike količine paketa (bilo koje vrste) sa više različitih adresa na jedan ili više strojeva i koji za posljedicu ima iskorištavanje resursa objekta napada koji postaje onemogućen u obavljanju svojih primarnih aktivnosti. Radi se na otkrivanju svih izvora napada." - izvor: http://www.cert.hr/actualities.php?lang=hr&page=5 (03. 07. 2005.).

pa i kontinenta - te uzrokovati ogromnu štetu. Koji put napadi znaju biti i uže ciljani - npr. prema određenoj kompaniji ili nekoj e-mail adresi.

Bitan element ove inkriminacije je namjera[24] ("tko s ciljem..."), dakle neće biti odgovoran netko tko npr. nepažnjom isključi ključna računala davatelja Internet usluga i dovede do prekida komunikacije.

Svakako treba dodati kako je ovo je tipična inkriminacija gdje možemo pronaći jednu specifičnost cyber-kaznenih djela. Napadač tako može pustiti u distribuciju računalni crv koji će se raširiti na tisuće drugih računala, koja će onda, bez znanja svojih korisnika sudjelovati u napadu; dakle velika je mogućnost da se iskoristi tuđa infrastruktura u počinjenu kaznenog djela, a bez ikakvog znanja vlasnika ili korisnika te infrastrukture (koji naravno ne mogu kazneno biti odgovorni za zloporabu svoje opreme, a i posredno će biti pogođeni tom zloporabom - usporavanjem zaraženih računala i opterećenjem njihovih mrežnih veza).

(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 [čl. 223. st. 3.J.

U pitanju je inkriminiranje ponašanja iz čl. 4. Konvencije - ometanje podataka.

Ovdje je *ratio legis* zaštita od oštećivanja, izmjena, brisanja ili uništavanja tuđih računalnih podatka ili programa, čime se ovaj oblik imovine[25] štite slično kao i materijalne stvari. Računalni podaci danas često predstavljaju iznimno vrijednu imovinu; ne treba posebno obrazlagati kolika se šteta može učiniti uništavanjem podataka nekoj banci, pripremljenih stranica za tisak dnevnih novina, arhive poslovnih partnera trgovačkom društvu i sl.

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 [čl. 223. st. 4.J.

U pitanju je inkriminiranje ponašanja iz čl. 3. Konvencije - nezakonito presretanje, kojim se traži sankcioniranje neovlaštenog presretanja nejavnih prijenosa računalnih podataka prema računalnom sustavu, iz njega ili unutar njega (uključujući i elektromagnetske emisije iz računalnog sustava koji prenosi te računalne podatke), počinjen tehničkim sredstvom.

Ratio legis je zaštita nejavne komunikacije. Ovo kazneno djelo je, jednostavnim rječnikom rečeno, "računalni" ekvivalent neovlaštenog snimanja i prisluškivanja.

---

[24] Namjera, shvaćena kao znanje i htijenje bića kaznenog djela, jest temeljni oblik krivnje jer se kažnjava namjerna povreda svih pravnih dobara, a ne samo onih najvažnijih (što je slučaj kod nehaja).
Vidi opširnije o pojmu namjere u: Novoselec, Petar: *Opći dio kaznenog prava,* Zagreb 2004. str.226.-235.

[25] Imovina ima nekoliko značenja - gospodarsko, pravno, knjigovodstveno:
- u gospodarskom smislu: "Skup dobara koja pripadaju određenom subjektu."
- kao pravna kategorija: "Skup subjektivnih imovinskih prava predstavljenih jednim nositeljem."
- kao knjigovodstvena kategorija: "Imovina ima dva samostalna sastavna dijela. Jedno su prava, koja predstavljaju aktivu; a drugo su obveze, koje predstavljaju pasivu."
Prema: Vedriš, Martin — Klarić, Petar: *Građansko pravo,* Zagreb, 1998., str. 93.-97.

Posebno je zanimljivo da Konvencija, pa onda i hrvatski zakonodavac - pravilno inkriminiraju i neovlašteno presretanje elektromagnetskih emisija iz računalnog sustava koji prenosi računalne podatke - dakle izričito se zabranjuje prisluškivanje bežičnog prijenosa podataka te prisluškivanje žičnog prijenosa koje je moguće izvesti bez izravnog priključenja na komunikacijsku liniju.[26]

Po našem mišljenju ovo djelo bi *de lege ferenda* trebalo izričito proširiti i na neovlašteno presretanje elektromagnetske emisije iz svih računalnih sustava, ne samo onih koji prenose podatke. Naime, kako računalni procesori i monitori (posebno klasični s katodnom cijevi) emitiraju elektromagnetska zračenja, ona se uz odgovarajuću opremu mogu prisluškivati s udaljenosti do nekoliko desetaka metara.

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 [čl. 223. st. 5.J.

U pitanju je stavak koji uvodi kvalificirani oblik ovog 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.

Smatramo da će se kao mogući problem pojaviti određivanje "znatne štete". Naime, dok je određivanje da li je objekt radnje npr. računalni sustav tijela državne vlasti relativno jednostavno - ne vjerujemo kako će intenzitet vršenja ovog kaznenog djela biti toliki da će sudska praksa moći na odgovarajući način odgovoriti na pitanje kolika je "znatna šteta".

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 [čl. 223. st. 6.J.

Cilj kaznenopravne zaštite koju uvodi ovaj članak (a sukladno članku 6. Konvencije) jest sprječavanje stvaranja i širenja tržišta naprava i - u praksi puno češćih - specijaliziranih programa za počinjenje kaznenog djela iz stavaka 1-4.

Ono što bi ovdje trebalo biti transparentnije navedeno -jesu osobe koje su ovlaštene za posjedovanje pa u određenim uvjetima i razvoj tih alata: a to su stručnjaci koji se bave računalnom zaštitom, te stoga vrše analize alata postojećih na tržištu, a i razvijaju alate s kojima u dogovoru sa strankom pokušavaju napad na njen sustav u cilju isprobavanja zaštite. Smatramo da *de lege ferenda* treba ovo pitanje riješiti uvođenjem posebne licence.

---

[26] Još je 1819. godine danski fizičar Hans Christian Oersted primijetio da u blizini vodiča kojim teče električna struja magnetska igla poskakuje. Godine 1832. Englez Michael Faradav je otkrio da promjenjivo magnetsko polje proizvodi struju u vodiču koji je postavljen u to polje (elektromagnetska indukcija).
Stoga, s obzirom da komunikacijski kabel (npr. običan mrežni kabel koji povezuje osobno računalo s lokalnom mrežom) kod prijenosa podataka stvara elektromagnetsko polje oko sebe - uz odgovarajuće uređaje to se polje opet može pretvoriti u struju te prikladnom opremom prisluškivati komunikacija bez ikakvog fizičkog kontakta!

Navedimo još da Konvencija u čl. 6. spominje i računalne lozinke, pristupne šifre ili slične podatke, kojime bi se omogućilo pristupanje cjelini ili nekom dijelu računalnog sustava. U praksi možemo zamisliti i situacije u kojima npr. nezadovoljan radnik distribuira po Internetu pristupne šifre za računalni sustav, tako da bi *de legeferenda* trebalo kriminalizirati takve i slične radnje.[27]

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 sefčl. 223. st. 7.J.

Smatramo kako ovaj stavak ne treba posebno obrazlagati - u pitanju je uobičajena praksa kaznenog zakonodavstva.

Za pokušaj kaznenog djela iz stavka 1., 2., 3. ili 4. ovoga članka počinitelj će se kazniti [čl. 223. st. 8.J.

S obzirom da Konvencija u svom čl. 11. st. 2. traži da države stranke propišu kažnjavanje i za pokušaj kaznenog djela[28] iz st. 1-4, a kako prema kriteriju zapriječene kazne pokušaj nije kažnjiv,[29] trebalo je izričito propisati i kaznu za pokušaj.

5.2. Računalno krivotvorenje - čl. 223.a KZ

Ovo je potpuno novo kazneno djelo u Hrvatskom zakonodavstvu.

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 godinefčl. 223.a st. l.J.

U pitanju je inkriminiranje ponašanja iz čl. 7. Konvencije - računalno krivotvorenje.

U suvremenom poslovanju kako gospodarstva, tako i javne uprave te drugih osoba sve se češće koriste elektroničke baze podataka, tako se danas brojne evidencije i očevidnici vode primarno, pa i isključivo, u elektroničkom obliku. Mnoge od tih elektroničkih baza podataka imaju iznimnu vrijednost za pravne odnose. Izmjena, uništavanje, brisanje, činjenje neuporabljivim takvih podataka - pa i takve i slične akcije napravljene od osobe ovlaštene za uporabu takvih podataka, a kako bi se takvi lažni podaci uporabili - danas mogu prouzročiti velike štete i predstavljaju iznimnu društvenu opasnost.

---

[27] Djelomična zaštita postoji sukladno Zakonu o zaštiti tajnosti podataka ("Narodne novine", br. 108/96), no smatramo da današnja važnost zaporki (šifri) računalnih sustava zavrjeđuje zaštitu u sklopu Kaznenog zakona.

Pokušaj od dovršenog kaznenog djela razlikuje posljedica koja kod pokušaja ne nastaje, a nastupa kod dovršenog djela, koje se upravo zbog ostvarenja posljedice i smatra dovršenim. Samo kod tzv. namjernih kaznenih djela moguće je kažnjavanje za pokušaj. Vidi opširnije: Kurtović, Anita — Tomašević, Goran: *Osnove kaznenog prava i postupka,* Split, 2002., str. 87.-89.

[29] Članak 33. st. 1. KZ-a propisuje: "Tko s namjerom započne ostvarenje kaznenog djela, ali ga ne dovrši kaznit će se za pokušaj kaznenog djela za koje se po zakonu može izreći kazna zatvora od pet godina ili teža kazna, a za pokušaj drugog kaznenog djela samo kad zakon izričito propisuje kažnjavanje i za pokušaj."

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 [čl. 223. a st. 2.J.

Ovim stavkom se uvodi kvalificirani oblik kaznenog djela[30] računalnog krivotvorenja. I ovdje, kao u čl. 223. smatramo da se može pojaviti problem određivanja znatne štete.

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 [čl. 223. a st. 3.J.

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 [čl. 223. a st. 4.J.

Za pokušaj kaznenog djela iz stavka 1. i 3. ovoga članka počinitelj će se kazniti [čl. 223.a st. 5.J.

Obrazloženje uvođenja ovih triju stavaka gotovo je identično obrazloženju odgovarajućih stavaka čl. 223., navedenih u prethodnom podpoglavlju, stoga ih ovdje nećemo posebno navoditi.

5.3. Računalna prijevara - čl. 224.a KZ

Ovdje je također u pitanju potpuno novo kazneno djelo u hrvatskom zakonodavstvu. U Obrazloženju Konačnog prijedloga Zakona o izmjenama i dopunama Kaznenog zakona[31] stoji: "S obzirom da računalna prijevara obuhvaća niz specifičnih postupaka na koje nije moguće primijeniti inkriminaciju tradicionalne prijevare (u hrvatskom KZ to je čl. 224), npr. nema dovođenja u zabludu druge osobe već je suština zabranjenog djelovanja u nedopuštenoj manipulaciji računalnim podacima, odnosno u ometanju nesmetanog funkcioniranja računalnog sustava ili programa, bilo je potrebno propisati novo kaznenog djelo koje bi osiguralo zaštitu od pojavnog oblika čija je opasnost zbog razvitka tehnologije sve izraženija."

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 otežа 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 [čl. 224.a st. l.J.

U pitanju je inkriminiranje ponašanja iz čl. 8. Konvencije - računalna prijevara.

---

[30] "Kvalifikatorne okolnosti mogu se odnositi na modalitete radnje, svojstvo počinitelja ili objekta radnje, pobude, težinu posljedice i si." — natuknica "kvalifikatorne okolnosti" u: Horvatić, Željko (gl. urednik): *Rječnik kaznenog prava,* Zagreb, 2002.

[31] Vlada Republike Hrvatske, Klasa: 740-02/04-01/01, Urbroj: 5030106-04-8 od 8. srpnja 2004.

Bitan element ovog oblika računalne prijevare je pribavljanje protupravne imovinske koristi, a posljedica djela prouzročenje štete drugome. Pod ovo kazneno djelo će se moći svrstati razni oblici upada u računalne sustave u svrhu promjene stanja na bankovnim računima, računalne prijevare s kreditnim karticama, plaćanje lažnim brojevima kreditnih kartica i sl. Tu također mogu spadati i razne blokade računalnog sustava kako bi se onemogućila provjera valjanosti kartica, brisanje svoje loše kreditne povijesti iz baze podataka banke i sl.

Tko kazneno djelo iz stavka 1. počini samo s ciljem da drugoga ošteti, kaznit će se kaznom zatvora od tri mjeseca do tri godine [čl. 224.a st. 2.J.

U pitanju je privilegirani oblik kaznenog djela[32] iz st. 1. Posljedica djela je dakle i ovdje prouzročenje štete drugome, ali je cilj počinitelja da ošteti drugoga; dakle cilj nije stjecanje protupravne imovinske koristi. Ovo počinjenje štete jest i *differentia specifica* u odnosu na kazneno djelo iz čl. 223. st. 2. i 3. S obzirom da i ponašanje iz čl. 223. st. 2. i 3. uzrokuje štetu - ovdje bi se u praksi moglo dogoditi da dođe do nedoumica pod koje kazneno djelo određeno ponašanje svrstati. Smatramo kako bi *de legeferenda* trebalo ponašanja iz ovog stavka podvesti pod čl. 223.

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 [čl. 224. a st. 3.J.

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 [čl. 224.a st. 4.].

Za pokušaj kaznenog djela iz stavka 2. i 3. ovoga članka počinitelj će se kazniti [čl. 224.a st. 5.].

Obrazloženje uvođenja ovih triju stavaka također je gotovo identično obrazloženju odgovarajućih stavaka čl. 223., stoga ih ovdje nećemo posebno navoditi.

5.4. Dječja pornografija na računalnom sustavu ili mreži - čl. 197.a KZ

Hrvatski KZ je već u svom izvornom tekstu iz 1997. poznavao kaznena djela "iskorištavanje djece ili maloljetnih osoba za pornografiju" [čl. 196.] i "upoznavanje djece s pornografijom" [čl. 197.]. Međutim, zbog širenja distribucije dječje i maloljetničke pornografije putem Interneta, bilo je potrebno u KZ-u propisati posebnu inkriminaciju s primjerenom kaznom.

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

[32] "Privilegirajuće okolnosti mogu se odnositi na modalitete radnje, svojstvo počinitelja ili objekta radnje, pobude, težinu posljedice i si." - natuknica "privilegirajuće okolnosti" u: Horvatić, Zeljko (gl. urednik): *Rječnik kaznenog prava,* op.cit.

maloljetnike u seksualnom eksplicitnom ponašanju ili koji su fokusirani na njihove spolne organe, kaznit će se kaznom zatvora od jedne do deset godina [cl. 197. a st. l.J.

U pitanju je inkriminiranje ponašanja iz čl. 9. Konvencije - kaznena djela vezana uz dječju pornografiju (napominjemo kako Konvencija pod pojmom dječja pornografija podrazumijeva i maloljetničku pornografiju).

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 [čl. 197.a st. 2.J.

Bitan element ove inkriminacije je dakle činjenje pristupačnim djeci slika, audiovizualnih sadržaja ili drugih predmeta pornografskog sadržaja putem računalnog sustava (dakle računala), mreže (Interneta ili kakve druge mreže - npr. privatne bežične mreže ili lokalne mreže u školi) te medija za pohranu računalnih podataka (disketa, CD-ova, DVD-ova i drugih medija koje koriste računala).

Pornografski sadržaji danas su u pravilu veoma lako dostupni na Internetu. Slično tome, mediji za pohranu računalnih podataka s pornografskim sadržajem se mogu kupiti na gotovo svakom kiosku. No dok se kod kupnje CD-a ipak može provjeriti dob kupca, surfanje Internetom je u pravilu anonimno - pružatelj usluga ne zna tko sjedi za računalom koje pristupa npr. nekoj web-stranici. Pitanje je - što vlasnik sadržaja treba učiniti kako bi spriječio da djeca pristupaju pornografskom sadržaju? Postavljanje linka s pitanjem: "Da li ste stariji od 18 godina?", gdje se klikom na "da" dobiva dostup pornografskom sadržaju - sigurno nije pouzdana metoda. No, nažalost, još uvijek nema nekog globalnog odgovora na ovo pitanje - postoje neki neformalni standardi o označavanju web-stranica s pornografskim sadržajem, ali su vrlo parcijalni i daleko od nekog službenog standarda.

U svakom slučaju - čl. 197.a st. 2. uspješno se može primijeniti na slučajeve izravnog nuđenja djeci pornografskih sadržaja - ali što se tiče slučajeva kada sama djeca pretražuju Internet u potrazi za takvim sadržajima i ulaze na pornografske web-stranice lažno se predstavljajući punoljetnima, smatramo daje potrebno izvršiti dodatno i preciznije normiranje (a problem u cjelini rješavati na međunarodnoj razini uvođenjem odgovarajućih standarda).

Posebne naprave, sredstva, računalni programi ili podaci korišteni ili prilagođeni započinjenje kaznenog djela iz stavka 1. i 2. ovoga članka oduzet će se [čl. 197.a st. 3.J.

Ova odredba je jasna te smatramo da je ne treba posebno obrazlagati.

5.5. Rasna i druga diskriminacija - čl. 174. KZ-a

Izmjenama i dopunama KZ-a 2004. godine proširena je inkriminacija u čl. 174. st. 3. kaznenog djela "rasne i druge diskriminacije". Također, kazneno djelo dopunjeno je novim st. 4. kojim se inkriminira poricanje, znatnije umanjivanje, odobravanje ili opravdavanje kaznenog djela genocida ili zločina protiv čovječnosti[33], a učinjeno putem računalnog sustava. Kako se st. 4. ne može tumačiti bez st. 3., navodimo oba stavka.

[33] Definicija genocida izvorno se nalazi u čl. 2. Konvencije o sprečavanju i suzbijanju zločina genocida iz 1948. godine. Traži se postupanje s namjerom "da se u cijelosti ili djelomično uništi neka nacionalna, etnička, rasna ili vjerska skupina".

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 [čl. 174. st. 3.J.

Tko s tim 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 novčanom kaznom ili kaznom zatvora od tri mjeseca do tri godine [čl. 174. st. 4.J.

U pitanju je inkriminiranje ponašanja iz čl. 6. Dodatnog protokola - kojim se traži sankcioniranje distribucije ili dostupnosti (putem računalnog sustava ili na neki drugi način) javnosti onih materijala koji poriču, znatnije umanjuju, odobravaju ili opravdavaju djela koja predstavljaju genocid ili kazneno djelo protiv čovječnosti, onako kako je to definirano u međunarodnom pravu i priznato kao takvo putem konačnih i obvezujućih odluka Međunarodnog vojnog suda uspostavljenog Londonskim sporazumom od 8. kolovoza 1945., ili bilo kojeg drugog međunarodnog suda uspostavljenog putem relevantnih međunarodnih dokumenata, a čiju jurisdikciju ta stranka priznaje.

To znači da Dodatni protokol izričito propisuje kako se inkriminiranje treba odnositi na nacističke zločine počinjene tijekom II. svjetskog rata[34] te na novije zločine, počinjene primjerice u bivšoj Jugoslaviji i Ruandi, a za koje postoje odgovarajući međunarodni sudovi[35].

Internet, iznimno jednostavan medij za publiciranje raznih materijala; počeo se zloporabiti od strane pojedinaca i organizacija koje putem Interneta publiciraju i društveno neprihvatljive stavove, a među njima je i poricanje, znatnije umanjivanje, odobravanje ili opravdavanje kaznenog djela genocida ili zločina protiv čovječnosti.

Ne treba posebno obrazlagati kao je negiranje, odobravanje i opravdavanje genocida i zločina protiv čovječnosti u potpunosti neprihvatljivo. Stoga, smatramo da koliko god odredba čl. 174. st. 4. djelovala složena, koliko god bila teška za uporabu i dokazivanje, ta odredba ima svoje mjesto u KZ-u, posebno ako uzmemo u obzir kako je Hrvatska tijekom XX. stoljeća bila poprište brojnih tragičnih događaja koji se ne smiju zaboraviti.

"Zločin protiv čovječnosti jest neljudsko postupanje izvršeno u sklopu širokog ili sustavnog napada na civilno stanovništvo", a uključuje ubojstvo, istrebljenje, porobljavanje, mučenje, proganjanje i sl. Vidi opširnije: Novoselec, Petar: Opći dio kaznenog prava, op.cit, str. 498.-500.

[34] U Obrazloženju Konačnog prijedloga Zakona o izmjenama i dopunama Kaznenog zakona, op. cit, se navodi kako je negiranje ili veličanje holokausta kao iskrivljavanje povijesnih činjenica u praksi Europskog suda za ljudska prava ocijenjeno povredom čl. 17 Konvencije za zaštitu ljudskih prava i temeljnih sloboda

[35] "Međunarodni kazneni sud za teška kršenja međunarodnog humanitarnog prava na području bivše Jugoslavije od 1991." osnovan je 25. svibnja 1993.godine rezolucijom Vijeća sigurnosti br. 827. "Međunarodni kazneni sud za Ruandu" radi kaznenog progona osoba odgovornih za genocid i zločine protiv čovječnosti počinjenih od 1. siječnja 1994. do 31. prosinca 1994. na području Ruande i susjednih zemalja, osnovan je 8. studenog 1994. rezolucijom Vijeća sigurnosti br. 955.

Nadalje, smatramo kako bi Republika Hrvatska trebala što prije ratificirati Dodatni protokol te svoje kazneno zakonodavstvo još potpunije prilagoditi Dodatnom protokolu.

6. ZAKLJUČAK

U današnjem globalnom društvu bez kriminaliziranja određenih društveno neprihvatljivih ponašanja vezanih uz računala i računalne mreže na sličan način u što većem broju država - pravna zaštita protiv takvih ponašanja jednostavno ne može biti učinkovita.

Ipak, zakonodavna inicijativa i dalje ostaje u rukama nacionalnih zakonodavaca. Hrvatsko kazneno zakonodavstvo od stupanja na snagu novog KZ-a 1997. godine kontinuirano u svoj pravni sustav uvodi nova kaznena djela vezana uz računala i računalne mreže. Posljednja izmjena i dopuna KZ-a, rađena velikim dijelom sukladno Konvenciji o kibernetičkom kriminalu i Dodatnom protokolu Konvencije, je još jedan kvalitetan korak u tom smjeru.

Međutim, zakon je puno lakše i jednostavnije donijeti nego ga ozbiljiti. Računalna kaznena djela su počesto teška za dokazivanje: zbog svoje "virtualnosti", specifičnosti tehnoloških sustava, kratkog roka u kojem je dokazivanje moguće (mnogi računalni zapisi se s vremenom brišu), međunarodne komponente i sl.. Čak i njihovo razumijevanje traži odgovarajuća stručna znanja - bez odgovarajućeg poznavanja tehnologije je teško uopće shvatiti bit nekih od opisanih računalnih kaznenih djela. Tu naravno može pomoći vještak, ali će biti potrebna i odgovarajuća stručnost svih: policije, Državnog odvjetništva i sudstva.

Ostaje nam nadati se da nova kaznena djela vezana uz računala i računalne mreže neće ostati samo dokaz suvremenosti hrvatskog kaznenog zakonodavstva, već da će u slučaju pojave ponašanja koja su njima kriminalizirana - doći do učinkovite primjene KZ-a u praksi.

SUMMARY

Computer revolution has brought up new forms of sociallv unaeceptable behaviour that required criminalization in certain way. Criminal Law of the Republic of Croatia has brought ehanges and additions on October 1, 2004 implemented into Croatian legislative regulations of the Convention on Cvbernetic Criminal and Additional Protocol of the Convention. By such, the Republic of Croatia has criminalized much sociallv unaeceptable behaviour in regard to computers and computer networks, making descriptions of some existing criminal acts concerning computers and computer networks completed.

Article deals in details with cyber-criminal acts ineluded into Croatian Criminal Law based on Convention on Cvbernetic Criminal and Additional Protocol as well as define their characteristics.