UDK 343.451
004.7
343.7
Primljeno 15. listopada 2003.
Pregledni znanstveni rad

Mr. sc. Šime Pavlović*

KOMPJUTORSKA KAZNENA DJELA U KAZNENOM ZAKONIKU

- osnove hrvatskog informacijskog kaznenog prava -

"Don't play games with criminals.
It will end in tears.
80% of people convicted of computer games piracy are involved in drugs, prostitution, tehfft or ather crime."
Poster ELSPA (European Leisure Software Publishers Association Crime Unit)**

Autor se u radu bavi kaznenopravnim aspektom kompjutorskih kaznenih djela, ne zanemarujući pri tome njihovu kriminološku stranu. Sadržaj rada sastoji se od nekoliko dijelova: kratkog uvoda, u kojem se iznose pitanja i problemi vezani za kompjutorski kriminalitet, kao što su: specifičnost toga kriminaliteta i njegovo definiranje te kaznenopravna analiza, u kojoj je autor nastojao dati pregled međunarodnih dokumenata i rješenja u hrvatskom KZ s usporednim prikazom kaznenih djela u nekim drugim zemljama (Austrija, Njemačka, SAD, Velika Britanija i dr.).

Tri kompjutorska kaznena djela iz KZ (čl. 223., 223.a i 224.a) obrađena su tako da čitatelj može usporediti te delikte sa sadržajem Konvencije o kibernetičkom kriminalu i zakonima drugih zemalja. U radu je dan, koliko je to bilo moguće, teoretski prikaz toga novog i složenog kaznenopravnog područja, uz navođenje odgovarajuće domaće i strane literature. Rad na kraju završava kratkim zaključkom u kojem autor iznosi svoje viđenje kompjutorskih kaznenih djela i kompjutorskog kriminaliteta.

---

* Mr. sc. Šime Pavlović, odvjetnik iz Zadra

** *John Muncie and Eugene McLaughlin, The Problem of Crime*, London-Thousand Oaks--New Delhi, 2001., str. 266.

Nekoliko važnijih kratica i napomena

AIDP, *Association Internationale de Droit Pénal* (*Međunarodno udruženje za kazneno pravo*), utemeljeno u Parizu 24. ožujka 1924.[1]

HLJKPP, *Hrvatski ljetopis za kazneno pravo i praksu (Croatian Annual of Criminal Law and Practice)*, nakladnik je Hrvatsko udruženje za kaznene znanosti i praksu (Croatian Association of Criminal Sciences and Practice), Zagreb

Konvencija, *Konvencija o kibernetičkom kriminalu (Convention on Cybercrime),* potpisana u Budimpešti 23. studenoga 2001. Njezino značenje je, među inim, i u tome što prelazi granice Vijeća Europe, jer su je osim članica Vijeća prihvatili SAD, Kanada, Japan i Južna Afrika.

KZ, *Kazneni zakonik* (Narodne novine, 110./97., 27./98., 129./00., 51./01. i 111./03.)

NN, *Narodne novine,* službeni list Republike Hrvatske, Zagreb

NN-MU, *Narodne novine - međunarodni ugovori*

URH, *Ustav Republike Hrvatske* (Narodne novine, 124/00.-pročišćeni tekst).

Vijeće Europe, *Council of Europe/Conseil de l'Europe*. Vijeće Europe međuvladina je međunarodna organizacija koja u zemljama članicama promiče demokraciju, poštovanje ljudskih prava i pravnu državu, a njegovo sjedište je u Strasbourgu.[2]

VSRH, *Vrhovni sud Republike Hrvatske*[3]

I. KRIMONOLOŠKI DISKURS

Je li moguće i u kojoj mjeri, s obzirom na postojanje njihovih specifičnih obilježja, različitih od drugih kaznenih djela, kompjutorske (računalne, kibernetičke) delikte povezati u jedinstvenu cjelinu; u čemu su sastoji njihova posebnost i možemo li zaključiti da postoji *kompjutorski (*računalni) *kriminalitet kao skup individualnih pojava*[4] ili *naprosto kao društvena činjenica* odnosno *dio ukupnosti svih delikata koji se u određenom razdoblju dogode na nekom*

[1] Vidi u: *Ž. Horvatić, Djelovanje međunarodnih organizacija u suzbijanju kriminala,* Pravni fakultet u Zagrebu - Poslijediplomski studij iz kaznenopravnih znanosti, Zagreb, 2002., str. 61-97.

[2] *G. Dojčinović*, *Mali leksikon europskih integracija*, Ministarstvo za europske integracije Republike Hrvatske, Zagreb, 2001., str. 56/57.

[3] Vidi: *Zakon o sudovima* (Narodne novine, 3./94., 100./96., 13./97., 129./00. i 101./03.).

[4] *Z. Šeparović, Kriminologija i socijalna patologija,* Pravni fakultet Zagreb i dr., 1987., str. 17.

području [5]. Kriminalitet ovdje ne promatramo u njegovu totalitetu, kao jedinstvenu pojavu u njezinu opsegu, kretanju i zakonomjernostima, već kompjutorski kriminalitet razmatramo kao dio te sveukupnosti, njegov specifični segment, s posebnostima i značajkama različitim od ostalih oblika kriminaliteta. Važnost kriminološkog pristupa kompjutorskim kaznenim djelima je nepobitna, jer ta djela u pretežitom dijelu nisu vezana za određenu zemlju, niti omeđena državnim granicama, što je donedavna bilo svojstveno kaznenom pravu. Kako se predmet rada ne sastoji u proučavanju kriminološkog aspekta kompjutorske delinkvencije, nego u kaznenopravnoj analizi triju kompjutorskih kaznenih djela iz Kaznenog zakonika, za potrebe rada dane su samo temeljne kriminološke naznake toga kriminalnog ponašanja.

O raširenosti, težini i opasnosti kompjutorskog kriminaliteta u dovoljnoj mjeri kazuje podatak da je u SR Njemačkoj 1992. godine registrirano 12.435 slučajeva toga pojavnog oblika kriminaliteta, od čega kompjutorsku prijevaru čini 2.485 slučajeva.[6]

Prema jednom izvoru iz 1999. godine u Velikoj Britaniji je zbog *softverskog piratstva* kompjutorsko tržište godišnje gubilo 7 milijardi funti.[7]

U suvremenom svijetu danas zbog *tzv. intelektualnog piratstva* na međunarodnom tržištu nastaje šteta od oko 300 milijardi američkih dolara. Intelektualnom piratstvu svojstvena je međunarodna organiziranost, a najugroženiji su razni kompjutorski programi.[8]

Postoje *pokušaji definiranja kompjutorskog kriminaliteta*. Prema definiciji jedne ekspertne grupe *OECD*-a iz 1983. godine, *kompjutorski kriminalitet predstavlja sva protupravna, nemoralna i nedopuštena ponašanja u vezi s automatskom obradom podataka i/ili njihovim prijenosom (any illegal, unethical or unathorized behaviour involving automatic data processing and/or transmission of data)*[9]**.** Drugi *kompjutorski kriminalitet određuju kao skup različitih oblika delinkventnog ponašanja kod kojeg kompjutor predstavlja sredstvo ili cilj kažnjiva djela (pri čemu bi tu spadala i ponašanja koja još nisu inkriminirana, ali koja bi, u slučaju da su se koristila nekim drugim "instrumentom", predstavljala kazneno djelo),* a treći u nj uključuju *sve umišljajne kažnjive napade na tuđu imovinu, počinjene u vezi s elektroničkom obradom podataka*[10]**.**

[5] *M. Singer, Kriminologija,* NZ "Globus", Zagreb, 1994., str. 23/24.

[6] *Osiguranje, časopis za teoriju i praksu osiguranja,* Zagreb, 1-2/94, str. 47.

[7] *The Independent, 25 October 1999*., prema: *J. Muncie-E. McLaughlin, The problem of Crime,* London-Thousand Oaks-New Delhi, 2001., str. 266.

[8] *Christiana Busch, Computer-based Crimes Intellectual Property,* Pravni fakultet Barcelona, u: *D. Derenčinović, Prikaz kolokvija AIDP-a o kibernetičkom kriminalu,* HLJKPP, Zagreb, 1./03., str. 226.

[9] *D. Krapac, Kompjuterski kriminalitet,* Pravni fakultet Zagreb, 1992., str. 13.

[10] *Ibidem*.

Taj pojam *obično obuhvaća zlouporabu kompjutora, kompjutorske prijevare, delikte počinjene uz pomoć kompjutora*[11]. Postoji *restriktivna definicija* koja kompjutorski kriminalitet svodi *samo na ona djela koja se uopće ne bi mogla počiniti bez posebnog stručnog znanja ili samo na ona djela koja se uopće ne bi mogla počiniti bez korištenja kompjutora*, dok su opet neke preopćenite, kao što je primjerice već spomenuta definicija ekspertne grupe OECD-a iz 1983. godine[12].

U analizi nedopuštenih ponašanja dolazi se do određene razdiobe, grupirane u nekoliko smislenih cjelina. U prvu ulazi kompjutorska prijevara. Drugu čini neovlašteno pribavljanje podataka. Treća obuhvaća neovlaštenu uporabu kompjutora u namjeri pribavljanja materijalne koristi. Četvrta cjelina obuhvaća neovlašteno prepravljanje ili uništenje podataka sadržanih u kompjutoru kao i onemogućivanje ili otežavanje pristupa tim podacima ovlaštenim korisnicima.[13]

U pravu su oni koji ističu da je o kompjutorskom kriminalitetu puno toga napisano, ali da nije postignut značajniji pomak glede suglasnosti njegove definicije. On zahvaća različita područja: od korištenja dječje pornografije, softverskog piratstva, krađe telefonskih i elektroničkih usluga, terorizma, trgovine drogom do drugih oblika kriminalnog ponašanja.[14]

Međunarodni organizirani kriminal adaptira se, prihvaća novu tehnologiju, koristi se kompjutorom i *Internetom*; nastaju nove kriminalne kategorije: pojavljuju se nove generacije kriminalaca. Elektroničke komunikacije koriste se za širenje i korištenje pornografije, stvara se nov oblik piratstva (*Software Piracy),* moderni pirati plagiraju kompjutorske programe, nedopušteno prisvajaju tuđa autorska prava *(Copyrights*) i na njima ostvaruju ogromnu zaradu; u kompjutorske programe i sustave ubacuju se virusi; vrše se prijevare; dekodiraju se tajne i zaštićene elektroničke poruke; neovlašteno se pristupa u elektroničke sustave (*Computer Hacking);* organiziraju se zabranjene lančane igre i kockanje (*Gambling)*. Tako bi pojednostavnjeno izgledala slika današnje kriminalne elektroničko-kompjutorske scene.[15]

Kompjutorski kriminalitet obuhvaća "krađu vremena", prijevaru potrošača naplaćivanjem preko cijene koštanja, utaju poreza, lažni bankrot, izbjegavanje poreza na dodanu vrijednost, prijevaru u zdravstvenom osiguranju, prodajne prijevare, ponašanja u kojima je kompjutor uporabljen kao sredstvo počinjenja

[11] *Singer,* bilj. 5., str. 589.

[12] O različitom definiranju kompjutorskog kriminaliteta v. u: *D. Dragičević, Kompjuterski kriminalitet i informacijski sustavi*, Informator, Zagreb, 1999., str. 110-113.

[13] Više v.: *Martin Wasik, Crime and the Computer,* Criminal Law Review, Sweet-Maxwell, London, April 1989., 257-270.

[14] *Mark D. Rasch, Criminal Law and The Internet,* published by the Computer Law Association, 1996., Toronto; vidi na Internet adresi: *http://www.sgrm.com/art14.htm*

[15] Usp. *J. Muncie-E. McLaughlin,* bilj. 7, str. 265/266.

tih delikata te specifična kaznena djela kao što su primjerice *hacking*, krađa konkurentske elektroničke pošte kao i velik broj prodajnih prijevara počinjenih putem Interneta.[16]

Polazeći od *zaštitnog objekta* (kompjutorski sustav, kompjutorski podaci i programi), *D. Dragičević* kompjutorski kriminalitet definira kao *ukupnost kaznenih djela, počinjenih na određenom području kroz određeno vrijeme, kojima se neovlašteno utječe na korištenje, cjelovitost i dostupnost tehničke, programske ili podatkovne osnovice kompjutorskog sustava ili tajnost digitalnih podataka*[17].

Na određeni način taj, u suvremenom svijetu, dobu silnog tehnološkog napretka, sve pojavniji oblik kriminaliteta može se definirati sažimanjem Preambule *Konvencije o kibernetičkom kriminalu* država članica Vijeća Europe, potpisane u Budimpešti 23. studenoga 2001. (NN-MU, 9./02.), u kojoj se ističe da je *ratio* donošenja Konvencije odvraćanje od "*postupaka usmjerenih protiv tajnosti, cjelovitosti i dostupnosti računalnih sustava, mreža i računalnih podataka, kao i za odvraćanje od njihovih zlouporaba, jer utvrđuje - na način opisan u ovoj Konvenciji - kriminalizaciju takvog ponašanja"*.

Kompjutorski kriminalitet mogli bismo, bez nekakve veće pretenzije, definirati kao *smisleni zbir kaznenih djela povezanih s kompjutorskim sustavom i kompjutorskim podacima ili u vezi sa sadržajem kompjutorskih informacija, počinjenih na određenom području kroz određeno vrijeme*.

Kompjutorski kriminalitet moguće je odrediti *u užem* i *širem smislu*. U *užem smislu* kriminalitet obuhvaća kaznena djela iz čl. 2. do 8. Konvencije o kibernetičkom kriminalu, delikte izvan tradicionalnog, postojećeg kataloga kaznenih djela, što bi značilo da su kaznena djela vezana uz dječju pornografiju (čl. 9. Konvencije) dio pornografskog kriminaliteta, a kaznena djela povrede autorskih i srodnih prava (čl. 10. Konvencije) sastavni dio imovinskog kriminaliteta, iz velike skupine prava intelektualnog vlasništva, a u njegovu *širem poimanju* i ta bi kaznena djela ulazila u kaznena djela kompjutorskog kriminaliteta. Radnje počinjenja djela iz čl. 9. Konvencije postoje u inkriminacijama glave XIV. KZ (kaznena djela protiv spolne slobode i spolnog ćudoređa) - iskorištavanja djece ili maloljetnika za pornografiju (čl. 196.) i upoznavanja djece s pornografijom (čl. 197.), a kaznena djela povrede autorskih i srodnih prava iz čl. 10. Konvencije u Glavi XVII. KZ - (kaznena djela protiv imovine) - povreda prava autora ili umjetnika izvođača (čl. 229.), nedozvoljena uporaba autorskog djela ili izvedbe umjetnika izvođača (čl. 230.) i povreda prava proizvoditelja zvučne ili slikovne snimke i prava u svezi s radiodifuzijskim emisijama (čl. 231.) te djela iz čl. 124a. i 124b. Zakona o autorskom pravu.

[16] *Ibidem,* str. 245.

[17] *Dragičević, bilj. 12*, str. 113.

Egzaktno određenje pojma kompjutorskog kriminaliteta ima svoje teorijsko i pragmatično značenje. Kaznena djela iz sastava kompjutorskog kriminaliteta predstavljaju koherentnu cjelinu; točnu određenost kaznenopravne zaštite, dobara i vrijednosti određenih zakonskim opisom kaznenog djela; grupirana su prema identičnosti, srodnosti, bliskosti objekta zaštite; sva ona imaju svoje unutarnje jedinstvo i povezanost. Upravo kroz jasnu definiciju kompjutorskog kriminaliteta moguća su teorijska razmatranja o tome što je kazneno djelo, vodeći pri tome računa o sadržaju čl. 1. KZ (*temelj i ograničenje kaznenopravne prisile)*. Uvažavajući brojne komponente u izgradnji kaznenih djela kompjutorskog kriminaliteta, nezaobilazno se nameće potreba poštovanja temeljnih ljudskih prava i sloboda (primjerice - dostupnosti i protoka informacija; zaštite privatnosti), ali i prihvaćanje postignuća u suvremenoj tehnologiji, informatici i elektronici, s pojavom novih rizika i opasnosti čovjeka; uvažavajući potrebu njegove sigurnosti i sigurnosti društva u cjelini; kao i neizbježnu pojavu zlouporabe u korištenju tim novim tehnološkim i informatičkim postignućima. Kompjutorskom kriminalitetu svojstveno je uvažavanje zahtjeva *međunarodnog kaznenog prava* (stoga ne začuđuje aktivnost međunarodne zajednice; usvajanje globalnih i regionalnih pravnih dokumenata, primjerice *Konvencije o kibernetičkom kriminalu* kao najznačajnijeg kaznenopravnog dokumenta). Upravo područje kompjutorskog kriminaliteta najjasnije nameće potrebu izgradnje međunarodnog kaznenog prava. Inkriminiranjem pojedinih naročito opasnih ponašanja afirmiraju se temeljna načela međunarodnog kaznenog prava: *solidarnost i suradnja među državama svijeta; povjerenje među državama; eliminiranje relacija momenta; učinkovita borba s kriminalitetom; pravičnost; zaštita prava i sloboda čovjeka; humanitarni pristup*[18].

Određenjem *kataloga kaznenih djela kompjutorskog kriminaliteta* postiže se približavanje dvaju različitih zakonodavnih pristupa - jednoga u kojem se kompjutorskim kaznenim djelom podrazumijeva svaki neovlašteni kompjutorski pristup i drugoga u kojem se inkriminiraju samo nedopuštena ponašanja ostvarena unatoč poduzetim zaštitnim mjerama. Mogućnost lakog uništenja ili mijenjanja kompjutorskih podataka nalaže hitnu zaštitu pohranjenih podataka (čl. 16. Konvencije o kibernetičkom kriminalu). U skladu s odredbom st. 2. čl. 16. Konvencije država stranka ovlaštena je izdati nalog nekoj osobi da zaštiti određene pohranjene kompjutorske podatke koje ta osoba posjeduje ili pohranjuje. Stranka država svojim će zakonskim i drugim mjerama obvezati tu osobu da kompjutorske podatke zaštiti i sačuva njihovu cjelovitost sve dok je to nužno, ali najviše 90 dana, kako bi nadležnim tijelima bilo omogućeno da zahtijevaju njihovo otkrivanje.

Uvod možemo zaključiti s neprijepornom konstatacijom da je rasprava o kompjutorskom kaznenom pravu usmjerena afirmaciji *opće teorije o zaštiti*

[18] O tim načelima v. u: *B. Zlatarić, Međunarodno krivično pravo* (priredio Z. Šeparović), Informator-Zagreb, 1979., str. 33-37.

informacija, u kojoj se aktivnost odvija smjerom od tjelesnih prema nematerijalnim predmetima. Ta informacijska matica leluja informacijski brod u čijoj se utrobi čuva pravo na informatičko samoodređenje i pohranjeni kompjutorski podaci, ali istodobno upozorava na postojanje opasnosti koje stvaraju informacijski virovi, navlastito kada se kroz brojne mreže plasiraju različiti sadržaji pod *paradigmom - "jačajmo načelo slobodnog protoka informacija i njihovu neograničenu pokretljivost"*. Ta opasnost posebno se izražava u novije doba, kada se dosadašnja aktivnost, usredotočena na fenomenologiju kompjutorskih delikata - primjerice *"hacking", "viruse*" i sl., usmjerava na sustav mreža, svojevrsnu arenu na kojoj se odvijaju različite *igre* iz kojih nastaju opasnosti. Brojem i rastom sustava mreža raste kriminalni potencijal - primjerice na *Internet* je danas priključeno oko 400 milijuna korisnika. Preko tih mrežnih prostora plasiraju se različiti kriminalni sadržaji: "*...širi se duh mržnje prema strancima, populariziraju neonacističke igre, poziva se na počinjenje kaznenih djela, nude se ilegalne kopije i roba koja potječe iz kriminalne djelatnosti, brojevi (kreditnih) kartica ilegalno se otkrivaju ili koriste i objavljuju tekstovi/ /slike s (dječjom) pornografijom"*.[19] I stoga, u gotovo beskrajnom informacijskom prostoru, stvorene tehnološke potencijale i opasnosti nužno je pravno urediti tako da se uravnoteže pravo na protok informacija i rizici koje u sebi nosi to pravo. Zemlja, globalno selo, u tim informacijskim prostranstvima i neslućenim mogućnostima traži konsenzus u donošenju međunarodnih propisa i o potrebi njihova sveopćeg provođenja.

Informacijska revolucija odvija se u prostoru dvaju suprotstavljenih procesa: *globalizacije*, snažnog trenda današnjice, s Internetom, kao pogodnim medijem u njenu širenju i jačanju, s jedne strane, i nastojanja da se u *otporu tome trendu sačuva identitet* pojedinca i zajednice, s opasnošću njegova prijelaza u radikalni individualizam, s druge strane. Internetizacija se sučeljava sa stvaranjem novih mreža širom svijeta. Postajemo dio umreženog društva, sa svim njegovim opasnostima i nesigurnim ishodom informacijsko-tehnološke budućnosti. To je naš *fatum*, naša sudbina!

II. MEĐUNARODNA AKTIVNOST I NAJVAŽNIJI DOKUMENTI U SPRJEČAVANJU KOMPJUTORSKIH KAZNENIH DJELA

Na međunarodnom se planu poduzimaju odgovarajuće aktivnosti usmjerene kaznenopravnoj zaštiti od kompjutorskih kaznenih djela.

Vijeće Europe (*Council of Europe)* usvojilo je 28. siječnja 1981. u Strasbourgu *Konvenciju o zaštiti pojedinaca glede automatske obrade osobnih podataka (Convention for the Protection of Individuals with regard to Auto-*

[19] *Gabriele Schmölzer, Internet i kazneno pravo,* HLJKPP, 2./97., str. 893.

matic Processing of Personal Data), a poslije je doneseno i nekoliko rezolucija. U Konvenciji se posebna pozornost posvećuje osiguranju kontrole pristupa osobnim podacima; razmjeni tih podataka između država; otklanjanju mogućih pogrešaka u informacijskim sustavima i sprječavanju piratstva.[20] U čl. 2. t. *a*. Konvencije izrazom *osobni podatak (personal data)* označava se svaka informacija koja se odnosi na ustanovljenu osobu ili podatak kojim se ona može identificirati.[21]

Organizacija za gospodarsku suradnju i razvoj (Organisation for Economic Cooperation and Development – OECD) 1983. godine utemeljila je odbor stručnjaka, koji je 1985. zemljama članicama preporučio koje bi dolusne (namjerne) radnje trebalo kriminalizirati. Potom je i *Vijeće Europe* putem posebne ekspertne komisije (*Select Commitee of Experts od Computer-Related Crime of the Council of Europe)* zajedno s *Europskom komisijom za probleme kriminala (Commitee on Crime Problems)* 13. studenoga 1989. donijelo *Preporuku br. R (89) 9*. U njoj se državama članicama preporučuje da u svojim nacionalnim zakonodavstvima inkriminiraju pojedine nedopuštene aktivnosti sadržane u *minimalnoj listi* inkriminacija (kompjutorsku prijevaru, krivotvorenje, oštećenje i uništenje kompjutorskih podataka i programa, kompjutorsku sabotažu, neovlašteno kopiranje programa ili tzv. topografiju elektroničkog mikoroprocesora) i u *opcijskoj listi,* sa sljedećim djelima: neovlaštenim mijenjanjem podataka i programa, kompjutorskom špijunažom, neovlaštenim korištenjem kompjutora (tzv. krađa vremena) i neovlaštenim korištenjem zaštićenog kompjutorskog programa.

*Ujedinjeni narodi (*dalje: UN) također su se pozabavili tim oblikom kriminaliteta. Na VIII. kongresu UN o sprječavanju zločina i postupanja s delinkventima, održanom 1990. u Havani, donesena je rezolucija kojom se od svih država članica UN traži da pojačaju napore prema suzbijanju manipulacija s kompjutorima, među koje napore ulazi i modernizacija kaznenog prava i postupka.[22]

---

[20] Internet adresa: *http:// www.coe.fr/dataprotection/edocs.htm*

[21] Usp. sadržaj Konvencije sa *Zakonom o zaštiti osobnih podataka* (NN, 103./03.). Taj je zakon donesen u skladu s Konvencijom. Valja istaknuti da se u Konvenciji, poslije donesenim rezolucijama i u našem zakonu uređuje zaštita osobnih podataka fizičkih osoba te nadzor nad prikupljanjem, obradom i korištenjem tih podataka.

[22] U *Rezoluciji 45/121* zemljama članicama preporučuje se da u suzbijanju kompjutorskog kriminaliteta uzmu u obzir sljedeće mjere: 1. Osuvremenjivanje nacionalnih kaznenih zakona, uključujući mjere kojima će se: - osigurati da se postojeća kaznena djela i zakoni glede istražnih radnji i dopuštenosti dokaza u sudskom postupku odgovarajuće primjenjuju i, ako se za tim pokaže potreba, učine potrebne izmjene; - u nedostatku zakona koji se mogu adekvatno primijeniti, kreiraju kaznena djela, istražni i dokazni postupci, kada je to nužno, kako bi se moglo učinkovito suprotstaviti novim i sofisticiranim oblicima kriminala; - osigurati oduzimanje i vraćanje nezakonito stečene imovine koja je nastala počinjenjem kompjutorskih kaznenih djela; 2. Unapređenje kompjutorske sigurnosti i preventivnih mjera, pritom vodeći računa i o zaštiti privatnosti, uvažavanju ljudskih prava i temeljnih sloboda te svakog upravljačkog mehanizma

Nakon rada posebne komisije *(Committe of Experts on Crime in Cyber PC--CY*), utemeljene 1997. od Vijeća Europe, sastavljene od stručnjaka s različitih područja, države članice Vijeća Europe i ostale države potpisnice u Budimpešti su 23. studenoga 2001. godine potpisale *Konvenciju o kibernetičkom kriminalu (Convention on Cybercrime)*. Upoznajmo se s uvodnim dijelom (preambulom Konvencije koji objašnjava njezine opće postavke). Konvencija je stvorena u okolnostima "*dubokih promjena nastalih digitalizacijom, konvergencijom i neprekidnom globalizacijom kompjutorskih mreža"*. Nastala je u vremenu zabrinutosti država članica Vijeća Europe i ostalih država potpisnica Konvencije "*zbog mogućnosti da kompjutorske mreže i elektroničke informacije budu iskorištene za počinjenje kaznenih djela",* ali i uz istodobno postojanje potrebe "*za zaštitom legitimnih interesa prilikom korištenja i razvitka informatičkih tehnologija"*. Značenje Konvencije posebno se ogleda u naznaci prirode kibernetičkog kriminala zbog kojeg se od država članica Vijeća Europe i ostalih država potpisnica "*zahtijeva povećana, brza i uhodana međunarodna suradnja u kaznenopravnim predmetima"*. Konvencija je "*nužna radi odvraćanja od postupaka usmjerenih protiv tajnosti, cjelovitosti i dostupnosti kompjutorskih sustava, mreža i kompjutorskih podataka, kao i za odvraćanje od njihovih zlouporaba"*. U preambuli se posebno značenje posvećuje ravnovjesju "*između interesa provedbe zakona i poštovanja temeljnih ljudskih prava utjelovljenih u Konvenciji Vijeća Europe o zaštiti prava i temeljnih sloboda čovjeka iz 1950. godine"* i drugih relevantnih međunarodnih sporazuma. Pojedini dijelovi Konvencije u ovome radu objasnit će se na mjestima gdje za to postoji potreba.[23]

Dragocjenu i neizostavnu pomoć međunarodnoj zajednici u borbi s kompjutorskim kriminalitetetom pruža *Međunarodno udruženje za kazneno pravo (Association International de Droit Pénal,* skr. AIDP*)*. AIDP izdaje: fr. *Revue Internationale de Droit Pénal,* engl. *International Review of Penal Law* (nakladnik Érès, Toulouse, France). U *Ljetopisu* se, među inim, objavljuju

koji se odnosi na korištenje kompjutora; 3. Primjenu mjera na temelju kojih će se upoznati javnost, sudska tijela i tijela kaznenog progona o problemima i važnosti prevencije kompjutorskog kriminaliteta; 4. Primjena odgovarajućih edukativnih mjera za suce, službenike i službe odgovorne za prevenciju, pokretanje kaznenog postupka, optuženje i suđenje za gospodarska i kompjutorska kaznena djela; 5. U suradnji sa zainteresiranim organizacijama, razraditi etička pravila korištenja kompjutora i programe učenja o tim pravilima kao dio nastavnog plana i vježbi u informatici; 6. Brigu o interesima žrtava kompjutorskog kriminaliteta u skladu s temeljnim načelima pravednosti za žrtve kriminala i zlouporabe moći *(Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power*) UN, uključujući oduzimanje nezakonito stečene imovinske koristi, uz poticanje žrtava na prijavljivanje takvih kaznenih djela nadležnim tijelima (o toj rezoluciji v. u: *Krapac, bilj. 9, str. 17/18, i Dragičević,* bilj. 12, *str. 198/199)*.

[23] Najvažniji *linkovi* Vijeća Europe, Europske zajednice i drugih relevantnih čimbenika *(Other Fora*) s njihovim *web-adresama* o aktivnosti u suzbijanju kompjutorskih kaznenih djela mogu se pronaći putem Internet-adrese: *http://www.usdoj.gov/criminal/cybercrime/intl.html*

izlaganja autora kolokvija i kongresa, renomiranih stručnjaka kaznenog prava i kriminologije.

Na pripremnim kolokvijima i međunarodnim kongresima AIDP raspravlja i o kompjutorskom kriminalitetu. Na *XV. međunarodnom kongresu*, održanom u Rio de Janeiru od 4. do 10. rujna 1994., u Drugoj kongresnoj sekciji obrađena je tema: *Kompjutorski delikti i druga kaznena djela protiv informatičke tehnologije*. Nakon rasprave donesena rezolucija podijeljena je na nekoliko dijelova. U prvom se ističe da je kazneno pravo *ultima ratio societatis* i da zato prije inkriminiranja određenih ponašanja države trebaju posegnuti za primjenom različitih zaštitnih mjera informacijske tehnologije, poraditi na svestranom obrazovanju i podizanju opće svijesti o njihovoj nužnosti kod korisnika i kontrolora kompjutorskih sustava, na razvijanju *"etike"* kompjutora u svim dijelovima društva i sl.; drugi dio obrađuje zlouporabe informacijske tehnologije, postojanje pravne praznine tradicionalnog kaznenog prava glede novih vrsta društvenih i privatnih interesa koji se trebaju pravno zaštititi, s prikazom njihova sadržaja; u trećem dijelu rezolucija se bavi zaštitom privatnosti koja mora biti uravnotežena s legitimnim interesima za slobodan protok informacija, uključujući i pravo građana na pristup informacijama prikupljenima od drugih subjekata; četvrta sekcija bila je posvećena kaznenom procesnom pravu.[24] U Ateni je od 10. do 13. travnja 2003. održan pripremni *Međunarodni kolokvij o kibernetičkom kriminalu* kao prethodnica XVII. međunarodnom kongresu AIDP-a koji bi se 2004. godine trebao održati u Kini. Na Kolokviju se, među inim, vodila rasprava o primjeni načela prostornog važenja kaznenog zakonodavstva u progonu kompjutorskih kaznenih djela; o problemima definiranja pojma *kompjutorski kriminal*; o katalogu kaznenih djela; o potrebi da nacionalna zakonodavstva propišu mjere hitne zaštite kompjutorskih podataka kako bi se poslije u kaznenom postupku mogli koristiti kao dokaz; o problemima dvostruke kažnjivosti; o praktičnim aspektima seksualne zlouporabe djece putem Interneta; o zaštiti intelektualnog vlasništva, navlastito o inkriminiranju tzv. intelektualnog piratstva i pitanjima korištenja nezakonitih kopija kompjutorskih programa ili čitavih programskih paketa, pritom je dana fenomenologija kršenja autorskih prava; istaknuti su problemi utvrđivanja mjesta počinjenja kaznenog djela ako je ono počinjeno putem Interneta i sl.[25]

U obradi kompjutorskih kaznenih djela ne može se zanemariti referat *Matthewa R. Zakarasa,* glavnog referenta II. sekcije XVII. međunarodnog kongresa AIDP (Kina, 2004.) o temi: *Međunarodni kompjutorski kriminal*.[26] U tome radu

[24] Iscrpnije v. u: *D. Krapac, XV. međunarodni kongres za kazneno pravo, Rio de Janeiro, rujan 1994.,* HLJKPP, 1./94., str. 425-439, posebno 429-431.

[25] Iscrpnije v. u: *Derenčinović, bilj. 8, str. 223-227.*

[26] *Section II, International Computer Crimes, Matthew R. ZAKARAS, General Report,* International Review of Penal Law, Érès, Toulouse, 3.-4./01., str. 813-836.

naglašava se razorno financijsko djelovanje kompjutorskih kaznenih djela. Primjerice kompjutorski virus *Volim te*, djelujući samo od svibnja 2000. godine, širom svijeta počinio je štetu od 10 milijardi USA $.[27] U radu je dan sadržaj buduće rezolucije; problematizira se nekoliko pitanja, kao što su utvrđivanje mjesta počinjenja kaznenog djela i dječja pornografija. Glede načela utvrđivanja represivne vlasti države i lokalizacije kaznenog djela u prostoru, počinjenog primjerice putem Interneta, u predloženoj se rezoluciji ističe kako neke države, uključujući Francusku i Belgiju, primjenjuju *teritorijalno načelo,* a i u rezoluciji se podržava primjena toga načela, ali uz supsidijarnu primjenu *univerzalnog načela* kod počinjenja pojedinih kaznenih djela, kao što su delikti poput dječje pornografije.[28]

Teritorijalno načelo sastoji se u primjeni kaznenog zakonodavstva države na svakoga tko na njenom području počini kazneno djelo predviđeno njezinim zakonom, neovisno o državljanstvu/nedržavljanstvu (apatrid, apolit) počinitelja. Čini se da bi, zbog činjenice što se kompjutorskim kaznenim djelima napadaju važni interesi međunarodne zajednice, trebalo primjenjivati *univerzalno načelo*.[29]

Kada je riječ o dječjoj pornografiji, u prijedlogu rezolucije posebno se ističe da *Cyberspace,* kao općesvjetska arena, omogućuje pedofilima gledanje, snimanje i prenošenje različitih slika, videotraka i crteža djece mlađe od 18 godina. *Chat rooms* (prostori u kompjutorskom programu za međusobno vođenje razgovora preko Interneta između osoba, nap. Š. P.) postali su pogodno sredstvo gledanja i vođenja razgovora s drugima o toj temi.[30]

Odredbe o teritorijalnom važenju kaznenih zakona sadržane su u *čl. 13.-17. hrvatskog KZ. Teritorijalno načelo* polazno je i osnovno, a kada su djela počinjena u inozemstvu, to načelo nadopunjuju: načelo zastave broda i načelo registracije zrakoplova te realno, personalno i univerzalno načelo.[31]

---

[27] *Ibidem*, str. 815.

[28] Usp. čl. 22. Konvencije o kibernetičkom kriminalu, koji glasi:

"1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se uspostavila sudbenost za sva djela utvrđena člancima 2.-11. ove konvencije, kad je djelo počinjeno:

a. na njezinu državnom području, ili

b. na brodu koji vije zastavu te stranke, ili

c. u zrakoplovu registriranom po pravu te stranke, ili

d. od strane njezina državljanina, ako je djelo kažnjivo po kaznenom pravu mjesta gdje je počinjeno ili ako je djelo počinjeno izvan nadležnosti svih država".

[29] Vidi u*: B. Zlatarić, bilj. 18*, str. 136-142; *F. Bačić, Kazneno pravo - Opći dio,* 5. izdanje, Zagreb, 1998., str. 99, te *čl. 14. st. 4. i čl. 16. st. 3. KZ.*

[30] *"Chat rooms have also become a means of access to paedophiles to view and talk to others about such topics"- Zakaras, bilj. 23,* str. 833.

[31] O svakome od tih načela v. u: *Bačić, bilj. 29*, str. 94-100 te u: *Bačić-Pavlović, Komentar Kaznenog zakonika,* Organizator, Zagreb, 2003., u objašnjenju čl. 13.-17. KZ.

Austrijski KZ u *§ 62*. sadržava odredbu prema kojoj se austrijski Kazneni zakon primjenjuje na sva djela počinjena na području Austrije (primjena *teritorijalnog načela)*. Mjesto počinjenja djela u *§ 67. st. 2*. (*Zeit und Ort der Tat)* smatra se mjesto u kojem je počinitelj radio ili bio dužan raditi ili u kojem je u cjelini ili djelomično nastupila posljedica iz zakonskog bića kaznenog djela ili je prema počiniteljevu predviđanju trebala nastupiti unutar austrijskog saveznog područja, uključujući i zračni prostor iznad toga područja kao i prostor ispod površine zemlje u mjeri u kojoj je realno dostupan.[32] S obzirom na to da je dovoljno da je bilo radnja bilo posljedica nastala na austrijskom području, austrijska jurisdikcija široko se primjenjuje, što se odnosi i na kompjutorska kaznena djela. Austrijska sudbena vlast primjenjuje *univerzalno načelo (§ 64. st. 1. t. 6. KZ)* kad je riječ o kaznenim djelima počinjenim u inozemstvu, neovisno o njihovoj kažnjivosti u mjestu počinjenja. Ta bi se obveza odnosila i na kompjutorska kaznena djela.[33]

III. KAZNENOPRAVNI PRISTUP

Tri kaznena djela iz KZ s usporednim prikazom kaznenih djela iz kaznenih zakona nekoliko drugih zemalja

Uvod

Pomnijom analizom kazneno-materijalnih odredba Konvencije (čl. 2.-10.) dolazi se do zaključka da je kaznena djela moguće grupirati u dvije skupine. U prvoj skupini su kaznena djela koja se mogu uvijek primijeniti na kompjutorski sustav i na kompjutorske podatke. Unutar te skupine su dvije podskupine. Podskupina inkriminacija protiv tajnosti, cjelovitosti i dostupnosti kompjutorskih podataka i sustava – nezakonit pristup (čl. 2.), nezakonito presretanje (čl. 3.), ometanje podataka (čl. 4.), ometanje sustava (čl. 5.) i zlouporaba naprava (čl. 6.), te podskupina s dva modificirana klasična kaznena djela - kompjutorsko krivotvorenje (čl.7.) i kompjutorska prijevara (čl. 8.). Drugu skupinu čine kaznena djela sa sadržajem informacija kao bitnom komponentom njihova bića,

[32] Prema hrvatskom KZ (čl. 27. st. 1. KZ) kazneno djelo je počinjeno kako u mjestu gdje je počinitelj radio ili bio dužan raditi tako i u mjestu gdje je u cjelini ili djelomično nastupila posljedica iz zakonskog opisa kaznenog djela, a u slučaju kažnjiva pokušaja i tamo gdje je ta posljedica prema njegovu predviđanju trebala nastupiti. Može se, dakle, zaključiti kako su austrijski i hrvatski KZ pitanje mjesta počinjenja kaznenog djela riješili primjenom *teorije ubikviteta (teorija jedinstva djela)*.

[33] Usp. *E. Foregger - E. E. Fabrizy, Strafgesetzbuch,* 7. izdanje, Wien, Manzsche Verlags- und Universitätsbuchhandlung, 199., str. 222, 225/226 i 235/236, te *Schmölzer, bilj. 19*., str. 903.

s kompjutorskim podacima u svezi s komunikacijama stvorenim pomoću kompjutorskog sustava kao dijela komunikacijskog lanca, koji podaci naznačuju podrijetlo komunikacije, njezino odredište, put, vrijeme, datum, veličinu, trajanje i vrstu te usluge (*podaci u prometu* - čl. 1.d. Konvencije).

U *hrvatskom kaznenom pravu* u prvoj su skupini kazneno djelo povrede tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava (čl. 223. KZ); računalno krivotvorenje (čl. 223.a KZ) i računalna prijevara (čl. 224.a KZ).[34] Druga skupina, kako je već navedeno, obuhvaća kažnjivost sadržaja ili, kako u 3. dijelu Konvencije stoji, *Kaznena djela u svezi sa sadržajem*. Kaznena djela iz te skupine uređena su u odgovarajućim glavama KZ, utemeljenim na sadržajnom jedinstvu zaštićenih dobara. Tu skupinu, u skladu s Konvencijom, čine kaznena djela vezana uz dječju pornografiju (čl. 9. Konvencije) i kaznena djela povrede autorskih i srodnih prava (čl. 10. Konvencije). KZ sadržava dva kaznena djela protiv spolne slobode i spolnog ćudoređa (gl. XIV. KZ): iskorištavanje djece ili maloljetnika za pornografiju (čl. 196.) i upoznavanje djece s pornografijom (čl. 197.) te tri kaznena djela protiv imovine (gl. XVII. KZ): povreda prava autora ili umjetnika izvođača (čl. 229.), nedozvoljena uporaba autorskog djela ili izvedba umjetnika izvođača (čl. 230.) i povreda prava proizvoditelja zvučne ili slikovne snimke i prava u svezi s radiodifuzijskim emisijama (čl. 231.) te dva kaznena djela iz čl. 124a. i 124b. Zakona o autorskom pravu.

[34] U radu se koristi izraz "*kompjutor",* a ne "*računalo*". Mislim da *računalo* nije najsretniji izraz za *kompjutor*. *Računalo* asocira na obradu određene računske operacije, izraz je bliži matematici-računstvu, a ne informacijskom sustavu, premda se s elektroničko-tehničkog stajališta može braniti argumentom da kompjutor predstavlja svaki uređaj ili stroj koji je u stanju prihvatiti podatke u odgovarajućem obliku, izvršiti tražene operacije s tim podacima i prikazati rezultate u obliku prihvatljivom za korisnika (v. V. Tasić-I. Bauer, Rječnik kompjuterskih termina, Beograd, 2001., str. 84). U prijevodu engl. *computer* u hrvatskom jeziku označava *kompjuter (*Europski rječnik, Zagreb, 1995., str. 169) odnosno *kompjuter* ili *elektronsko računalo* (M. Drvodelić, Englesko-hrvatski rječnik, Zagreb, 1981., str. 133.; isto Vićan-Pavić-Smerdel, Engleski za pravnike, Zagreb, 1992., str. 207, te D. Božić, Rječnik englesko-hrvatski/hrvatsko engleski, Split, 200., str. 98) pa se može reći da se u našem jezičnom izričaju uvriježila riječ *kompjuter* ili *kompjutor (*manje adekvatan, jer se ne može izvesti prijevodom izvornog značenja iz engleskog govornog područja u kojem je i nastao). Ispravnost ovoga stajališta može se argumentirati činjenicom da se neki kazneni zakonici, pa i oni izvan anglosaksonskog pravnog područja, koriste izrazom *computer* (austrijski, njemački, švicarski KZ). U slovenskom KZ (v. Lj. Bavcon i dr., Kazenski zakonik Republike Slovenije, Ljubljana, 1994.) u uporabi je izraz *računalo (*kazneno djelo *vdor u računalniški sistem* iz *čl. 242.)*. Poradi korektnosti, tamo gdje postoji zakonsko nazivlje u kojem se koristi izraz *računalo,* a ne *kompjutor*, u ovome radu također će se koristiti taj izraz.

Zaštitni objekt kaznenog djela

Opća izlaganja o kaznenom djelu uče nas da je bitna komponenta bića kaznenog djela *zaštitni objekt,* materijalna odrednica neprava. "*Kazneno djelo je u svojoj biti povreda pravom zaštićenih vrijednosti, povreda dobara pojedinca i zajednice koja su dobila pravnu zaštitu"*.[35] Koje su, dakle, vrijednosti zaštićene inkriminacijama iz kataloga kompjutorskih kaznenih djela? Postoje pokušaji stvaranja opće teorije o kaznenopravnoj zaštiti *informacije*. Različite zaštitne vrijednosti - *pravo na privatnost*, *financijski interesi i intelektualno vlasništvo predstavljaju nedjeljivu cjelinu informacijskog prava i prava o informacijskoj tehnologiji*. *Informacija* je ono što ih povezuje. Pored materije i energije, informacija je entitet *sui generis*. Zadaća informacijskog prava jest utvrditi razliku između kaznenopravne zaštite tjelesnih stvari, svojstvenih navlastito pojedincu, i netjelesnih stvari, atribuiranih javnosti.[36]

Zbog same činjenice da je informacija netjelesna stvar; da su joj imanentni sloboda protočnosti i dostupnosti; da je od prvorazredne važnosti za gospodarstvo i politički sustav; da se nad njom teško može steći ekskluzivno pravo vlasništva jer tangira prava i slobode drugih, dolazimo do toga da se na nju ne mogu primijeniti pravila o tradicionalnoj podjeli vrijednosti zaštićenih kaznenim pravom. Neovisno što su pojedine inkriminacije smještene u različitim glavama KZ, možemo se složiti sa stajalištem o nastanku *informacijskog kaznenog prava*. U jezgri tih delikata postoji nešto zajedničko, nešto što ih povezuje - to je, kako je već rečeno, **informacija**, to je iskazivanje činjenica, to su programi koji su kadri prouzročiti da kompjutorski sustav obavi određenu funkciju. Sve te supstantive reprezentira izraz *kompjutorski podaci (computer data) iz* čl. 1.b. Konvencije. U određivanju zaštitnog objekta nameću se nezaobilazna pitanja - što je sa zaštitom *nositelja informacije,* s njegovim pravom na tajnost i s pravom ekskluzivnog korištenja informacijom; kako zajamčiti integritet, dostupnost i pravilnost informacije; što je s pravima drugih i u kojoj mjeri oni mogu putem informacija biti upoznati s osobnim podacima ostalih osoba - primjerice pretraživati njihove bankovne račune, medicinske podatke i sl. Ambivalentni položaj društva glede zaštite navedenih prava ovisi, donekle, i o tome je li riječ o *masovnim* ili *individualnim komunikacijama*. Čini se da je sadržaj *individualne komunikacije* uvijek zaštićen bez obzira na korišteno sredstvo priopćivanja (medij), pa bio to i Internet. Privatna sfera i sloboda izražavanja odvijaju se u neometanoj individualnoj komunikaciji. To pravo zajamčeno je člankom 8. *Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda*.[37] Konvencija u čl. 10. jamči slobodu mišljenja i slobodu

[35] *Bačić, bilj. 29,* str. 114.

[36] *D. Krapac, bilj. 9*, str. 45-49, i isti autor, *bilj. 24,* str. 429-430.

[37] "*1. Svatko ima pravo na poštovanje svog privatnog i obiteljskog života, doma i dopisivanja.*

2. Javna vlast se neće miješati u ostvarivanje tog prava, osim u skladu sa zakonom i ako je u demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira, ili

primanja i širenja informacija i ideja bez miješanja javne vlasti i bez obzira na granice, uz točno predviđene mogućnosti restrikcija navedenih u odredbi st. 2. čl. 8. Konvencije. Komuniciranje na daljinu ne utječe na jamstva iz čl. 8. i 10. Europske konvencije i zato ih treba štititi od zahvata neovlaštenih osoba. Potpuno je druga situacija kada je riječ o *masovnoj komunikaciji*, kada se misaoni sadržaj ili informacija javno obznanjuje. Dostupnost informacije je neograničena, ali i ovdje važe pravila potrebnog nadzora i zabrana upletanja u skladu s odgovarajućim posebnim propisima. Kod takvog oblika javnog priopćivanja za kazneno je pravo bitan sadržaj informacije, kome je namijenjena, kakve poruke sadrži, je li zlouporabljena tajna, povrijeđeno pravo korisnika konkretnog medija. *Kaznena odgovornost* će postojati ako je poruka, informacija s kriminalnim sadržajem, primjerice obavijesti s pornografskim sadržajem, nuđenje stvari s elementima pranja novca, nuđenje ilegalnih kopija tuđih autorskih djela, sudjelovanje u lančanim igrama na sreću, ucjene, iznude, širenje *ksenofobičnih* ideja.

U proučavanju informacije kao objekta kaznenopravne zaštite nastaje u određenom smislu *bifurkacija*: (1.) ako je informacija javnopravno dobro, koje je u slobodnom demokratskom društvu u načelu bez ograničenja, slobodno protječe, širi se, tada joj se ne može pružiti zaštita koju kazneno pravo pruža materijalnim, tjelesnim stvarima; (2.) na drugom kraku je *sadržaj* objavljene *informacije* kao skupa činjenica ili činjeničnih tvrdnji, podataka i poruka koji se odnose na određeni pojam na temelju kojih se donose određene odluke ili poduzimaju određene radnje, pri čemu je nužno zaštititi ne samo pošiljatelja nego i onoga kome je poruka namijenjena i slobodan protok informacije, ali uz kontrolu i zaštitu njezina sadržaja. U toj dvojnosti ne smije se zanemariti oblik prezentacije informacije i sredstvo kojim se ona prenosi, širi ili prima.

Počinitelj i oblici počinjenja kaznenog djela

Kompjutorska kaznena djela ne uklapaju se u tradicionalno određenje, u kaznenopravnu fizionomiju počinitelja kaznenih djela. Pojavljuju se specifični tipovi počinitelja. *Hacker* je preteča složenijim oblicima počinitelja.

Najjednostavnija podjela počinitelja je na *unutarnje i vanjske,* ovisno djeluju li iz informacijskog sustava u kojem su zaposleni ili su napadači koji djeluju s udaljenih, vanjskih kompjutora. Unutarnji počinitelji najčešće *kradu vrijeme (time-theft),* tj. ovlašteni zaposlenici kompjutorskim se sustavom neovlašteno koriste za osobne potrebe. Krađa vremena je najmanje opasan oblik nedopuštena ponašanja, ona ne utječe na cjelovitost i sigurnost rada kompjutorskih mreža i

gospodarske dobrobiti zemlje, te radi sprječavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih."

telekomunikacija, čime se otvara pitanje potrebe njezina inkriminiranja. Tendencija je povećanje broja vanjskih počinitelja.

Razvojem i širenjem informatičke tehnologije raste i broj počinitelja, a njihova *dobna granica* sve je niža. Prema podacima Ministarstva obrane SAD (*Department of Defense*), sofisticiranost alata za počinjenje kaznenih djela u obrnuto je proporcionalnom odnosu s pismenosti delinkvenata, što znači da je za njihovo počinjenje potrebno manje znanja.[38]

Zbog prirode kompjutorskog kriminaliteta, koji ne poznaje zemljopisne i političke granice, s radnjom počinjenja kojoj pogoduje slobodan i nesmetan protok informacija, može se zaključiti da su počinitelji: domaći i strani državljani; uglavnom osobe sa zavidnim informacijskim, telekomunikacijskim i tehničkim znanjem; sposobni usavršavati sredstva i metode za savladavanje sigurnosnih sustava; sa zavidnom međusobnom suradnjom i stalnom stručnom izobrazbom.

Profil počinitelja ovisi o sadržaju kaznenog djela. Ako je riječ o *neovlaštenom pristupu kompjutorskom sustavu,* sastav počinitelja je raznovrstan - zaposlenici, serviseri, komitenti, dobavljači ili, što je i najčešće, hakeri; pri *ometanju podataka i sustava* počinitelji su u pravilu osobe s većim tehničkim znanjem i uglavnom djeluju izvana, a u pravilu su to hakeri, profesionalci ili kriminalci iz organiziranih kriminalnih udruženja, teroristi; *kompjutorske prijevare* u visokom postotku čine zaposlenici tvrtki (*computer personnel)*, dakle osobe ovlaštene za pristup kompjutorskom sustavu – rukovoditelj kompjutorske obrade (*computer-services manager),* programeri, sistem-inženjeri, operateri i dr., dok se za počinjenje djela ne traži veće stručno znanje; *kompjutorsko krivotvorenje* svojstveno je dobrim aplikatorima sofisticirane tehnologije; kaznena djela *povrede autorskih i srodnih prava*, poznata kao *softversko piratstvo*, zasigurno najčešći oblik zlouporabe informacijske tehnologije, ne zahtijevaju veća znanja ili korištenje posebnih sredstava, a karakterizira ih grupno počinjenje kaznenih djela; kaznena djela u vezi s *dječjom pornografijom, ksenofobijom i sl*. (*djela sa štetnim i nezakonitim sadržajem)* čine osobe koje se mogu grupirati u četiri kategorije: prvu *"čine oni koji to rade iz materijalnih pobuda, da bi prodajom ovakvih materijala ostvarili nezakonitu imovinsku korist; u drugu spadaju oni koji se pritom rukovode nekim ideološkim ciljevima, npr. neonacisti i rasisti; u trećoj su psihički poremećene osobe, koje na taj način zadovoljavaju svoje niske pobude, dok četvrtu grupu čine profesionalni kriminalci koji se koriste informatičkom i komunikacijskom tehnologijom da bi olakšali izvođenje svojih nezakonitih aktivnosti".*[39]

U raspravi o počinitelju pojavljuju se dva važna pitanja: 1. kada za kazneno djelo odgovara *opskrbljivač (access-provider i service-provider)* i 2. što je

[38] *Dragičević, bilj. 12,* str. 95.

[39] *Ibidem,* str. 144.

postupanje *s dužnom novinarskom pažnjom* korištenjem kompjutorskog sustava u novinarskoj djelatnosti?

Ad 1. Posrijedi je vrlo suptilna i složena materiji kaznenog prava - *kažnjivost organizatora i opskrbljivača* za prenesene sadržaje putem mreže zbog *počinjenja djela* tzv. *nepravim deliktom nečinjenja*. Imaju li te dvije figure položaj garanta? Prije analize odgovornosti *garanta,* zbog lakšeg razumijevanja ove posve složene materije, valja u nekoliko crta objasniti što je to *nepravo kazneno djelo nečinjenjem*. U teoriji kaznenog prava kaznena djela nečinjenjem dijele se na *prava* i *neprava kaznena djela nečinjenjem*. U skladu s čl. 25. st.1. KZ, kazneno djelo može se počiniti činjenjem i nečinjenjem. *Kazneno djelo nečinjenja* postoji kad počinitelj propusti dužno činjenje. Uvjet postojanja djela sastoji se u pravnoj obvezi na činjenje. Nije sporno postojanje uzročnosti kod pravih kaznenih djela nečinjenjem (*delicta omissiva)*. Otpada pozivanje na nepostojanje djela zato što iz ničega ne može nastati nešto (*ex nihilo nihil)*. Težište odgovornosti je na nesprječavanju posljedice izazvane drugim uzrocima, a morala se i mogla spriječiti. Ekvivalent prouzročenju posljedice kaznenih djela činjenja (*delicta commissiva)* jest nesprječavanje posljedice omisivnih kaznenih djela. Kod tih kaznenih djela počinitelj krši imperativnu normu o poduzimanju određene radnje, nema tu povrede neke garantne dužnosti. Riječ je o negarantnim djelima nečinjenja. U našem postavljenom pitanju naglasak je na *nepravim kaznenim djelima nečinjenjem (delicta commissiva per omissionem)*. Radnja počinjenja sastoji se u kršenju dužnosti sprječavanja nastupanja posljedice. Kaznena odgovornost počiva na obvezi spriječiti nastup posljedice. Ta djela može počiniti samo osoba s određenim svojstvom, čime ulaze u *delicta propria*. Neprava kaznena djela nečinjenjem dijele se na *zakonski regulirana djela nečinjenja,* kod kojih je samo nečinjenje kao radnja počinjenja djela naznačeno u zakonskom opisu bića kaznenog djela, i *zakonski neregulirana djela nečinjenja* kod kojih postoji delikt nečinjenja kao radnja počinjenja iako uopće nije naznačena u zakonskom opisu djela.[40] Navedena trodioba kaznenih djela nečinjenja jest, primjerice, kod kaznenog djela *nepružanja pomoći (čl. 104. KZ)*. Sam zakonski opis prema kojem kazneno djelo čini onaj tko ne pruži pomoć osobi koja se nalazi u izravnoj životnoj opasnosti iako je to mogao učiniti bez veće opasnosti za sebe ili drugoga (st. 1.) ili ako drugoga ostavi bez pomoći u životnoj opasnosti koju je sam prouzrokovao (st. 2.), obuhvaća sliku jedne situacije i obvezu pojedinca na određeno činjenje. Riječ je o pravom kaznenom djelu nečinjenja sa svojim vlastitim zakonskim opisom. Ali ako je nastupila smrt, teška tjelesna ozljeda ili je zdravlje teško narušeno osobi izloženoj opasnosti (st. 3.), nepružanje pomoći postaje zakonski regulirano

[40] Usp. *Bačić, bilj. 29,* str. 147 i dalje; *Ž. Horvatić-P. Novoselec, Kazneno pravo -Opći dio,* MUP RH, Zagreb, 1999., str. 178 i dalje, te *F. Bačić - Š. Pavlović, bilj. 31,* u objašnjenju čl. 25. KZ.

nepravo kazneno djelo nečinjenjem, uz uvjet da je jedna od navedenih posljedica rezultat nehajnog postupanja počinitelja osnovnog djela. Ako je neka od posljedica iz opisa djela obuhvaćena počiniteljevim dolusom, pa i eventualnim, počinitelj će odgovarati za ubojstvo ili umorstvo, odnosno odgovarajuće kazneno djelo teške tjelesne ozljede. Ova treća situacija predstavlja slučaj zakonski nereguliranog nepravog kaznenog djela nečinjenjem. Tu se položaj garanta ocjenjuje u skladu s odredbom čl. 25. st. 2. KZ, općom normom u kojoj se konstituiraju *tzv. garantna djela nečinjenja*. Kod zakonski nereguliranih garantnih kaznenih djela posebno je naglašen odnos, veza pojedinca (počinitelja djela) i zaštićenog dobra, ali osim te garantne situacije postoji i garantna obveza na poduzimanje aktivne radnje radi zaštite pravnog dobra od ugrožavanja ili povrede. *Osnove garantne obveze su zaštita i nadzor*. Granice su odgovarajući pravni propisi.

U našem promatranom slučaju postoji obveza nadzora nad radom trećih osoba, kontrolna funkcija pojedinca (organizatora mreže ili opskrbljivača), a u određenim situacijama i odgovornost opskrbljivača, koji upravljajući mrežom stvara rizik, navlastito u *"prethodnom ponašanju kojim je stvorena opasnost (načelo ingerencije)"*.[41]

U ocjenjivanju postojanja garantnog nadzora i garantne obveze *organizatora mreže* koja prenosi odgovarajući sadržaj valja razlikovati *access-providera,* koji korisnicima stavlja na raspolaganje samo infrastrukturu, od *service--providera,* koji sudjeluje i u sadržajnom oblikovanju informacija.[42] Nije upitna kaznena odgovornost *service-providera* za dolusna djela (prema Konvenciji o kibernetičkom kriminalu postoji odgovornost jedino za dolusno počinjenje kaznenog djela, pritom i mogućnost počinjenja i s eventualnim dolusom). Njihova odgovornost uključuje sve oblike sudjelovanja više osoba u počinjenju kaznenog djela (čl. 35. KZ): počinitelja, poticatelja i pomagatelja.

Za odgovornost *service-providera* ne traži se poduzimanje radnje bez koje druga osoba kazneno djelo ne bi mogla počiniti, dovoljan je već i doprinos kojim se utjecalo na sadržaj radnje počinjenja, na način njezina odvijanja.

S kaznenopravnog stajališta, međutim, delikatniji je položaj opskrbljivača, osobe koja rukovodi mrežom, ali "*ne obavlja nikakvu kaznenopravno relevantnu djelatnost - čak niti u obliku doprinosa djelu - nego korisnicima mreže jednostavno prepušta da rade što ih je volja. S kaznenopravnog stajališta tada se postavlja pitanje o kažnjivosti opskrbljivača za počinjenje djela nečinjenjem*

[41] *Schmölzer, bilj. 19,* str. 900.

[42] Izraz *"service provider" (davatelj usluga)* prema čl. 1.c. *Konvencije o kibernetičkom kriminalu* označava "*i. svaki javni ili privatni entitet koji korisnicima svojih usluga omogućuje komuniciranje pomoću kompjutorskog sustava i ii. svaki drugi entitet koji obrađuje ili pohranjuje kompjutorske podatke za takvu komunikacijsku službu ili korisnike te službe"*.

u smislu nepravog delikta nečinjenjem" (§ 2. austrijskog KZ; riječ je o *Begehung durch Unterlassung*,[43] nap. Š.P.).

"Ostvarenje materijalnog delikta nečinjenjem, tj. kažnjavanje zbog neotklanjanja posljedice, pretpostavlja da je počinitelj na temelju posebne obveze koju mu nameće pravni poredak bio dužan spriječiti nastup posljedice, a njegovo se nečinjenje može izjednačiti s ostvarenjem bića kaznenog djela činjenjem. Odlučna je pretpostavka, dakle, tzv. garantni položaj koji može proizlaziti iz zakona, dragovoljne (ugovorne) obveze ili iz prethodnog činjenja kojim je stvorena opasnost, dok korektiv na temelju jednake vrijednosti igra pritom podređenu i ograničenu ulogu".[44] Opskrbljivač bi mogao odgovarati jedino ako je nekom svojom prethodnom radnjom stvorio opasnost tipičnu i očekivanu za prethodno poduzetu radnju i što se kod njega upravo poradi nečinjenja stvara obveza i mogućnost poduzimanja dužne radnje kojom će se spriječiti nastupanje zabranjene posljedice.

Upravljajući mrežom opskrbljivač stvara izvjesni rizik, jer među inim druge osobe (partneri) mogu zlorabiti danu im slobodu u korištenju mreže, čega je opskrbljivač svjestan, ali i uz to ne poduzima adekvatne mjere, već pristaje na postojeće stanje, s njime se miri, ispravno na strani takvog opskrbljivača, svjesnog kaznenopravno relevantnih događaja, postoji kaznenopravni "*temelj*" odgovornosti *"za nepravo kazneno djelo nečinjenjem"*.[45]

Potpuno je druga situacija s kaznenom odgovornošću *access-providera*. Njegova obveza se iscrpljuje u osiguranju infrastrukture partnerima bez ikakvih daljnjih ovlaštenja u mreži kojom upravlja. U određenim situacijama njegova bi se odgovornost mogla podvesti u garantnu obvezu *nadzora nad radom trećih osoba*, izvan slučajeva dragovoljnog preuzimanja zaštitne funkcije ili slučajeva opasne prethodne radnje. Autoritet ili obveza nadzora, postupanje s položaja nadređenog prema podređenom, moglo bi zbog propusta nadzora dovesti do kaznenopravne odgovornosti. Opskrbljivač pritom mora biti svjestan kaznenopravnih događaja na mreži, ali "zatvaranjem očiju" prelazi preko toga, pasivno se ponaša, iako realno može spriječiti nastavak kriminalnih postupaka. Na njegovoj subjektivnoj strani uglavnom će se raditi o *dolus eventualis*. Ovdje je, kao što je već rečeno, za kaznenu odgovornost opskrbljivača značajno postojanje pravnih propisa o uređenju dužnosti nadzora poradi zaštite trećih osoba koje se koriste mrežom.

Ad 2. Kriteriji odgovornosti u hrvatskoj informativnoj djelatnosti normativno su regulirani u *Ustavu Republike Hrvatske* (NN, 124./00. - pročišćeni tekst)[46],

[43] V. *Foregger-Fabrizy, bilj. 33.*, str. 29.

[44] *Schmölzer, bilj. 19,* str. 900.

[45] *Ibidem*.

[46] "Jamči se sloboda mišljenja i izražavanja misli.

Sloboda izražavanja misli obuhvaća osobito slobodu tiska i drugih sredstava priopćavanja, slobodu govora i javnog nastupa i slobodno osnivanje svih ustanova javnog priopćavanja.

Zakonu o javnom priopćavanju (NN, 69./03.-pročišćeni tekst)[47] i *Zakonu o elektroničkim medijima* (NN, 122./03.)[48]. Nezaobilazni međunarodni dokumenti jesu *Konvencija o zaštiti ljudskih prava i temeljnih sloboda (NN-MU, 6./99.)*.[49] i *Povelja temeljnih ljudskih prava Europske unije* od 8. prosinca 2000.[50]

Potrebe ovoga rada ne dopuštaju širu raspravu o odgovornosti pri obavljanju novinarske djelatnosti, no u svakom slučaju ovdje se ta odgovornost postavlja

---

Zabranjuje se cenzura. Novinari imaju pravo na slobodu izvještavanja i pristupa informaciji.

Jamči se pravo na ispravak svakome komu je javnom viješću povrijeđeno Ustavom i zakonom utvrđeno pravo" (članak 38.).

"Zabranjeno je i kažnjivo svako pozivanje ili poticanje na rat ili uporabu nasilja, na nacionalnu, rasnu ili vjersku mržnju ili bilo koji oblik nesnošljivosti" (članak 39.).

[47] "(1) Javna glasila dužna su objavljivati točne, cjelovite i pravodobne informacije, poštujući pravo javnosti da bude upoznata o događajima, pojavama, osobama, predmetima ili djelatnostima, kao i druga pravila novinarskog zanimanja i etike.

(2) Javna glasila dužna su poštivati privatnost, dostojanstvo, ugled i čast građana, a poglavito djece, mladeži i obitelji.

(3) Zabranjeno je objavljivati informacije prikupljene na nezakonit način (prislušnim uređajima, skrivenim kamerama, krađom, protupravnom uporabom sredstava automatske obrade podataka i slično) te informacije koje su zakonom određene državnom ili vojnom tajnom" (članak 13.).

"(1) Zabranjena je promidžba i javno izlaganje tiskovina s naslovnicama pornografskog sadržaja" (članak 17. stavak 1.).

[48] " Programski sadržaji nakladnika koji obavlja djelatnost radija i televizije trebaju osobito:

- objavljivati istinu, poštivati ljudsko dostojanstvo i temeljne slobode te pridonositi poštovanju tuđih mišljenja i uvjerenja,

- pridonositi slobodnom oblikovanju mišljenja, svestranom i objektivnom informiranju slušatelja i gledatelja, kao i njihovoj izobrazbi i zabavi,

- promicati hrvatske kulturne stečevine i poticati slušatelje i gledatelje na sudjelovanje u kulturnom životu,

- promicati međunarodno razumijevanje i osjećaj javnosti za pravdu, braniti demokratske slobode, služiti zaštiti okoliša, boriti se za ravnopravnost žena i muškaraca,

- promicati razumijevanje za pripadnike nacionalnih manjina" (članak 12.).

[49] "1. Svatko ima pravo na slobodu izražavanja. To pravo obuhvaća slobodu mišljenja i slobodu primanja i širenja informacija i ideja bez miješanja javne vlasti i bez obzira na granice. Ovaj članak ne sprječava države da podvrgnu režimu dozvola ustanove koje objavljuju djelatnosti radija i televizije te kinematografsku djelatnost.

2. Kako ostvarivanje tih sloboda obuhvaća dužnosti i odgovornosti, ono može biti podvrgnuto formalnostima, uvjetima, ograničenjima ili kaznama propisanim zakonom, koji su u demokratskom društvu nužni radi interesa državne sigurnosti, teritorijalne cjelovitosti ili javnog reda i mira, radi sprječavanja nereda ili zločina, radi zaštite zdravlja ili morala, radi zaštite ugleda ili prava drugih, radi sprječavanja odavanja povjerljivih informacija ili radi očuvanja autoriteta i nepristranosti sudbene vlasti" (članak 10.).

[50] "1. Svatko ima pravo na slobodu izražavanja. To pravo obuhvaća slobodu mišljenja i slobodu primanja i širenja informacija i ideja bez miješanja javne vlasti i bez obzira na granice.

2. Poštuje se sloboda i pluralizam medija" (članak 11.). O Povelji v. u: *N. Bodiroga - S. Barić, Povelja temeljnih ljudskih prava s komentarom,* Organizator, Zagreb, 2002.

u kontekstu poštovanja novinarske etike i navlastito prohibitivne norme iz čl. 39. URH o zabrani *govora mržnje*.[51]

Tri kaznena djela iz KZ

Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava

Članak 223.

(1) Tko unatoč zaštitnim mjerama neovlašteno pristupi računalnim podacima ili programima.

kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(2) Tko onemogući ili otežа rad ili korištenje računalnih sustava, računalnih podataka ili programa ili računalnu komunikaciju,

kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(3) Tko ošteti, izmijeni, izbriše, uništi ili na drugi način učini neupotrebljivim ili nedostupnim tuđe računalne podatke ili računalne programe,

kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(4) Tko presreće ili snimi nejavni prijenos računalnih podataka koji mu nisu namijenjeni prema, unutar ili iz računalnog sustava, uključujući i elektromagnetske emisije računalnog sustava koji prenosi te podatke, ili tko omogući nepozvanoj osobi da se upozna s takvim podacima,

kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(5) Ako je kazneno djelo iz stavka 1., 2., 3. ili 4. ovoga članka počinjeno u odnosu na računalni sustav, podatak ili program 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.

(6) Tko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugome dostupne posebne naprave, sredstva, računalne programe ili računalne podatke 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 programi ili podaci 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.

[51] Iscrpnije v. u : *V. Alaburić, Sloboda izražavanja u praksi Europskog suda za ljudska prava,* Narodne novine, Zagreb, 2002., i u: *Bačić-Pavlović, bilj. 31,* u objašnjenju čl. 203. KZ.

Uvod

Riječ je o kaznenom djelu iz sastava tzv. *kompjutorskog (računalnog) kriminaliteta*.

Opisi radnje počinjenja kaznenog djela usklađeni su s odredbama članaka 2. do 6. *Konvencije o kibernetičkom kriminalu* (NN-MU, 9./02., u daljnjem tekstu: *Konvencija*), koja u smislu čl. 140. URH predstavlja dio unutarnjeg pravnog poretka Republike Hrvatske. Dispozicije djela iz st. 1. i 2. bile su nekonzistentne sve do ZID-a KZ/03. *St. 2.* (prije st. 1.) obuhvaćao je slučajeve oštećenja, mijenjanja, brisanja, uništenja tuđih računalnih podataka ili računalnih programa, dok je *st. 1.* (prije st. 2.) obuhvaćao neovlašteno pristupanje računalnim podacima ili programima ili neovlašteno presretanje njihova prijenosa. Riječ je o dva potpuno odvojena nedopuštena ponašanja. Prijašnji nelogični raspored ispravljen je ZID-om. U oba slučaja *kompjutor je objekt radnje* i to je ono što povezuje te dvije inkriminacije. U KZ se ne daje pojam za *"podatak*", što se susreće u *njemačkom KZ (§ 202. a - Ausspähen von Daten)*[52] i u *čl. 1b. Konvencije*.

Izrazom *kompjutorski podaci* (*computer data*) označava se svako iskazivanje činjenica, informacija ili koncepata u obliku prikladnom za obradu u kompjutorskom sustavu, uključujući i program koji je u stanju prouzročiti da kompjutorski sustav izvrši određene funkcije (čl. 1.b. Konvencije).

U ovome članku sadržane su inkriminacije protiv tajnosti, cjelovitosti i dostupnosti kompjutorskih podataka i sustava.

Analiza kaznenog djela

Stavak 1.

Kriminalizira se neovlašteni pristup računalnim podacima ili programima unatoč zaštitnim mjerama. Radnja počinjenja neovlaštenog pristupa obuhvaća ponašanja usmjerena na izbjegavanje provjere pristupa središnjem kompjutorskom sustavu i na taj način omogućavanje korištenja podacima, programima i drugim mogućnostima koja inače stoje na raspolaganju ovlaštenom korisniku.

Najčešći počinitelji kaznenog djela su tzv. *hakeri* (npr. poznati slučaj dvojice zadarskih srednjoškolaca koji su 1997. godine upali u kompjutorski sustav Pentagona).

[52] *A. Schönke - H. Schröder, Strafgesetzbuch, Kommentar,* Verlag C. H. Beck, München, 26. izdanje, 2001., str. 1614. U st. 2. toga paragrafa podaci u smislu st. 1. jesu samo oni podaci koji su snimljeni ili prenošeni elektronički, magnetski ili na neki drugi način koji ih štiti od izravnog pristupa: "(2) Daten im Sinne des Absatzes 1 nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden."

Postojećim kaznenim djelom inkriminira se nezakonit pristup (*čl. 2. Konvencije*). Neovlašteni pristup postoji ne samo glede cjeline računalnog sustava nego i njegova dijela.

Računalni podaci ili programi moraju prethodno biti posebno zaštićeni. Tako je u čl. 26. *Zakona o elektroničkom potpisu* (NN, 10./02.) propisano da je potpisnik dužan pažljivo koristiti i čuvati sredstva i podatke za izradu elektroničkog potpisa te zaštititi i čuvati sredstva i podatke za izradu elektroničkog potpisa od neovlaštenog pristupa i uporabe. U čl. 6. st. 1. *Pravilniku o mjerama i postupcima uporabe i zaštite elektroničkog potpisa i naprednog elektroničkog potpisa, sredstava za izradu elektroničkog potpisa, naprednog elektroničkog potpisa i sustava certificiranja i obveznog osiguranja davatelja usluga izdavanja kvalificiranih certifikata* (NN, 54./02.) u postupku provođenja mjera i postupaka uporabe sredstava za izradu elektroničkog potpisa nameće se potpisniku obveza njihove zaštite od neovlaštena pristupa, krađe i oštećivanja. U stavku 2. i 3. toga članka posebna dužnost propisana je glede zaštite i sigurnosti sredstava za izradu naprednog elektroničkog potpisa (sadrži certifikat i elektronički potpis davatelja usluga certificiranja koji je izdao certifikat). U našim financijski i tehnički siromašnim uvjetima nemoguće je u cijelosti osigurati tehničku, programsku i podatkovnu zaštitu.

Moguće su različite mjere i sredstva zaštite. Veoma su skupa sredstva zaštite i osobe koje ju provode. Uobičajene su sljedeće metode i sredstva zaštite: 1. fizička zaštita; 2. provjera pristupa; 3. pravilno postavljanje i zaštita lozinke; 4. kriptografske metode; 5. kerberos; 6. vatreni zidovi *(firewalls);* 7. digitalni potpis; 8. digitalni vremenski biljeg; 9. stenografija; 10. izdvajanje; 11. sigurnosne kopije; 12. zaštita od virusa i 13. nadzor rada i korištenja kompjutorskog i mrežnog sustava.[53]

Glede subjektivne strane inkriminacije traži se *dolusna* radnja (namjerni pristup).

U čl. 223. ili bilo kojem drugom članku hrvatskog KZ nije inkiminirana neovlaštena uporaba kompjutorskog vremena ili usluga. KZ *australijske države Tasmanije (članak 12. Theft Act,* 1968.) kriminalizira *furtum usus* tako što kazneno odgovara osoba koja bez ovlaštenja namjerno uporabi kompjutor.[54]

U *§ 202 a. st. 1. njemačkog KZ* kazneno djelo krađe podataka (*Ausspähen von Daten)* glasi:

"Tko neovlašteno, sebi ili drugome, pribavi podatke koji mu nisu namijenjeni i koji su protiv neovlaštena pristupa posebno zaštićeni, kaznit će se zatvorom do tri godine ili novčanom kaznom."[55]

[53] O svakoj od tih metoda i sredstava zaštite v. u: *Dragičević, bilj. 12,* str. 78-92.

[54] *Wasik, bilj. 13*, str. 265.

[55] V. *Schönke - Schröder, bilj. 52,* str. 1614.

U *čl. 342.1 st. 1. kanadskog KZ* postoji kazneno djelo *neovlaštene uporabe kompjutora (Unauthorized use of computer)*. To kazneno djelo čini onaj tko se prijevarno i neovlašteno (a) izravno ili neizravno koristi kompjutorskim uslugama, ili (b) izravno ili neizravno pomoću elektromagnetskih, akustičnih, mehaničkih ili drugih uređaja prouzročuje prekid rada kompjutorskog sustava, ili (c) izravno ili neizravno pristupi ili omogući pristup u kompjutorski sustav radi počinjenja djela pod (a) ili (b) ili kaznenim djelom iz čl. 430. uzrokuje štetu na elektromagnetskom, akustičkom, mehaničkom ili drugom uređaju odnosno funkciji ili kompjutorskom sustavu. Za to kazneno djelo propisana je kazna zatvora do 10 godina.[56]

U Velikoj Britaniji na snazi je Computer Misuse Act (*Zakon o kompjutorskim zlouporabama*) iz 1990. godine. U njemu se kriminalizira *hacking*. Zakon ima 18 članaka, od kojih se u prva dva inkriminira neovlašteni pristup računalnim programima i podacima, dok treći obuhvaća kazneno djelo neovlaštenog preinačivanja kompjutorskog sadržaja. Prva inkriminacija, temeljni hakerski delikt, glasi:

*"**1.** (1) Za počinjenje kaznenog djela kriva je osoba koja:*

a. s ciljem da osigura pristup bilo kojem programu ili podatku smještenom u bilo kojem kompjutoru postupi tako da kompjutor ostvari neku radnju;

b. namjeravani pristup osigurava neovlašteno, i

c. svjesna je da je kompjutor obavio neku radnju i da ona nije imala ovlaštenje za pristup računalu.

(2) Namjera potrebna za počinjenje kaznenog djela ne mora biti usmjerena na

a. određeni program ili podatke;

b. program ili podatke određene vrste, ili

c. *program ili podatke određenog kompjutora.*

(3) Za kazneno djelo iz ovoga članka osoba proglašena krivom kaznit će se kaznom zatvora do šest mjeseci ili novčanom kaznom 5. razreda ili s obje kazne."
[57]

Iz sadržaja navedene inkriminacije vidi se da se kažnjava svako neovlašteno osiguravanje pristupa računalu. Za razliku od ostalih dvaju kaznenih djela, ono je blaže, kažnjivo je kao sumarni, a ne optuživi delikt.

Kazneno djelo iz članka 2. glasi:

*"**2.** (1) Počinitelj je kriv za kazneno djelo iz ovoga članka ako počini djelo iz članka 1. (kazneno djelo neovlaštena pristupa) s namjerom*

[56] *G. P. Rodrigues, Criminal Code,* Pocket Criminal Code, Carswell, Toronto-Calgary-Vancouver, 1988., str. 179 i 212.

[57] Internet adrese:

- *http://insomnia.org/~arny/cmuse.html*
- *http://www.swan.ac.uk/law/staff/pntodd/statutes/stats-c/computer.htm*
- *http://www.ja.net/CERT/JANET-CERT/law/cma.html*

a. *da počini djelo na koje se odnosi ovaj članak; ili*

b. *da olakša počinjenje takva djela (sebi ili drugoj osobi);*

c. djelo koje namjerava počiniti ili olakšati njegovo počinjenje opisano je u nastavku ovoga članka kao daljnje kazneno djelo.

(2) Ovaj članak obuhvaća kaznena djela

a. *za koja je u zakonu točno utvrđena kazna; ili*

b. *za koja osobi dobi od 21 godine ili starijoj (prethodno neosuđivanoj) može biti izrečena kazna zatvora od pet godina (ili u Engleskoj ili Velsu zbog ograničenja iz članka 33. Magistrates Courts Act 1980 može biti izrečena takva kazna).*

(3) Za primjenu ovoga članka nije odlučno je li daljnje kazneno djelo počinjeno istodobno kad i kazneno djelo neovlaštenog pristupa ili u neko drugo vrijeme.

(4) Počinitelj će odgovarati za djelo iz ovoga članka neovisno o tome što je počinjenje daljnjeg djela nemoguće.

(5) Počinitelj kaznenog djela iz ovoga članka kaznit će se

a. *po presudi donesenoj u sumarnom postupku, kaznom zatvora do šest mjeseci ili novčanom kaznom do propisanog maksimuma, ili s obje kazne, i*

b. *po presudi donesenoj na temelju optužnice, kaznom zatvora do pet godina ili novčanom kaznom, ili s obje kazne."*

Ovaj delikt predstavlja teži oblik djela iz članka 1. (kazneno djelo neovlaštenog pristupa) u slučaju kad predstavlja pripremnu radnju za počinjenje nekog težeg djela za koje je propisana točno određena (fiksna) kazna ili kazna zatvora od pet godina ili u duljem trajanju. Kazneno djelo postoji neovisno o tome je li počinjeno teže, naknadno djelo. Za postojanje djela dovoljno je dokazati počiniteljevu namjeru usmjerenu na počinjenje naknadnog djela (st. 3.) pa i bez obzira na to je li uopće moguće njegovo počinjenje (st. 4.).

Za oba kaznena djela (čl. 1. i 2.) nužno je na strani počinitelja postojanje *izravnog dolusa (dolus directus)* koji ne mora obuhvaćati točno određeni kompjutor *(hardware)* ili programsku podršku (*software)* točno određenog kompjutora, no mora postojati svijest o protupravnosti ponašanja (neovlašteni pristup programima i podacima).

Kazneno djelo iz članka 3. bit će objašnjeno u komentaru st. 3. čl. 223. KZ.

U *Sjedinjenim Američkim Državama* kazneno djelo počinjeno je već samim stvaranjem mogućnosti neovlaštenog programskog pristupa određenim računalnim programima ili osnovnim podacima (*base data)*. Takvom kaznenom dispozicijom nastoji se izbjeći opasnost kažnjavanja samo uspješnih neovlaštenih pristupnika. Kažnjiva je svaka radnja kojom počinitelj nastoji ostvariti svoju namjeru neovlaštenog pristupa u program ili podatkovnu bazu, neovisno o tome je li ona realizirana.[58]

[58] *Wasik, bilj. 13,* str. 261.

Zbog pojačane zaštite američkih državljana i nacionalne sigurnosti, navlastito nakon terorističkog napada na Svjetski trgovinski centar u New Yorku 11. rujna 2001., u SAD je na snazi *Zakon o domovinskoj sigurnosti* (*Homeland Security Act of 2002)*[59]*,* iz iste, 2002. godine, pojačan dodatkom nazvanim *Zakon o povećanju kibernetičke sigurnosti* (*Cyber Security Enhancement Act*)[60]. Tom dopunom (dodatkom) u postojeći zakon unose se nove odredbe usmjerene obuzdavanju širenja mogućnosti programa tzv. *cyber* kriminalaca. Pooštrene su kazne za hakere. Štoviše, za one koji neovlaštenim pristupom u kompjutorske sustave svjesno, namjerno i bezobzirno pokušaju ili prouzroče smrt ili ugroze živote drugih, predviđena je mogućnost izricanja doživotne zatvorske kazne.[61] Daju se šira ovlaštenja i mogućnosti djelovanja policiji, među inim i pravo nadzora telefonskog broja, *e-mail i IP* (*Internet Protocol*, tehničko sredstvo koje omogućava protok informacija iz jedne kompjutorske mreže u drugu - nap. Š. P.) adrese osumnjičenika za *cyber* napade koji traju, kao i policijsko zahtijevanje informacija dobivenih putem *ISP*-ova (*Internet Service Provider*, dobavljač Internet usluga, uglavnom kompanije putem kojih se osigurava pristup Internetu pojedincima, tvrtkama i ostalim zainteresiranim osobama - nap. Š. P.) - za to policiji nije potreban sudski nalog. Primjenom Zakona o povećanju kibernetičke sigurnosti otvara se niz pitanja, navlastito postojanje opasnosti ugrožavanja privatnosti pojedinca.[62] U procjeni opasnosti treba voditi računa je li riječ o kućnim ("vrtnim"), bezopasnim hakerima ili o hakerima-teroristima.[63]

U *Švedskoj* je još 1973. godine donesen *Swedish Data Act,* s dopunama iz 1982. godine koji u čl. 21. predviđa kazneno djelo nedopuštenog, protuzakonitog pristupa podacima.[64]

Kalifornijski kazneni zakon (Californian Penal Code) u *čl. 502.(d)* počinitelјem kaznenog djela neovlaštenog programskog pristupa smatra svaku osobu koja zlonamjerno pristupi kompjutorskoj mreži ili kompjutorskom programu ili bazi podataka, dok u čl. 9. u *Victoria's Crimes (Computer) Act 1988* australij-

[59] Internet adresa:

- *http://www.whitehouse.gov/deptofhomeland/bill/index.html*

[60] Internet adresa:

- http://thomas.loc.gov/cgi-bin/query/F?c107:3:/temp/~c107rovj50:e646:

[61] *Ibidem*, str. 3, sa sljedećim sadržajem: *"(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both"*.

[62] O pregledu i kritici *Zakona o povećanju kibernetičke sigurnosti* v. u: *Anita Ramasastry,* Assistant Professor of Law at the University of Washington, *The Cyber Security Enhancement Act's "Good Faith Disclosure" Exception: A Serious Threat To Individual Privacy,* FindLaw Reosurces, 28. ožujka 2002. (Internet adresa: http://writ.news.findlaw.com/commentary/200220328-ramasastry.html)

[63] *Ibidem,* str. 2.

[64] *Wasik, bilj. 13,* str. 261.

ske države Viktorije postoji kazneno djelo neovlaštenog kompjutorskog pristupa, s radnjom počinjenja koja glasi: *"Nije dopušteno pribavljati pristup ili ulaz u kompjutorski sustav ili dio kompjutorskog sustava bez zakonskog ovlaštenja*."[65]

Stavak 2.

Za razliku od djela iz st. 1. ovoga članka, u ovoj inkriminaciji zaštita se odnosi na sprječavanje radnji počinjenja kojima se onemogućuje ili otežava rad ili korištenje računalnog sustava, računalnih podataka ili programa ili računalnih komunikacija. Više je modaliteta radnje počinjenja: unošenje, prenošenje, oštećivanje, brisanje, kvarenje, mijenjanje ili činjenje neuporabljivim računalnih podataka (čl. 5. Konvencije).

Dolus počinitelja obuhvaća "*namjerni čin ozbiljnog neovlaštenog sprječavanja funkcioniranja računalnog sustav"* (čl. 5. Konvencije).

Računalni sustav" (computer system) označava svaku napravu ili skupinu međusobno spojenih ili povezanih naprava, od koji jedna ili više njih na osnovi programa automatski obrađuju podatke (čl. 1a. Konvencije).

Stavak 3.

Kazneno djelo sastoji se u oštećenju, izmjeni, brisanju, uništenju ili na drugi način činjenju neuporabljivim ili nedostupnim tuđih računalnih podataka ili računalnih programa.

Oštećenje na određeni način predstavlja kompjutorsku sabotažu. Inkriminiranjem radnje oštećenja nastoji se zaštititi cjelovitost kompjutorskih podataka i programa. Taj oblik kaznenog djela odnosi se prema kaznenom djelu uništenja i oštećenja tuđe stvari (čl. 222. KZ) kao specijalno u odnosu na općenitije kazneno djelo *(lex specialis derogat legi generali)*.

Izmjena je poseban modalitet radnje počinjenja kaznenog djela prijevare (čl. 224. KZ), jer se izravnom izmjenom ili putem programa nezakonito manipulira svojstvima prijevare. Izmjenom tuđih automatski obrađenih podataka ili računalnih programa oni se ujedno kompjutorski krivotvore.

Druge radnje počinjenja jesu *brisanje* ili *uništenje*, kao i svaki *drugi način* činjenja neuporabljivim ili nedostupnim tuđih računalnih podataka ili računalnih programa. Najčešći oblik je ubacivanje kompjutorskog *virusa* s ciljem onemogućavanja ili otežavanja pristupa programima ili podacima ovlaštenih korisnika odnosno stvaranje programskih smetnji. Činjenje neuporabljivim i činjenje nedostupnim tuđih računalnih podataka ili računalnih programa razlikuju se u

[65] *Ibidem*.

tome što je pojam činjenja nedostupnim širi jer uključuje i situacije kada podaci nisu izbrisani ili oštećeni, ali im ovlašteni korisnik ne može pristupiti.

Za dovršenje djela potrebno je nastupanje određene *posljedice - neuporabljivost ili nedostupnost podataka ili programa*.

Kazneno djelo može se počiniti samo s *dolusom* ili, kako ga Konvencija definira, *"namjernim činom neovlaštenog oštećivanja, brisanja, kvarenja, mijenjanja ili činjenja neuporabljivim računalnih podataka"* (čl. 4. st. 1. Konvencije) ili *"namjernim činom ozbiljnog neovlaštenog sprječavanja funkcioniranja računalnog sustava…*" (čl. 5. Konvencije).

Motivi počinjenja su različiti - nezadovoljstvo programera, operatera ili drugog djelatnika zaposlenog u tvrtki u kojoj se koriste kompjutorski podaci; koristoljublje; pribavljanje povjerljivih poslovnih podataka druge tvrtke (gospodarska špijunaža); sabotaža; čin terorističke naravi (npr. brisanje podataka o teroristima za kojima je raspisana tjeralica); prikrivanje drugog kaznenog djela ili sredstvo počinjenja drugog delikta itd.

KZ Austrije u §126a. sadržava kazneno djelo *oštećenja podataka (Datenbeschädigung)* prema kojem se inkriminira nanošenje drugome štete, na način da se podaci, koji se obrađuju, prenose ili čine dostupnima automatskom opremom, a da njima počinitelj djela nije ili nije sam ovlašten raspolagati, izmijene, izbrišu ili učine neuporabljivima**.**

Opis dispozicije glasi :

" (1) Tko neovlašteno preinači, izbriše ili na drugi način učini neuporabljivim kompjutorske podatke koji se obrađuju, prenose ili automatskom opremom čine dostupnim i na taj način drugome prouzročuje štetu, kaznit će se kaznom zatvora do šest mjeseci ili novčanom kaznom do 360 dnevnih dohodaka.

(2) Pod podacima u smislu stavka 1. smatraju se osobni i drugi podaci i programi.

(3) Tko gornjim djelom prouzroči štetu u iznosu većem od 2.000 eura, kaznit će se kaznom zatvora do dvije godine ili novčanom kaznom do 360 dnevnih dohodaka, tko prouzroči štetu u iznosu većem od 40.000 eura, kaznit će se kaznom zatvora od šest mjeseci do pet godina." [66]

U članku 3. *Computer Misuse Act 1990* [67] inkriminira se *neovlašteno preinačivanje kompjutorskog sadržaja* (*Unauthorised modification of Computer material)*.

Opis bića djela glasi:

"(1) Počinitelj je kriv za kazneno djelo:

a. ako poduzme neku radnju kojom prouzroči neovlašteno preinačenje sadržaja bilo kojeg kompjutora, i

[66] *Foregger - Fabrizy, bilj. 33, str. 384.*

[67] V. Internet adrese u *bilj. 57.*

b. ako radnju poduzima s odgovarajućom namjerom i odgovarajućim znanjem.

(2) Odgovarajuća namjera iz (1)b. prethodnog stavka sastoji se u prouzročenju preinačenja sadržaja bilo kojeg kompjutora kako bi se time

a. pogoršao rad bilo kojeg kompjutora,

b. onemogućio ili spriječio pristup bilo kojem programu ili podacima u bilo kojem kompjutoru, ili

c. pogoršao rad takvog programa ili vjerodostojnost takvih podataka.

(3) Namjera ne mora biti usmjerena

a. prema nekom određenom kompjutoru,

b. prema nekom određenom programu ili podacima odnosno prema programu ili podacima neke određene vrste, ili

c. prema nekom određenom preinačenju ili izmjeni neke određene vrste.

(4) Odgovarajuća namjera iz stavka (1)b. obuhvaća znanje o neovlaštenom preinačenju.

(5) U smislu ovoga članka nije važna vrsta preinačenja iz stavka 2. ovoga članka niti je li ono trebalo biti trajno ili privremeno.

(6) U smislu Criminal Damage Act 1971. preinačenje kompjutorskog sadržaja neće predstavljati oštećenje kompjutorskog ili nekog drugog medija za pohranu podataka osim ako ne nastupi fizičko oštećenje kompjutorskog ili drugog medija za pohranu podataka.

(7)Počinitelj kaznenog djela iz ovoga članka kaznit će se

a. za sva djela na kaznu zatvora do šest mjeseci ili novčanu kaznu do propisanog maksimuma ili s obje kazne, i

b. presudom donesenom za optuživo djelo na kaznu zatvora do pet godina ili novčanu kaznu ili s obje kazne."

Ovom inkriminacijom sankcionira se neovlašteno preinačivanje ili uništenje kompjutorskih podataka usmjereno otežavanju ili onemogućivanju ili ometanje korištenja kompjutorskih podataka ili rada kompjutorskog sustava ili dovođenje u pitanje vjerodostojnosti podataka. U kazneno djelo ulaze svi oblici kompjutorskog krivotvorenja, prijevare i sabotaže.

Stavak 4.

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 kompjutorskog sustava koji prenosi te kompjutorske podatke), počinjene tehničkim sredstvom. Temelj te inkriminacije jest članak 3. Konvencije. Djelo se sastoji u namjernom činu presretanja ili neovlaštenom snimanju prijenosa koji nisu namijenjeni počinitelju. Jedna od radnji počinjenja jest i neovlašteno omogućivanje nepozvanoj

osobi da se upozna s takvim podacima. Nepozvanom se smatra svaka osoba koja nije ovlaštena upoznati se s kompjutorskim podacima, uključujući i elektromagnetske emisije kompjutorskog sustava koji prenose te podatke. Omogućivanje da se nepozvana osoba upozna dovoljno je za dovršenje kaznenog djela bez obzira na to je li se nepozvana osoba poslije upoznala s tim podacima. Osoba koja je ovlašteno snimila kompjutorske podatke (primjerice pripadnik sigurnosne službe) odgovarat će za ovo kazneno djelo ako je snimke predala drugoj nepozvanoj osobi.

Postojat će stjecaj ovoga kaznenog djela s nekim drugim djelima, uz mogućnost *inkluzije*. Stjecaj je tako moguć s kaznenim djelom iznošenja osobnih ili obiteljskih prilika (čl. 201.KZ); ucjene (čl. 205. KZ) ili neovlaštenog snimanja ili prisluškivanja (čl. 131. KZ).

Stavak 5.

Po uzoru na kazneno djelo *oštećenja podataka (Datenbeschädigung) švicarskog KZ (čl. 144. bis)*[68] , s obzirom na visinu počinjene štete[69] ili prema posebnom značenju podataka za ustanovu, poduzeće ili državno tijelo, u hrvatski KZ u st. 5. unesen je kvalificirani oblik djela iz st. 1., 2., 3. i 4. ovoga članka.

Iz opisa kaznenog djela ne vidi se na što se šteta odnosi. Je li riječ o šteti nastaloj neposrednim gubicima uzrokovanim radnjom počinjenja ili o troškovima restitucije (*restitutio in integrum*) ili o šteti nastaloj zbog duljeg ili kraćeg 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 treba u smislu čl. 56. KZ počinitelju uzeti kao otegotnu okolnost.

Dolusom je obuhvaćena i svijest o posebnom značenju podataka. Za prouzročenje štete dovoljan je nehaj (čl. 43. st. 2. KZ).

---

[68] *S. Trechsel, Schweizerisches Strafgesetzbuch,* Schulthess Polygraphischer Verlag, 2. izdanje, Zürich, 1997., str. 534. Opis bića kaznenog djela *oštećenja podataka* glasi:

"1. Tko neovlašteno izmijeni, izbriše ili uništi elektronički ili na sličan način snimljene ili prenošene podatke kaznit će se, na zahtjev, zatvorom ili novčanom kaznom.

Ako je počinitelj prouzročio veliku štetu, može biti kažnjen zatvorskom kaznom. Djelo se goni po službenoj dužnosti.

2. Tko proizvodi, stavlja u promet, reklamira, nudi ili na drugi način stavlja na tržište ili daje upute za proizvodnju programa, za koje zna ili može znati da su namijenjeni u svrhe iz navedene toč. 1., kaznit će se kaznom zatvora ili novčanom kaznom.

Ako počinitelj to počini s ciljem pribavljanja koristi, može biti kažnjen kaznom zatvora do pet godina."

[69] Prema *pravnom shvaćanju Kaznenog odjela VSRH* od 24. studenoga 1997., neodređeno vrijednosno zakonsko obilježje *znatna šteta* postoji kad vrijednost prouzročene štete prelazi 30.000,00 kn (*Su 726-IV/97).*

U informatičkom svijetu česta radnja počinjenja ovoga delikta jest širenje kompjutorskih *virusa* ili *tzv. malicioznih kompjutorskih programa* (kompjutorski programi izrađeni s ciljem poremećaja ili uništenja drugih kompjutora i blokiranja kompjutorske mreže). Nedavno je tako osamnaestogodišnji američki haker Internet zarazio virusom *W32.BlasterVorm*. Blasterom je zaraženo najmanje 7.000 kompjutora širom svijeta; Internet je bio blokiran; šteta prouzročena samo Microsoftu kreće se između pet i deset milijuna USA$. Mladom hakeru iz Minneapolisa (SAD) sigurnosni propusti u operacijskom sustavu *Windows* omogućili su nesmetan pristup u tisuće kompjutora s kojih je uslijedio napad na Microsoftov *site* (lokacija na Webu) 16. kolovoza 2003. Nakon što je otkriven i uhićen, a potom pušten uz posebne mjere opreza (zabrana pristupa Internetu ili kojoj drugoj mreži uz stavljanje na elektronički monitor), hakera očekuje suđenje, a ako bude proglašen krivim, očekuje ga kazna zatvora do deset godina i novčana kazna od 250.000 USA$ zbog namjernog prouzročenja i pokušaja prouzročenja štete. Zbog prirode, značenja i težine kaznenog djela u akciju otkrivanja i uhićenja uključio se *FBI (Federal Bureau of Investigation)*.[70]

Stavak 6.

U st. 6. inkriminira se *zlouporaba naprava* iz čl. 6. Konvencije. Riječ je o *dolusnom* (namjernom) neovlaštenom činu proizvodnje, prodaje, pribavljanja radi uporabe, uvoza, distribuiranja ili činjenja dostupnim na neki drugi način naprava, uključujući i računalne programe, stvorenih ili prilagođenih prvenstveno radi počinjenja kaznenog djela iz stavaka 1., 2., 3. 4. ovoga članka ili računalne lozinke, pristupne šifre ili slične podatke, kojima bi se omogućilo pristupanje cjelini ili nekom dijelu računalnog sustava, s namjerom da budu uporabljeni u svrhu počinjenja tih kaznenih djela ili o posjedovanju neke od navedenih stvari namijenjenih za počinjenje kaznenih djela iz st. 1., 2., 3. i 4. ovoga članka.

Ako je počinitelj radnje djela iz st. 6. ujedno i počinitelj nekog od kaznenih djela iz st. 1.-4., neće odgovarati i za djelo iz st. 6., jer je riječ o kaznenom djelu iz sastava tzv. *delicta preparata*.

Stavak 7.

Ova odredba temelji se na sigurnosnoj mjeri oduzimanja predmeta (čl. 80. KZ).

[70] V. *R. Gabelić, Posljednja opomena informatičkom svijetu,* Poslovni tjednik, Zagreb, br. 76./03., str. 54/55; *Otkriven kreator Blastera,* Jutarnji list, Zagreb, 31. kolovoza 2003., str. 9.; *Uhićen pa pušten autor virusa Blaster,* Novi list, Rijeka, 31. kolovoza 2003., str. 12.

Stavak 8.

Zbog značenja zaštićenih vrijednosti i težine djela, ovom odredbom propisana je kažnjivost za pokušaj kaznenih djela iz st. 1. do 4. ovoga članka. Time je ujedno ispunjena obveza iz st. 2. čl. 11. Konvencije o kažnjavanju pokušaja počinjenja "*bilo kojeg od kaznenih djela utvrđenih člancima 3.-5., 7., 8. te člankom 9. stavkom 1. točkom (c) ove Konvencije.*"

Odnos toga djela prema drugim kaznenim djelima

U praksi i teoriji sigurno će se postaviti pitanje postoji li jedno kazneno djelo i koje ili stjecaj kaznenih djela ako ista osoba neovlašteno pristupi računalnim podacima ili programima (djelo iz st. 1.), a potom ostvari jednu od posljedica djela iz st. 2. Neke tehnološki razvijene zemlje (Finska, Nizozemska, Velika Britanija, SAD) kombiniraju temeljno hakersko djelo (djelo iz čl. 223. st. 1. hrvatskog KZ) s drugim, nakon neovlaštenog pristupa, počinjenim kaznenim djelom.

Postavlja se, također, pitanje odnosa djela iz st. 2. čl. 223. KZ prema kaznenom djelu krađe (čl. 216.) odnosno djela iz st. 3. čl. 223. i uništenja i oštećenja tuđe stvari (čl. 222.); u slučaju, primjerice, krađe samog medija (npr. *hardwera* - materijalne osnovice koju čini informatička tehnologija, pojednostavnjeno rečeno riječ je o stroju), pojedinih uređaja (npr. *modema* - naprave koja pretvara digitalne signale iz kompjutora i ostalih medija za pohranu podataka u analogne i prenosi ih preko telefonskih linija do drugog modema koji primljeni signal ponovno pretvara u digitalni oblik) ili drugih medija na kojima su navedeni podaci pohranjeni ili uništenja i oštećenja medija. U *Austriji* postoji stjecaj kaznenog djela oštećenja podataka (*Datenbeschädigung*) iz *§ 126a. KZ* i kaznenog djela oštećenja tuđe stvari *(Sachbeschädigung*) iz *§ 125. KZ* u slučaju uništenja ili oštećenja medija na kojem su podaci pohranjeni, odnosno djela iz *§126a*. i djela krađe *(Diebstahl*) iz *§ 127. KZ* u slučaju krađe medija.[71]

Nekoliko napomena o krađi identiteta putem Interneta

Neograničene su mogućnosti novih oblika hakerske aktivnosti putem Interneta. Dok pojedine kriminalne aktivnosti poput dinosaura izumiru, nove se rađaju. Suvremeni tehnološki izazovi stavljaju u kušnju inertne i zastarjele organizacije, sredstva i ljude. Nastaje potreba bitnih promjena, zasijecanje u gotovo arhaične metode borbe protiv novih oblika kriminaliteta. Novi izazov

[71] V. *Foregger - Fabrizy, bilj. 33,* str. 379-381, 385-392.

je *krađa identiteta*. O čemu je zapravo riječ? U svijetu su živa imigracijska kretanja. Iz nerazvijenih i siromašnih zemalja tisuće siromašnih i gladnih kreće se prema razvijenom Zapadu. Mnogi se nastanjuju u bogatim zemljama, žive u ilegali, prijeti im trajni izgon. Sve te svoje nevolje i frustracije mogu ukloniti te si osiguranje normalnog života priuštiti dobivanjem *zelene karte (green card*) ili *dozvole o stalnom boravku*.

Treće tisućljeće na određen način stimulira nastanak nove vrste kažnjivih djela - *krađe identiteta* - i potrebe njihova sankcioniranja. Na Zapadu, konkretno u Italiji, primjerice, skupina talijanskih hakera, zapravo kriminalaca, izmislila je *kloniranje mladenki*, koje su, ne znajući za to, postale supruge imigranata. Putem Interneta i kompjutorske tehnike "kradu" se osobni podaci djevojaka, slažu u krivotvorene dokumente i putem njih legalizira boravak stranaca u Italiji. Tako dobiveno talijansko državljanstvo skupo je plaćeno, koštalo je oko 5.000.000 eura. Gangsterska igra je otkrivena kad su prave vlasnice saznale za krađu i cijeli slučaj prijavile policiji.[72]

Jedino što vlasnicima *e-maila* ostaje jest da budu oprezni pri njihovu korištenju putem Interneta.

U zaštiti protiv krađe identiteta kompjutorska tehnologija i te kako vodi računa - primjerice *smard card* (inteligentna, pametna kartica), osobito u trgovačkom i bankarskom poslovanju, s mogućnošću digitalnog potpisivanja i enkripcije, osigurava se kodiranjem podataka i primjenom *tokena*. *Token* (u engl. govornom području *znak, simbol)* poseban je samostalan, osobnom lozinkom zaštićen uređaj, služi primjerice za identifikaciju korisnika izravnog bankarstva, čime se isključuje mogućnost neovlaštenog pristupa računima. Za ulazak u uređaj uporabljuje se sustav jednokratnih lozinki i time onemogućuje korištenje već jednom iskorištene lozinke.

Računalno krivotvorenje

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.

[72] Dnevne novine *Novi list,* Rijeka, 7. prosinca 2002., str. 68.

(3) Tko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugome dostupne posebne naprave, sredstva, računalne programe ili računalne podatke 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 programi ili podaci 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 2. ovoga članka počinitelj će se kazniti.

Uvod

Novo je kazneno djelo u KZ uneseno na temelju *Konvencije o kibernetičkom kriminalu* (NN-MU, 9./02., u daljnjem tekstu: *Konvencija*), koja je u skladu s čl. 140. URH dio unutarnjeg pravnog poretka Republike Hrvatske.

Moderno, novo doba karakterizira *elektronička pošta* (elektronička razmjena podataka između pravnih i fizičkih osoba), elektroničko poslovanje i ostali oblici daljinskog komuniciranja. Radi zaštite podataka i dokumenata u toj razmjeni bilo je nužno predvidjeti zaštitu i putem kaznenopravne reakcije. Sigurnost odvijanja te razmjene obuhvaća nekoliko segmenata. Najprije osiguranje osobe koja je sastavila dokument s ciljem osiguranja njezine vjerodostojnosti. Zatim zaštita autentičnosti *podataka u prometu (traffic data;* kompjutorski podaci u vezi s komunikacijama stvorenim pomoću kompjutorskog sustava koji je dio komunikacijskog lanca, a naznačuju podrijetlo komunikacije, njezino odredište, put, vrijeme, datum, veličinu, trajanje ili vrstu te usluge - čl. 1.d. Konvencije). Zaštićuju se podaci koji se koriste u *pravnom prometu* (*traffic data)*. 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 kompjutorskih sustava odnosno naprava kao dijela toga sustava.

U čl. 7. Konvencije kazneno djelo *računalnog krivotvorenja* postoji kao namjerni delikt u slučaju neovlaštenog unošenja, mijenjanja, brisanja ili činjenja neuporabljivim računalnih podataka, čega je posljedica nevjerodostojnost podataka, pri čemu postoji *dolus* usmjeren na to da se oni u pravnom prometu smatraju vjerodostojnima, ili da se po njima postupa kao da su takvi, i to bez obzira na to jesu li ti podaci izravno čitljivi i razumljivi. Konvencija strani potpisnici omogućuje da može propisati da tek postojanje prijevarne ili slične nepoštene namjere povlači kaznenu odgovornost.

Kazneni zakon SR Njemačke ima dva kaznena djela – *krivotvorenje podataka s dokaznom snagom* – § 269. (*Fälschung beweiserheblicher Daten)* i *mijenjanje*

podataka – § 303a. (*Datenveränderung)*. Prvo djelo (§269.) označava kompjutorsko krivotvorenje u kojem se inkriminira prijevarna radnja u pravnom prometu koja se sastoji od izradbe ili promjene podataka važnih za dokazivanje tako da oni pri njihovu očitovanja predstavljaju lažnu ili krivotvorenu ispravu, ili uporaba tako prepravljenih ili izmijenjenih podataka. Smisao inkriminacije je zaštita sigurnosti i pouzdanosti (uvjerljivosti, izvornosti, autentičnosti) pravnog prometa i podataka (elektroničkih dokumenata) u prometu. Drugo djelo (§ 303 a.) sastoji se u protupravnom brisanju, zatajivanju, činjenju neuporabljivim ili mijenjanju podataka.[73]

Analiza kaznenog djela

Stavak 1.

Radnja počinjenja alternativno je određena. Djelo se može počiniti svakom neovlaštenom izradbom, unošenjem, brisanjem, izmjenom ili činjenjem neuporabljivim kakvog računalnog podatka ili programa.

Da bi postojalo djelo, nužno je da računalni podatak ili program imaju vrijednost za pravne odnose. Računalni podatak ili program mora, dakle, biti prikladan ili određeno služiti kao dokaz postojanja neke činjenice, nekog pravnog posla, pravnog ili drugog događaja bitnog za pravne odnose ili poslovni promet. Osim toga, za postojanje djela treba utvrditi počiniteljev *dolus* - da se krivotvoreni računalni podatak ili program uporabi kao pravi.

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

U opisu djela objekt radnje nije određen u skladu s Konvencijom, koja u čl. 7. sadrži računalne podatke, ali ne i programe (čl. 223.a KZ). Naime, u čl. 1. b. Konvencija pod pojmom računalnih podataka (*computer data*) razumije svako iskazivanje činjenica, informacija ili koncepata u obliku prikladnom za obradu u računalnom sustavu, uključujući i program koji je kadar prouzročiti da računalni sustav izvrši određenu funkciju. Nije, dakle, u KZ trebalo unositi i programe kao objekt radnje. Program, inače dio računalnih podataka, predstavlja niz naloga koji definiraju redoslijed koraka koje kompjutor treba izvršiti s navedenim podacima da bi se dobile željene informacije; to je postupak prevođenja problema na jezik koji kompjutor prihvaća.

Djelo je *delictum communium*.

Može se počiniti samo s *izravnim dolusom (dolus directus)*. Za postojanje djela traži se utvrđenje posebne namjere (uporaba krivotvorenih računalnih podataka).

[73] *Schönke - Schröder, bilj. 52,* str. 2245 i 2345.

Stavak 2.

Inkriminacijom iz st. 2. posebno se od počinjenja kaznenog djela iz st. 1. zaštićuju podaci ili programi određenih tijela, ustanova ili društava. Tako se tom odredbom zaštićuju računalni podaci ili programi, primjerice Ministarstva obrane, Ministarstva financija ili podaci Vodoprivrede Republike Hrvatske.

Drugi (alternativni) oblik ovoga kaznenog djela postoji kad je djelom iz st. 1. prouzročena *znatna šteta***.**[74]

Počinitelj može biti bilo tko (*delictum communium)*.

Djelo je *dolusno*. Dolus obuhvaća svijest i znanje o korisniku računalnih podataka, odnosno da se djelom uzrokuje znatna šteta. Za voljni element nužno je postojanje posebne namjere, pa se djelo može počiniti samo s izravnim dolusom.

Stavak 3.

U ovoj odredbi inkriminira se svaka neovlaštena izradba, nabavljanje, prodaja, posjedovanje ili činjenje drugome dostupnim posebnih naprava, sredstava, računalnih programa ili računalnih podataka stvorenih ili prilagođenih za počinjenje kaznenog djela iz st. 1. ili 2.[75]

Ovdje, kao i kod kaznenog djela iz čl. 277. (izradba, nabavljanje, posjedovanje, prodaja ili davanje na uporabu sredstava za krivotvorenje) i iz čl. 314. (izradba, nabavljanje, posjedovanje, prodaja ili davanje na uporabu sredstava za krivotvorenje isprava), zakonodavac nastoji osigurati kaznenopravnu intervenciju u ranijoj fazi, prije počinjenja nekog drugog kaznenog djela (iz st. 1. i 2. čl. 223.a). Kazneno djelo je nesamostalno (*delictum preparatum*) u slučaju kad njegov počinitelj ostvari i djelo iz st. 1. ili st. 2. Nema stjecaja s djelima iz st. 1. i 2., jer se djelo iz st.3. gubi. Djelo je formalni delikt, iscrpljuje se samom, alternativno određenom, radnjom počinjenja.

Kazneno djelo je *dolusno*. Dolus 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.

Stavak 4.

Instrumenta sceleris (predmeti namijenjeni za počinjenje kaznenog djela iz st. 1. ili 2.) u smislu čl. 80. st. 3. KZ obvezno se oduzimaju, neovisno o njihovu vlasništvu.

[74] V. *pravno shvaćanje VSRH u bilj. 69.*

[75] *O pojedinim modalitetima radnje počinjenja v. objašnjenje uz čl. 223. st. 6.*

Stavak 5.

Zbog težine i opasnosti kaznenih djela iz st. 1. i 2. u ovoj odredbi je propisano kažnjavanje za pokušaj tih djela, kako je to određeno u st. 2. čl. 11. Konvencije.

Računalna prijevara

Članak 224.a

(1) Tko s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist izmijeni tuđe računalne podatke ili računalne programe ili na drugi način utječe na njihovo korištenje i na taj način prouzroči štetu drugome,
kaznit će se kaznom zatvora od šest mjeseci do pet godina.
(2) Tko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugome dostupne posebne naprave, sredstva, računalne programe ili računalne podatke 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.
(3) Posebne naprave, sredstva, računalni programi ili podaci stvoreni, korišteni ili prilagođeni za činjenje kaznenih djela, a kojima je počinjeno kazneno djelo iz stavka 1. ili 2. ovoga članka oduzet će se.
(4) Za pokušaj kaznenog djela iz stavka 1. ovoga članka počinitelj će se kazniti.

Stavak 1.

Računalna prijevara je novo kazneno djelo. Temelj inkriminacije je *Konvencija o kibernetičkom kriminalu* (NN-MU, 9./02., u daljnjem tekstu: *Konvencija*).[76]

U čl. 8. Konvencije određeni su bitni elementi inkriminacije. Stranama potpisnicama Konvencije sugerira se usvajanje zakonskih mjera kojim će se u unutarnjem zakonodavstvu kaznenopravno sankcionirati *"namjerni čin neovlaštenog uzrokovanja štete na imovini drugoga."*

Radnja počinjenja alternativno je određena - djelo se po Konvenciji može počiniti *"a. bilo kakvim unošenjem, mijenjanjem, brisanjem ili činjenjem neuporabljivim računalnih podataka"* ili *"b. bilo kakvim ometanjem funkcioniranja računalnog sustava."*

[76] Vidi *uvodni dio izlaganja uz čl. 223.a KZ.*

Od kaznenog djela prijevare (čl. 224. KZ) ovo kazneno djelo razlikuje se u tome što počinitelj, time što "*izmijeni tuđe računalne podatke ili računalne programe*" (dio opisa djela iz st. 1. čl. 224.a KZ), ne dovodi *"nekoga*" (fizičku osobu) *"u zabludu ili ga održava u zabludi"* (dio opisa djela iz st. 1. čl. 224.), niti je djelom iz čl. 224.a taj drugi doveden u položaj da "*na štetu svoje ili tuđe imovine nešto učini ili ne učini"* (dio st. 1. čl. 224.).

Objekt kaznenog djela jesu tuđi računalni podaci ili računalni programi. Kako je riječ o tehničkim pojmovima nedefiniranim u čl. 89. KZ, trebalo je po ugledu na čl. 8. Konvencije u opis djela umjesto *"računalni podaci ili računalni programi*" unijeti izraze *"računalni podaci ili računalni sustavi*". Konvencija u čl. 1. izrazom *računalni sustav* označava svaku napravu ili skupinu međusobno spojenih ili povezanih naprava, od koji jedna ili više njih na osnovi programa automatski obrađuje podatke, dok se izrazom *računalni podaci* označava svako iskazivanje činjenica, informacija ili koncepata u obliku prikladnom za obradu u računalnom sustavu, uključujući i program koji je kadar prouzročiti da računalni sustav izvrši određenu funkciju.

Opis djela sličan je kaznenom djelu *prijevarne zlouporabe podataka* (*Betrügerischer Datenverarbeitungsmißbrauch)* iz *§ 148a. austrijskog KZ*). Dispozicija tog djela glasi:

"(1) Tko s namjerom da sebi ili drugome pribavi protupravnu imovinsku korist ošteti imovinu drugoga na način da utječe na učinak automatske obrade podataka programiranjem, unosom, izmjenom ili brisanjem podataka (§ 126a. st. 2.) ili drugim djelovanjem kojim se utječe na sam postupak obrade, može se kazniti kaznom zatvora do šest mjeseci ili novčanom kaznom do 360 dnevnica.

(2) Tko ovo djelo ponovi ili prouzroči štetu čija vrijednost prelazi 2.000 eura, kaznit će se kaznom zatvora do tri godine; tko ovim djelom prouzroči štetu veću od 40.000 eura, kaznit će se kaznom zatvora od jedne do deset godina."[77]

I *njemački KZ* u *§263 a.* ima kazneno djelo *kompjutorske prijevare (Computerbetrug)* sa slijedećom dispozicijom:

"(1) Tko u namjeri da sebi ili drugome pribavi protupravnu imovinsku korist, prouzroči drugome štetu na način da neodgovarajućim programiranjem, uporabom netočnih ili nepotpunih podataka ili drugim neovlaštenim djelovanjem utječe na tijek ili rezultat obrade podataka, kaznit će se kaznom zatvora do pet godina ili novčanom kaznom.

(2) Smisleno se primjenjuju stavci 2.-5. § 263."[78]

Iako je to kazneno djelo sa svojim specifičnostima, ali kao *lex specialis* prijevare, na njega se smisleno (*mutatis mutandis*) primjenjuju odredbe kaznenog djela *prijevare (Betrug)* iz *§ 263*.[79]

[77] *Foregger - Fabrizy, bilj. 33,* str. 457.

[78] *Schönke - Schröder, bilj. 52,* str. 2105.

[79] *Ibidem,* str. 2047.

Radnja počinjenja kaznenog djela iz st. 1. čl. 224.a KZ alternativno je određena. Sastoji se od izmjene tuđih računalnih podataka ili računalnih programa ili drugog načina utjecaja na njihovo korištenje.

U opisu djela postoji izvjesna nelogičnost. S jedne strane za njegovo ostvarenje dovoljno je utvrditi da se ono čini iz koristoljubivih pobuda -*"s ciljem pribavljanja protupravne imovinske koristi",* 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 *dolusom,* pri čemu se traži specijalna namjera (pribavljanje protupravne imovinske koristi), dok je za prouzročenje štete drugome dovoljan nehaj (čl. 43. st. 2. KZ).

Stavci 2. do 4.

O tim inkriminacijama v. izlaganje uz čl. 223.a st. 3. do 5.

Ostala kaznena djela u svezi s uporabom kompjutora (najkraće)

Kako je već rečeno (I. Kriminološki diskurs), preostala djela sadržana su u čl. 9. i 10. Konvencije, a odnose se na dječju pornografiju i povredu autorskih i srodnih prava. U KZ su to sljedeća kaznena djela: iskorištavanje djece ili maloljetnika za pornografiju (čl. 196.), upoznavanje djece s pornografijom (čl. 197.), povreda prava autora ili umjetnika izvođača (čl. 229.), nedozvoljena uporaba autorskog djela ili izvedbe umjetnika izvođača (čl. 230.), povreda prava proizvoditelja zvučne ili slikovne snimke i prava u svezi s radiodifuzijskim emisijama (čl. 231.) te dva kaznena djela iz Zakona o autorskom pravu (čl. 124a. i 124b.).[80]

IV. ZAKLJUČAK

Što iznijeti na kraju rada, kako bi trebao glasiti njegov *sažetak,* kakva bi bila njegova poruka*?* Nameće se nekoliko osnovnih misli: na pomolu je novo kompjutorsko (računalno, kibernetičko) kazneno pravo, sa svim svojim specifičnostima i otvorenim pitanjima; njegova temeljna karakteristika je transnacionalnost i potvrda potrebe postojanja međunarodnog kaznenog prava, s kompju-

[80] O tim kaznenim djelima v. u: *F. Bačić-Š. Pavlović, Kazneno pravo - Posebni dio,* Informator, Zagreb, 2001., str. 163-164, 243-249, 250-252, te od *istih autora, bilj. 31,* u objašnjenju navedenih članaka KZ i u dijelu knjige koji se odnosi na *tzv. posebno kazneno zakonodavstvo*.

torskim kaznenim djelima kao njegovim neodvojivim dijelom; kaznenopravna reakcija tu je više usmjerena na zaštitu netjelesnih nego na dosadašnje tradicionalne materijalne vrijednosti; u kompjutorskim kaznenim djelima sučeljena su dva suprotna prava - slobodan protok, dostupnost i pravilnost informacija, s jedne strane, i zaštita interesa drugih na koje se informacija odnosi (jamčenje prava na zaštitu osobnih podataka), uz njihovo istodobno pravo pristupa informacijama koje su o njima drugi saznali, s druge strane; kako stati na kraj zlouporabi informacijske tehnologije, pritom polazeći od toga da je kaznenopravna intervencija *ultima ratio societatis*.

Sofisticiranost informacijske tehnologije i dobra upućenost počinitelja kompjutorskih kaznenih djela u sve njezine tajne više je nego ozbiljan signal međunarodnoj zajednici i njezinim članicama, među njima i Hrvatskoj, da se tim kaznenim djelima posebno posvete, jer se njihovim počinjenjem uzrokuje se ne samo materijalna šteta u milijardama USA $ nego se, što je još opasnije i pogibeljnije, krši *temeljno ljudsko pravo na poštovanje privatnog života, doma i komunikacije*.

Na kraju. *Globalizacija* je zahvatila ne samo ekonomske, kulturne, političke i vojne prostore nego i našu virtualnu stvarnost, s pojavom *prava na pružanje otpora* kao reakcije na taj proces, navlastito isticanjem zahtjeva za svekolikom samostalnošću, uključujući stvaranje novih mreža, ali i opasnošću pojave radikalnog individualizma i fundamentalizma s njihovim različitim oblicima i lošim stranama. Umreženo društvo, umreženi planet Zemlja stavlja nas u ozbiljna iskušenja, dovodi u pitanje naša individualna prava i slobode, vodi nas prema *Orwellovim: Animal Farm* i *Nineteen-Eighty-Four!* Protiv međunarodnog organiziranog kriminala, s kompjutorskim kaznenim djelima kao njegovom bitnom sastavnicom, koju posebno karakteriziraju terorizam, prostitucija, pedofilija, pornografija, krađe tuđih intelektualnih ostvarenja i tuđeg identiteta, krivotvorenja i prijevare, međunarodna zajednica i svaka njezina članica trebaju djelovati *nunc aut numquam!*

Summary

COMPUTER CRIME IN THE CRIMINAL CODE

In this paper the author deals with the criminal-law aspect of computer crime, without neglecting the criminological aspect. This work consists of several parts with a short introduction in which the issues and problems related to computer criminality are presented, such as: the specific feature of this criminality and its definition, as well as a criminal-law analysis in which the author provides an overview of international documents and solutions in the Croatian Criminal Code with a comparative presentation of criminal offences in some other countries (Austria, Germany, USA, Great Britain, etc.).