Rusmir TANOVIĆ [1]

Kaznenopravna zaštita informacijskih sustava

Criminal Law Protection of Information systems

Sažetak

U ovom izlaganju o veoma kompleksnoj problematici kompjuterskog kriminaliteta, moglo bi se istači da kaznena zakonodavstva koja nemaju zakonsku regulativu kompjuterskih kaznenih djela, odnosno, kaznenih djela vezanih za zloupotrebe korištenja elektronskog računala, Interneta, u svom zakonskom reguliranju ove problematike, uputno bi bilo slijediti rješenja kaznenih zakonodavstava SR Njemačke i R Austrije te kombinirati njemački i austrijski pristup u konstrukciji novih inkriminacija. Sve to iz razloga, obzirom da su u spomenutim zakonodavstvima u potpunosti označeni zaštitni objekti inkriminacija, individualni i društveni interes utvrđen sa visokom preciznošću i visokom legislativnom preciznošću u definiranju inkriminacija, jer su spomenuta zakonodavstva u potpunosti penalizirala pojave zloupotreba nastalih korištenjem elektronskog računala.

Uvod

Primjena elektronskog računala danas veoma je rasprostranjena. Gotovo da nema područja ljudske djelatnosti na kojem elektronsko računalo u suvremenom razvijenom svijetu ne nalazi svoju primjenu, od gospodarstva, državne uprave, znanosti do osobnih i kućnih računala. Funkcioniranjem i primjenom elektronskog računala javio se i problem pravne regulative primjene elektronskog računala u različitim područjima ljudske djelatnosti.

[1] Diplomirani pravnik

Primjenom elektronskog računala, pojavile su se i opasnosti njegove zloupotrebe. Informatička revolucija od 20% početkom 80-tih godina donijela je sa sobom brojne oblike manipulacija sa elektronskim računalom.[2] Oblici manipulacija su brojni i raznovrsni, počev od manipulacija sa podacima prilikom njihova unosa u elektronsko računalo preko neovlaštenog pristupa računalu i korištenja pohranjivanjem podataka do njihovog mijenjanja ili brisanja onesposobljavanjem ili uništavanja cjelokupnog sustava, bilo u pogledu njegove materijalne osnovice odnosno podrške (engl. *hardwere*) kao što je samo računalo sa svojim ulaznim uređajima, kontrolnom jedinicom, aritmetičko-logičkom jedinicom i glavnom memorijom te izlaznim uređajima i sredstvima za komuniciranje na daljinu, bilo u pogledu nematerijalnih elemenata kao što su programi, metode, vezane uz organizaciju, upravljanje, obradu, korištenje rezultata obrade podataka (engl. *softwere*).[3] U praksi je zabilježen čitav spektar napada na programsku podršku elektronskog računala.

Prema autoru J. Soyka , kaznena djela učinjena uz korištenje elektronskog računala ili kompjuterska kaznena djela najčešće se pojavljuju kao imovinski delikti i ne bi se razlikovali od ostalih imovinskih delikata izvršenih uz pomoć tehničkih uređaja, kada ih ne bi obilježavale neke nove, posebne okolnosti kao što su : elektronsko računalo može biti objekt kaznenog djela i sredstvo njegovog izvršenja. Kao objekt kaznenog djela ono se javlja kao tzv. gramatički objekt kod opisa nekih kaznenih djela izvršenih takvim manipulacijama sa strojnom ili programskom podrškom računala koje dovode do njegovog otuđenja, onesposobljavanja ili upropaštavanja. Kao sredstvo izvršenja kaznenih djela, računalo može poslužiti kao predmet sa kojim se počinitelj poslužio pri radnji izvršenja, bez kojega ona ne bi bila ostvariva; Način funkcioniranja elektronskog računala omogućava takav intelektualni angažman počinitelja, koji njegovom djelu pridaje atribute " savršenog zločina", kojeg obilježava pažljivo planiranje, radnja izvršenja koja ne ostavlja materijalne tragove, traje izuzetno kratko, i dovodi do perpetuiranja dislociranih posljedica na duži vremenski period; Manipulacije s elektronskim računalom, počinjene u svrhu pribavljanja protupravne imovinske koristi imaju novi

---

[2] S. Nora/ A. Minc: Die Informatisierung der Gesellschaft, Frankfurt/M - New York 1979.Informatička revolucija je pojam koji se može prikazati godišnjom stopom porasta broja centralnih i tzv. periternih jedinica-terminali vanjske memorije ispisivala i drugo.

[3] V. Ferišaka: Osnove informatike , Informator, Zagreb,1985.

kriminogeni i kriminalistički kvalitet u odnosu na tzv. "knjigovodstvene delikte" i ne mogu se izjednačavati.[4]

Pored manipulacija na elektronskim računalima ili s njima u cilju postizanja imovinske koristi, razvoj informatičke tehnologije donio je i mogućnost njihove upotrebe u cilju napada na druga individualna i kolektivna pravna dobra kao na tajnost podataka osobne naravi koji predstavljaju tzv. intimitet, odnosno privatnu sferu građana te na neka druga politička prava građana.[5]

Danas nema egzaktnih kriminoloških studija o kriminalitetu uz pomoć elektronskog računala.[6] Tamna brojka kriminaliteta je visoka u toj oblasti a razlozi za to su po našem mišljenju poteškoće u otkrivanju i dokazivanju ovakvih kaznenih djela, ne prijavljivanje kaznenih dijela ili ne suradnja sa organima otkrivanja i gonjenja.[7]

I
Kompjuterski kriminalitet

"Kompjuterski kriminalitet predstavlja sva protupravna, nemoralna i nedopuštena ponašanja u svezi s automatskom obradom podataka ili njihovim prijenosom."[8] Međutim, postoje i druge definicije kompjuterskog kriminaliteta. Kompjuterski kriminalitet označava sve slučajeve zloupotrebe elektronskog računala koji su pravno određeni kao kaznena djela. [9]

Pravni teoretičari u SAD koji se bave ovom tematikom, razlikuju: *computer abuse, computer crime* i *computer related*

---

[4] J. Soyka: Computer Kriminalität, Fälle und Fakten, W.Heyne, München, 1986.

[5] U. Sieber: Computer Kriminalitet und Strafrecht, Carl Heymanns Verlag, Köln, 1.Aufl., 1977. 2. Aufl. 1980.

[6] Isto. U Sieber je proveo jedno od najopsežnijih europskih istraživanja sredinom 70-tih godina u kojem je na bazi 31. kaznenog postupka u SR Njemačkoj za kompjuterske delikte dao karakteristične osobine i svojstva osuđenih osoba za kompjuterske delikte.

[7] O tomu opširnije u : A. Bequai , How to Prevent Computer Crime - A. Guide for Managers, J. Wiley and Sons, Chiecester,1983. R. A. H. von zur Mühlen, Computer-Kriminalität, 1972., Magazin "Chip", (SR Njemačka), br. 3 1992., Tjednik Computerwoche (SR Njemačka) od 02. 12. 1983.

[8] Definicija kompjuterskog kriminaliteta dana od međunarodne ekspertne grupe u okviru OECD-a 1983. godine. Computer-Related Crime: Analisis of Legal Policy in the OECD Area, Paris, 1984., DSTI/ICCP.

[9] Ovu definiciju dao je njemački teoretičar R. von zur Mühlen-Computer Kriminalität, Gefahren und Abwehrmassnahmen, Neuwied und Berlin, 1972.

crime. [10] *Computer abuse* obuhvaća namjerne zahvate u programsku podršku računala u cilju stjecanja kakve imovinske koristi. *Computer crime* obuhvaća sve ilegalne radnje sa računalima za progon čijih počinitelja je potrebno poznavanje tehnologije elektronskog računala. *Computer related crime* obuhvaća kriminalitet "bijelog okovratnika", gospodarski i imovinski kriminalitet kao i sve oblike napada na računalo kao sabotaže, uništavanje podataka do ugrožavanja i uništavanja ljudskog života i zdravlja putem računala.

Mišljenja smo da kod ovakvih i sličnih klasifikacija i njihove metodološke vrijednosti, kod pravih definicija pojam "kompjuterski kriminalitet" i njegove klasifikacije treba poći od onoga što takve zlouporabe tehnologije elektronskog računala čini kaznenim djelima.

Na međunarodnom planu, kaznenopravnu zaštitu od kompjuterskog kriminaliteta, poduzela je Organizacija za gospodarsku suradnju i razvoj OECD, koja je 1983. godine formirala odbor stručnjaka koji je dvije godine kasnije, zemljama članicama preporučio u izvještaju *"Computer-related Criminality": Analysis of Legal Policy in the OECD Area*", da razmotre opseg u kojem bi se umišljajne manipulacije s elektronskim računalima mogle kriminalizirati u unutrašnjem pravu, sugerirajući da to bude unošenje, mijenjanje ili brisanje podataka, programa, u namjeri da se ono iskoristi za: protupravni prijenos novca ili vrijednosti, krivotvorenje, oštećivanje ili upropaštavanje računala i njegovih vrijednosnih sustava, i drugo.

Vijeće Europe je na temelju izvještaja jednog ekspertnog komiteta, 13. 9. 1989. godine donijelo Preporuku br. R/89/9. Po njoj, zemlje članice ove međunarodne organizacije trebaju u donošenju novih propisa unutarnjeg kaznenog prava, slijediti minimalnu listu inkriminacija a mogu je proširiti i sa nekim inkriminacijama sa "opcijske liste". Na prvu su stavljene inkriminacije kompjuterske prijevare i krivotvorenja, oštećenje i upropaštavanje podataka i programa, kompjuterska sabotaža, neovlašten pristup podacima i programima, neovlašteno kopiranje programa ili tzv. topografije elektronskog

[10] U pravnom sustavu SAD-a u kome postoji najveći broj inkriminacija kompjuterskog kriminaliteta, nema jedinstvene definicije pojma "kompjuterski delikt" - computer crime. O tomu vidjeti studiju Ministarstva pravosuđa SAD-a, "Computer crime", izdanje Bureau of Justice Statistics, US Department of Justice, Washington, 1979.

mikroprocesora-*chip*-a, a na drugu, neovlašteno mijenjanje programa, podataka, kompjuterska špijunaža te neovlašteno korištenje elektronskog računala tzv. krađa vremena.

Ujedinjeni Narodi su na VIII Kongresu UN o sprječavanju zločina i postupanju sa delinkventima održanom u Havani 1990. godine donijeli rezoluciju, Kongresnu rezoluciju koju je prihvatila u svom trećem odboru Opća skupština UN, svojom rezolucijom 45/121 od 14. 12. 1990. godine, koja od svih država članica UN traži da pojačaju napore u pravcu suzbijanja manipulacija sa elektronskim računalima "koje zaslužuju primjenu kaznene sankcije" te da razmotre primjenu različitih mjera u tom pravcu, među koje spada modernizacija kaznenog prava i postupka.

II
Kaznenopravna inkriminacija u svezi sa zloupotrebama elektronskog računala

Funkcioniranjem elektronskog računala odnosno njegovom primjenom u različitim područjima ljudske djelatnosti javlja se problem pravne regulative i kaznenopravne zaštite.

Teoretičari kaznenog prava i drugi koji se bave problematikom elektronskog računala, funkcioniranjem odnosno primjenom te odnosom kompjuterske tehnologije uopće sa kaznenim pravom i praksom te općenito pravnom regulativom, klasificirali su manipulacije s elektronskim računalom koje suvremeno kazneno pravo obuhvaća svojim inkriminacijama. Teoretičari Jaburek-Schmölzer[11] navode slijedeće oblike manipulacija sa podacima pohranjenim u memoriji računala: manipulacije pri unosu koje se odnose na unos lažnih podataka među prave, krivotvorenje postojećih, uklanjanje postojećih ili kombiniranje ovih načina; manipulacije pri ispisu koje se odnose na krivotvorenje različitih isprava koje su produkt ispisa elektronskog računala kao i neovlašteno distribuiranje dobivenih podataka i drugo.

Teoretičar Gliss[12] razlikuje 25 manipulacija na elektronskom računalu ili manipulacija s računalom prema konfiguraciji računala ili njegovim tehničkim karakteristikama, koje su

---

[11] Jaburek, W. - Schmölzer, G.: Computer - Kriminalität, A. Orae, Wien, 1985.
[12] H. Gliss: Computerkriminalität - Erscheinung sformen, Bedrohungspotential und Wachstumstrends, 1985.

najvažnije: manipulacije s unosom podataka - ulazne; manipulacije sa podacima koji su rezultat obrade u računaru - izlazne manipulacije, prekide i ponavljanja programskih postupaka; testiranje izvornih podataka; stimuliranje ispravne obrade podataka kroz pokusne programe; zaobilaženje kontrolnih mehanizama; izigravanje principa tajnosti i drugo. Ovakve i druge oblike manipulacije na elektronskom računaru uzimamo kao tehničke pojmove i svakako da se razlikuju od kaznenopravnog pojma radnje izvršenja nekog kompjuterskog delikta.

Kod najčešćih oblika manipulacija koje navode teoretičari Jaburek-Schmölzer, Gliss, treba razlikovati to, da li se one vrše zato da bi se neovlašteno utjecalo na normalan rad elektronskog računala ili zato da bi se pomoću njih računalo upotrijebilo u postizanju kakve kriminalne svrhe kao npr. računalo kao sredstvo manipulacije što u oba slučaja može predstavljati kažnjivo djelo.

Međutim, manipulacije na računalu mogu predstavljati dovršene kažnjive radnje tek onda kada je počinitelj prema svojoj zamisli o toj manipulaciji ostvario povredu zaštićenog dobra. Ali, manipulacije sa računalom mogu predstavljati dovršene kažnjive radnje već prije ostvarene povrede zaštićenog dobra jer nakon poduzimanja takve manipulacije do povrede dolazi daljnjom automatskom obradom podataka i nije potrebna počiniteljeva naknadna volja i djelatnost u pravcu kriminalnog iskorištavanja rezultata manipulacije, pa u tom smislu treba razlikovati: manipulacije na strojnoj podršci - *hardwere*; manipulacije na programima - *softwere.*; manipulacije na podacima i informacijama. Elektronsko računalo se može pojaviti kao cilj i sredstvo manipulacija.

Elektronsko računalo kao cilj manipulacija javlja se kod onih nedopuštenih oblika interakcije sa njegovim korisnikom kod kojih ono sa svojom strojnom i programskom podrškom u kaznenopravnom smislu predstavlja gramatički objekt kriminalne radnje kao što su slučajevi napada na strojnu podršku računala - *hardwere*, sa ciljem da se ono onesposobi za redovnu funkciju i neovlašteno mijenjanje ili brisanje programa u cilju njegovog onesposobljavanja što je razlika od cilja stjecanja imovinske koristi te neovlaštenog pristupa programu elektronskog računala da bi se neovlašteno došlo do podataka i informacija koje ono sadrži (to je tzv. kompjuterska špijunaža kao najčešći oblik industrijske špijunaže).

Elektronsko računalo kao sredstvo manipulacija javlja se kod onih nedopuštenih interakcijskih oblika između računala i korisnika koji služe ostvarenju neke kriminalne radnje i u kojima se računalo pojavljuje kao predmet s kojim je počinjena kriminalna radnja. Kod strojne - *hardwere* podrške računala, manipulacije mogu napadati razne interese a ne samo imovinske kao u svrhu industrijske špijunaže, zaokruživanja suma na bankovnim računima metodom tzv. "sjeckanja", "salama tehnike". U literaturi se različito klasificiraju manipulacije sa podacima pohranjenim u memoriji računala, ovisno da li za cilj imaju da se time netko dovede u zabludu ili u njoj održi ili u namjeri pribavljanja protupravne imovinske koristi.[13]

Ipak, kod nekih oblika manipulacija koje mogu dovesti do posljedica i koje nisu samo štetne u smislu pojma građansko pravne deliktne odgovornosti već predstavljaju takav oblik ponašanja da je opravdano postaviti pitanje o društvenoj opravdanosti njihove penalizacije, progona njihovih počinitelja po propisima pozitivnog prava. Time je opravdano da neke karakteristike manipulacija kaznenopravno zaštitimo.[14]

Neke od manipulacija na elektronskom računalu kod kojih se elektronsko računalo pojavljuje kao predmet s kojim je kriminalna radnja izvršena te kod kojih ne postoje zapreke za primjenu već postojećih inkriminacija u postojećim kaznenim zakonima kod kojih takva manipulacija predstavlja samo jedan novi način izvršenja nekog postojećeg kažnjivog djela, ostaju slučajevi manipulacija sa računalom u kojima specifičnosti tehnologije elektronskog računala daju tim manipulacijama poseban stupanj opasnosti ili predstavljaju takav način ponašanja koji se ne može obuhvatiti postojećih inkriminacijama kaznenog prava koje ne prati razvoj tehničkih znanosti, informatičke tehnologije.

Međutim, pri kriminalizaciji nekog ponašanja treba poći od temeljnih postavki među kojima teoretičari kaznenog prava ističu: da određeno dobro predstavlja fundamentalnu društvenu vrijednost koja iziskuje pravnu zaštitu te da napad na njega predstavlja ponašanje sa odgovarajućom količinom kaznenog

---

[13] O tomu opširnije u: Jaburek, W. - Schmölzer, G.: Computer - Kriminalität, A. Orae, Wien, 1985., Zimmerli, E./Liebl, K.: Computermissbrauch, Computersicherheit: Fälle - Abwehr - Aufdeckung, Peter Hohl, Ingelheim, 1984., Wasik, M.: Crime and the Computer, Clarendon, Press, Oxford, 1991.

[14] R. T. Nimmer: The Law of Computert Technology, New York, J. Wiley, 1985.

prava; okolnost da se kao kazneno djelo može predvidjeti neko ponašanje samo ako je to sa stanovišta društvene korisnosti neophodno tj. ako se zaštita temeljnih vrijednosti ne može ostvariti nekim drugim mjerama; inkriminiranjem nekog ponašanja da se može postići uspješna zaštita društva i čovjeka tj. da je konstrukcija kaznenopravne zaštite takva da se može ostvariti u praksi.

Kazneno pravnu zaštitu na planu informacijskih tehnologija treba usmjeriti na nesmetano korištenje podataka te njihov integritet, dostupnosti i pravilnost kao individualna i društvena pravna dobra. Isto tako, kaznenopravnu zaštitu treba ostvariti i na planu zaštite osobnih podataka građana, koja predstavlja zaštitu njihovog tzv. intimiteta, bilo kroz postojeće inkriminacije ili donošenjem novih.

Mišljenja smo da u svezi sa zloupotrebama elektronskih računala treba inkriminirati: neovlašteno korištenje sustava elektronskog računala bez mijenjanja podataka i programa kao što su neovlašteni pristup podacima i programima (*hacking*), prisluškivanje i kompjuterska špijunaža, neovlašteno korištenje usluga elektronskog računala, neovlašteno kopiranje i reprodukcija kompjuterskog programa; neovlašteno mijenjanje podataka i programa kao što su kompjuterska prijevara, krivotvorenje isprava i ovjeravanje neistinitog sadržaja; neovlašteno uklanjanje ili upropaštavanje podataka programske i strojne podrške elektronskog računala, tzv. kompjuterska špijunaža.[15]

III
Usporednopravni prikaz kaznenih zakona u nekim zemljama o zlouporabama elektronskog računala

Veći broj tehnološki razvijenih zemalja donio je nova ili dopunio već postojeća kaznena djela na području materijalnog kaznenog zakonodavstva i kaznenopravno zaštitio funkcioniranje i primjenu elektronskog računala u svezi sa zloupotrebama.

Zakonodavstvo Sjedinjenih Američkih Država

---

[15] O prijedlozima mogućih rješenja inkriminacija u svezi sa zloupotrebama elektronskog računala u Federaciji BiH, vidjeti članak autora Tanović R., "Potreba krivičnopravne regulative, kompjuterski kriminalitet i neophodnost koncipiranja krivičnog djela kompjuterske zloupotrebe", Pravna misao 1-4/96, Sarajevo.

U SAD-u, prva Savezna država Florida, već je 1978. godine donijela inkriminacije protiv zloupotreba elektronskog računala. Ostale države su donijele zakon koji se odnosi na kompjuterske delikte i danas to nije učinila jedino država Vermont. Međutim, ti zakoni su različiti među državama. Na federalnom planu, Kongres je 1984. godine donio "Zakon o krivotvorenju ovlaštenja na pristup elektronskom računalu te prijevari i zloupotrebi računala", a godine 1986., "Zakon o kompjuterskoj prijevari i zloupotrebi". Ona zakona su sadržana u federalnoj zbirci propisa U. S. Code, Tit. 18, pogl. 30 i 47.

Zakon o krivotvorenju ovlaštenja na pristup elektronskom računalu te prijevari i zloupotrebi računala iz 1984. godine, inkriminira samo neovlašteni pristup računalu i pribavljanje informacija te svjesno preinačavanje ili uništenje podataka. U ovom zakonu, kazneni okviri kreću se kod novčane kazne (koja se može izreći samostalno ili zajedno s kaznom zatvora), od 5. 000 dolara (ili dvostrukog iznosa kriminalne koristi) do 100.000 dolara (za povratnike u slučaju kompjuterske špijunaže u korist strane države ili protiv odredbi Zakona o atomskoj energiji iz 1954. godine), kod kazne zatvora od godinu dana do dvadeset godina. Prijevara se inkriminira samo u svezi korištenja ili rasparčavanja krivotvorenih kreditnih kartica i identifikacijskih isprava za bankomate (U. S. Code, Tit. 18, Ch. 47, par. 1029) ukoliko je počinitelju donijela imovinsku korist veću od 1.000 dolara. U oba slučaja kažnjava se i pokušaj.

Zakonski propisi o intelektualnom vlasništvu-*Copyright Act* iz 1976. godine, noveliran 1980. godine,[16] proširili su zaštitu i na kompjuterske programe. *Semiconductor Chip Protection Act* iz 1984. godine, zaštitio je tzv. topografiju mikroprocesora. Zakonski propisi o zaštiti osobnih podataka-*Privacy Act* iz 1974. godine (5 U. S. Code par. 552a), te drugi zakoni o zaštiti "privatnosti" jesu ustavnopravni pojmovi nastali u praksi Vrhovnog federalnog suda SAD-a koji su *Right to Financial Privacy Act* iz 1978.godine (12 U. S. Code par. 3401-3422) koji za kršenje nekih svojih odredbi ustanovljavaju kaznenu odgovornost, zatim *Computer Matching and Data Privacy Protection Act* iz 1988. godine (5 U. S. Code par. 552a), koji predstavlja stanovitu dopunu zakona iz 1974. godine. Regulira korištenje kompjuterske tehnike od strane federalnih organa te

[16] O autorskom pravu SAD-a opširnije u Tanović R.: Osnove precedentnog prava Common Law, DD "Informator", Zagreb, 1998.

organa pojedinih država prilikom nadzora nad platnim prometom u kojem su pojedinci adresati određenih pošiljki.

Zakon o krivotvorenju ovlaštenja na pristup elektronskom računalu te prijevari i zloupotrebi računala iz 1984. godine ograničio se na penalizaciju prijevara i slične djelatnosti u svezi s elektronskim računalima, manipulacijama sa kreditnim karticama odnosno informacijama, ustanovivši za te nove delikte federalnu jurisdikciju te povjerivši istragu za njih "tajnoj službi" ministarstva financija.

Zakon o kompjuterskoj prijevari i zloupotrebi iz 1984. godine, proširio je federalnu zaštitu osobnih podataka na informacije u posjedu financijskih institucija, uveo tri nova kaznena djela: "Neovlašteni pristup računalu u namjeri izvršenja prijevare", "Zlonamjerno oštećenje prilikom neovlaštenog pristupa računalu" i "Neovlašteno odavanje kompjuterskih lozinki". [17]

Zakonodavstvo Velike Britanije

Engleska parlamentarna komisija za zakonodavne reforme-*law commission*, predložila je donošenje Zakona o sprječavanju kompjuterskih zloupotreba, tako da je Parlament, nakon dužih rasprava, 1990. godine, donio Zakon o zloupotrebama putem elektronskog računala-*Computer Misuse Act*, koji je stupio na snagu 28. 08. 1990. godine. Međutim, povod za donošenje toga zakona u Velikoj Britaniji je taj što je Dom lordova 1987. godine ukinuo osudu u jednom slučaju kompjuterskih *hackera* koji su izazvali pažnju javnosti već i stoga koristeći javnu mrežu za prijenos podataka *"Prestel"*, upali u kompjuter vojvode od Edinburgha. Slučaj je zaključen kao *Gold and Schifree case* 1988., 2 WLR 984 HL.

Zakon u dijelu koji određuje inkriminacije, vrijedi i u Škotskoj. Zakon sadrži dvije inkriminacije neovlaštenog pristupa programima i podacima sadržanim u računalu te jednu inkriminaciju neovlaštenog preinačavanja sadržaja (engl. *content*) elektronskog računala. Dvije inkriminacije neovlaštenog pristupa programima i podacima sadržanim u računalu razlikuju se po tome što jedna penalizira već samu

[17] O zakonodavstvu u SAD opširnije u: U. S. Code, Tit. 18, pogl. 30 i 47. , U. S. Code, Tit. 18, Ch. 47, par. 1029, 5 U. S. Code par. 552a, 12 U. S. Code par. 3401-3422, 5 U. S. Code par. 552a, M. Wasik: Crime and the Computer, Clarendon, Press., Oxford, 1991.

činjenicu neovlaštenog pristupa računalu a druga neovlašteni pristup kao pripremnu radnju za druge delikte. Za prvu inkriminaciju predviđa se kazna zatvora do šest mjeseci ili novčana kazna tzv. 5. razreda i kao tzv. sumarni delikt smatra se lakšim kaznenim djelom. Za drugu inkriminaciju, kao teže kazneno djelo koje se može suditi kao sumarno ali i kao tzv. optuživo, zapriječena je kazna do pet godina zatvora.

Inkriminacija neovlaštenog preinačavanja sadržaja elektronskog računala podrazumijeva neovlašteno preinačavanje kompjuterskog materijala za koje se kao kazna može izreći zatvor do pet godina, može se suditi ili kao sumarni ili kao optuživi akt. Sve tri inkriminacije vrše se sa direktnim umišljajem koji međutim, ne mora biti usmjeren na određenu strojnu ili programsku podršku odnosno podatke određenog računala ali mora obuhvaćati svijest o protupravnosti tj. da počinitelj nema pravno valjane osnove za pristup računalu. [18]

Zakonodavstvo SR Njemačke

U SR Njemačkoj je 01. 08.1986. godine stupio na snagu tzv. Drugi zakon za sprječavanje privrednog kriminaliteta, [19] koji je kao nove inkriminacije u kaznenom zakonu SR Njemačke unio "kompjutersku špijunažu", "kompjutersku prijevaru", "krivotvorenje podataka od važnosti za dokazivanje", "preinačavanje ili brisanje podatka", "kompjutersku sabotažu".[20] Prilikom donošenja ovog zakona bilo je upozorenja da se u konstrukcijama inkriminacija zakon ne smije previše vezati za trenutačni stupanj tehničkog razvoja jer bi opisi bića kaznenih djela dobili samo privremeni karakter a praksu opteretili problemima pravilne interpretacije zakonske terminologije. [21]

---

[18] O tomu opširnije u M. Wasik: Crime and the Computer, Clarendon, Press., Oxford, 1991.

[19] Manfred Möhrenschlager: Der Regierungsentwart eines Zweiten Gesetzes zur Beleämpfung der Wirtschaftskriminalität, Wistra, 6/82, 1/83 i 2/83.

[20] Strafgezetzbuch: par. 202a Ausspähen von Daten; par. 263a Computerbetreng; par. 269 Fälschung Beweiserhcblicher Daten; par. 303a Datenveränderung; par. 303b Computersabotage. 32. Auflage, Beck-Texte in dtv 1998.

[21] Sieber, U.: Informationstechnologie und Strafrechtsreform zur Reichwcite des künftigen Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität, Carl Heymanns Verlag, Köln, et. al. 1985.
Sieber U.: Computerkriminalität und Strafrecht, Carl Heymanns, Verlag, Köln, et.. al. 1. Aufl. 1977, 2. Aufl. 1980.

Inkriminacija "kompjuterska sabotaža" par. 202a Kaznenog zakonika SR Njemačke, podrazumijeva slučaj kada se netko, posebnim uređajima priključi na komunikacijske linije koje povezuju sustave elektronskih računala i tako neovlašteno pribavio podatke. Oni se odnose ili samo na usmene konverzacije ili pak zaštićuju u uskom tehničkom smislu, telekomunikacijske uređaje kao uređaje za prijenos podataka, pod čiji se pojam onda ne može svrstati računalo kao uređaj za obradu podataka.[22] Inkriminacija "neovlašteno korištenje sustava elektronskog računala bez mijenjanja podataka i programa", danas u zakonodavstvu većine zemalja pokazuje dva oblika.

Neke su zemlje, u osnovnom obliku inkriminirale "*hacking*" (neovlašteni pristup podacima i programima) kao radnju koja se sastoji u neovlaštenom pristupanju podataka pohranjenih na elektronskom računalu (Velika Britanija, Francuska, Švedska, Danska) odnosno, kao u SAD, u pristupanju podacima određene kategorije na određenim računarskim sustavima. Kvalificirani oblik "*hackinga*" predstavlja slučaj neovlaštenog pristupa elektronskom računalu radi neke kriminalne svrhe.

Drugi oblik je sadržan u odredbi par. 202a Kaznenog zakonika SR Njemačke, uvedene 1986. godine. Ona kažnjava zatvorom do tri godine ili novčanom kaznom onoga tko za sebe ili drugoga neovlašteno pribavi podatke koji mu nisu namijenjeni i koji su posebno zaštićeni protiv neovlaštenog pristupa.

Kod ove inkriminacije, kaznenopravna zaštita se ograničava na interes raspolaganja podacima onoga tko je na to pravno ovlašten, pri čemu nisu važna vlasničkopravna pitanja koja se tiču medija na kome su podaci zabilježeni kao ni interes zaštite tajnosti određenih podataka. Ovlaštenikov interes na raspolaganje podacima, koji po njegovoj volji u času manipulacije počinitelju ne stoje na raspolaganju, nisu mu namijenjeni, treba štititi od manipulacija kojima se zaobilazi zaštitni sistem.

Njemački teoretičari smatraju da obilježje bića ovog kaznenog djela "posebno zaštićeni podaci" predstavlja nužnu manifestaciju ovlaštenikovog interesa na očuvanje tajnosti, koja

[22] O tomu opširnije u M. Wasik: Crime and the Computer, Clarendon, Press., Oxford, 1991.

legitimira ovu inkriminaciju.[23] Kao počinitelj ovoga kaznenog djela prema njemačkom kaznenom pravu može se pojaviti svaka osoba koja nema ovlaštenja na pristup podacima. Za objektivnu stranu kaznenog djela dovoljno je da je počinitelj sebi ili drugome pribavio podatke koji mu nisu namijenjeni.

Radnja "pribavljanja podataka" dovršena je onda kada se počinitelj upoznao sa njihovim sadržajem i ostvario faktičko pritežanje nositelja na kojem su registrirane (disketa i sl.) odnosno, pribavio algoritam čitanja kodiranih podataka. [24] Naime, kod određivanja kriminalne zone "*hackera*", koji neovlašteno pristupi nekom računarskom sustavu bez povezivanja njegovih datoteka sa podacima, ne potpada pod udar ovog propisa. Njemački teoretičari ističu da se djelo može pojaviti u idealnom stjecaju sa nekim drugim deliktima kao krađom (diska), odavanja tajne ili neovlaštenog korištenja autorsko pravno zaštićenog programa. [25]

Inkriminacija "neovlašteno korištenje usluga elektronskog računala" u najvećem broju suvremenih zakonodavstava nije određena kao kazneno djelo. Izuzetak čine pojedine države SAD-a i Kanada, kao inkriminacija "krađa usluga" određena po propisima američkog modela kaznenog zakonika. [26] Novela kanadskog Kaznenog zakona iz 1985. godine kažnjava svakoga tko protupravno ili prijevarno pribavi, neposredno ili posredno neku uslugu elektronskog računala.[27] Ova inkriminacija u zakonodavstvu nekih zemalja podvodi se pod kazneno djelo "neovlaštene posluge s automatom" (par. 149. st. 2. austrijskog KZ), "oduzimanje električne energije" (par. 132. austrijskog KZ).

Međutim, poseban slučaj manipulacije s računalom predstavlja neovlašteno korištenje neke programske podrške, što se npr. u SAD kažnjava kao krađa. Naime, u SAD-a došlo se do zakonskog proširenja definicije krađe na elektronske impulse,

---

[23] Lenckner, Th.: Computerkriminalität und Vermögensdelikte, C. F. Müller, Karlsruhe, 1981.
Stree W.: Kommentar par. 303a, 303b, 303c, Strafgesetzbuch, u Lenckner /Cramer/Eser/Stree (urednici), Strafgesetzbuch, Kommentar begründet von A. Schönne U. H. Schröder 23. Aufl. C. H. Beck, München, 1988.

[24] Isto.

[25] H. Schmitz/D. Schmitz, ComputerKriminalität , Forkel Verlag, Wiesbaden, 1990.

[26] Tanović R.: Osnove precedentnog prava Common Law, (poglavlje Kazneno pravo u SAD-u), Informator, Zagreb, 1998.

[27] M. Wasik: Crime and the Computer, Clarendon, Press., Oxford, 1991.- Section 301.2 of the Criminal Code.

elektronski obrađivane podatke i informacije, programsku podršku za računala u obliku čitljivim za stroj ili osobu, usluge računala te druge taktilne ili netaktilne vrijedne predmete koji se odnose na sustav računala ili njegovu mrežu te njihove kopije. [28]

Inkriminacija "neovlašteno korištenje usluga elektronskog računala" podrazumijeva nepostojanje ovlaštenja za korištenje računala i podsjeća na "*hacking*" ali se od njega razlikuje po tome što kod njih nema elemenata manipulacije sa fizičkom ili elektronskom zaštitom elektronskog računala te je usporediva sa krađom u njemačkom kaznenom zakoniku (par. 242-244a, 252-.*an Verwandten*, 247-*geringwertiger Sachen*, 248a-*von Leichen* 168), jer njezin počinitelj oduzima vlasniku računarskog sustava novčanu vrijednost vremenskog razdoblja u kojem je neovlašteno radio sa sustavom, koja se može još povećati ako je računalo bilo npr. u najmu, pa ga njegov najmoprimac kroz to razdoblje nije mogao koristiti a morao je platiti i najamninu.[29]

Inkriminacija "neovlašteno kopiranje i reprodukcija kompjuterskog programa" je u većini zemalja podvedena pod odredbe Zakona o autorskom pravu. Zemlje *common law* tradicije tu su zaštitu ustanovile u okviru svog zakonodavstva o copyrightu (u SAD, federalni *Computer Softwere Protection Act* iz 1980., u Velikoj Britaniji *Copyrights, Designs and Patent Act* iz 1988).[30] Naime, neovlašteno kopiranje i reprodukcija kompjuterskih programa, predstavlja manipulaciju s računalom koja je danas jedna od najraširenijih. Zakoni o autorskom pravu mogu zaštiti kompjuterske programe ukoliko se postigne suglasnost oko pitanja

---

[28] Isto, fus nota 28 i 29.

[29] Strafgesetzbuch, 32, Auflage, Beck-Texte im dtv., 1998.
Naime, svakodnevni su slučajevi da pojedinci neovlašteno iskorištavaju pristup računalu da na njemu obavljaju svoje privatne poslove različite vrste počev od igre sa kartama, šahom, razne igrice, a radi dosade tijekom radnog vremena, preko korištenja računala u pojedinim institucijama preko granice vremena dodijeljenog pojedinim pripadnicima tih institucija pa do pisanja čitavih kompjuterskih programa namijenjenih kasnije komercijalnoj upotrebi ili prodaji trećim osobama. Ovakve manipulacije slične su "*hackingu*" ali su usporedive sa krađom jer njezin počinitelj oduzima vlasniku računarskog sustava novčanu vrijednost vremenskog razdoblja u kojem je neovlašteno radio sa sustavom.

[30] Tanović R.: Osnove precedentnog prava Common Law, (poglavlje Kazneno pravo u SAD-u) Informator, Zagreb, 1998. M. Wasik: Crime and the Computer, Clarendon, Press., Oxford, 1991.-Section 301.2 of the Criminal Code.

predstavlja li takav program autorsko djelo te predstavlja li njegovo kopiranje radnju neovlaštenog umnožavanja i korištenja. [31]

U Njemačkoj su novelom Zakona o autorskom pravo iz 1985. godine, kompjuterski programi svrstani u "govorna djela"- *sprachwerke*, koja, ukoliko po stanovištima judikature i teorije, predstavljaju umnu tj. "duhovnu tvorevinu" zbog toga što analiza njihovog "duhovno-estetskog sadržaja" provedena kroz ispitivanje sistemskih kvaliteta programa, postavljanja njegovog semantičkog i sintaktičkog algoritma i prevođenja logičkih u mašinske naredbe te kodiranja, pokazuje da se kod njega ne radi o matematskom algoritmu, nego o tvorevini koja sadrži "stvaralački stupanj originalnosti", individualiteta i načina rješavanja problema s kojima je programer bio suočen. [32]

Time, svako njihovo korištenje bez izričite dozvole autora programa, odnosno nositelja autorskih prava na programu ostvareno u tehničkom smislu prilikom učitavanja nekog programa u centralnu procesorsku memoriju, predstavlja neovlašteno korištenje u smislu elemenata autorsko pravnih inkriminacija, naročito onda kada se programi neovlašteno kopiraju radi rasparčavanja u javnosti.

U Njemačkoj, nakon ovog noveliranja, iznova je pokrenuto noveliranje Zakona o autorskom pravu, u cilju ocjene "originalnosti" kompjuterskog programa kao autorskog djela. Po prijedlogu novih odredbi par. 69. Zakona o autorskom pravu, zaštićeni su kompjuterski programi "ako predstavljaju individualna djela u smislu da su rezultat vlastite duhovne kreacije svog autora" pri čemu se za tu ocjenu ne primjenjuju nikakvi drugi kao npr. estetski kriteriji.[33]

Kazneno djelo prijevara - *betrug*, par. 263 njemačkog kaznenog zakonika, [34] predviđa kao element bića kaznenog djela dovođenje u zabludu druge osobe, što se ne može realizirati na nekom stroju, osim ako uz njegovo funkcioniranje nisu povezani subjektivni psihološki procesi njegovog operatera. U pravilu, toga nema nego počinitelj sam svojim pretraživanjem podataka u elektronskom računalu eliminira subjektivni

---

[31] M. Wasik: Crime and the Computer, Clarendon, Press., Oxford, 1991.- Section 301.2 of the Criminal Code.

[32] H. Schmitz/D. Schmitz, Computerkriminalität , Forkel Verlag, Wiesbaden, 1990.

[33] Isto.

[34] Strafgesetzbuch, 32, Auflage, 1998. Beck-Texte im dtv.

element klasičnog bića kaznenog djela prijevare na strani oštećenog vlasnika sredstva. Elektronsko računalo koje je "prevareno" postupa u skladu s programiranim pravilima o transferu sredstava na koja je vlasnik sredstava, povjeravajući ih toj instituciji, bio pristao.

Njemačko zakonodavstvo je taj problem 1986. godine, riješilo novom inkriminacijom "kompjuterska prijevara" par. 263a *commputerbetrug*, [35] koja glasi: "par. 263a kompjuterska prijevara (1) Tko u namjeri da sebi ili drugom pribavi kakvu protupravnu imovinsku korist ošteti imovinu neke osobe utjecajem na rezultat jednog postupka obrade podataka i to nepravilnim programiranjem, primjenom nepravilnih podataka, neovlaštenom upotrebom podataka ili nekim drugim neovlaštenim utjecajem na njezin tok, kaznit će se lišenjem slobode do pet godina ili novčanom kaznom."

Njemački teoretičari kaznenog prava komentirajući kazneno djelo "kompjuterska prijevara" ističu da "nepravilno programiranje" znači takvu manipulaciju koja program mijenja na način koji ne odgovara volji i predstavi njegovog odvijanja na strani ovlaštene osobe. [36] Manipulacija "primjena nepravilnih podataka" znači unošenje u programsku obradu podataka koji netočno označavaju odnose i pojave u stvarnosti ili dovode do pogrešnog uvjerenja o potpunosti neke pojave ili odnosa. Manipulacija "neovlaštena upotreba podataka" je takva s kojom počinitelj neovlašteno pristupa sustavu elektronskog računala. Manipulacija "neovlašteno utjecanje na tok obrade podataka" odnosi se na sve manipulacije koje ne znače primjenu nepravilnih ili nepotpunih podataka nego manipulacije sa strojnom podrškom, čija se tehnika u zakonu ne može precizirati, što nadalje otvara pitanja primjene poznatog zahtjeva za jasnoćom i preciznošću zakonskih opisa kaznenog djela iz načela zakonitosti. Utjecanje na tok programa strojne obrade, postoji već onda kada ona odstupa od prethodno zamišljenog i utvrđenog rezultata. Utjecanje na postupak obrade podataka ujedno i isključuje primjenu ove inkriminacije na neke druge oblike manipulacija kao na neovlašteno korištenje usluga elektronskog računala jer kod neovlaštenog korištenja usluga nema promjena u programu ili podacima.

---

[35] Isto.

[36] H. Schmitz/D. Schmitz, Computerkriminalität , Forkel Verlag, Wiesbaden, 1990.

Inkriminacija "krivotvorenje podatka važnih za dokazivanje" određena je par. 269 njemačkog kaznenog zakonika, [37] koja glasi: "(1) Tko podatke važne za dokazivanje u pravnom prometu radi obmane tako pohrani ili preinači da bi oni, prilikom njihovog opažanja predstavljali lažnu ili krivotvorenu ispravu odnosno upotrijebi tako pohranjene ili preinačene podatke, kaznit će se lišenjem slobode do pet godina ili novčanom kaznom. (2) Kaznit će se i za pokušaj."

Inače, u zakonu SR Njemačke, isprava - *urkunden*, ima tri funkcije: dokaznu, garantivnu, perpetuirajuću. [38] Dokazna funkcija podrazumijeva ispravu koja je po sadržaju namijenjena ili podesna da bude dokaz u pravnom prometu. Garantivna funkcija podrazumijeva ispravu iz koje se vidi tko ju je izdao i to garantira njezinu vjerodostojnost. Perpetuirajuća funkcija podrazumijeva da isprava materijalizira misleni sadržaj neke izjave.

Inače, kod inkriminacije "krivotvorenje podataka važnih za dokazivanje", počinitelj djeluje s eventualnim umišljajem, pri čemu mora imati svijest o svim okolnostima tj. da se pohrana ili preinačenje podataka vrši kako bi se oni prilikom korištenja upotrijebili kao "prava isprava" tj. kako bi oni u pogledu njezine autentičnosti obmanuli nekog sudionika u pravnom prometu.

Odredbom par. 270 njemačkog kaznenog zakonika, "lažljivo utjecanje na obradu podataka" jednako je kao i "obmana u pravnom prometu"-par. 267, čime je zakonodavac želio "pokriti" slučajeve u kojima bi netko manipulirajući s elektronskim računalom, u njemu pohranio ili preinačio podatke bez posebne namjere da se oni učine dostupnima trećim osobama odnosno da se tako neka osoba dovede u zabludu oko njihove vjerodostojnosti.

Njemačko zakonodavstvo dopunilo je i neke odredbe o tzv. intelektualnim falsifikatima: par. 271-ovjeravanje neistinitog sadržaja, par. 272-upotreba neistinite službene isprave; par. 348-krivotvorenje službene isprave, i to tako što je u dispozicije tih propisa unio "podatke", njihovu "pohranu", te "datoteke" tj. pojmove iz automatske obrade podataka kao nove gramatičke objekte tih kaznenih djela. [39]

---

[37] Strafgesetzbuch, 32. Auflage, 1998. Beck-Texte im dtv., par. 269.

[38] Strafgesetzbuch, 32, Auflage, 1998. Beck-Texte im dtv., par 133, 267, 274, 348.

[39] O komentaru na ove inkriminacije u njemačkom kaznenom zakonodavstvu opširnije u: Möhrenschlager, M.: Der Regierungsentwurf eines Zweiten

Inkriminacija "izmjena podataka" par. 303a kao i "kompjuterska sabotaža" par. 303b, uvedene su u njemačko kazneno zakonodavstvo 1986. godine, [40] kao nove inkriminacije Drugim Zakonom o suzbijanju privrednog kriminaliteta.

Inkriminacija "izmjena podataka" par. 303a-*datenveränderung*, objekt zaštite je javni interes na neometanu i neškodljivu upotrebu podataka, dok je inkriminacija "kompjuterska sabotaža" par. 303b-*computersabotage*, interes privrednih subjekata i javnih vlasti na neometano funkcioniranje njihovih sustava automatske obrade podataka.

Inkriminacija "izmjena podataka" glasi: "(1) Tko protupravno podatke (par. 202.a 2), izbriše, ukloni, učini neupotrebljivim ili izmjeni, kaznit će se lišenjem slobode do dvije godine ili novčanom kaznom. (2) Kažnjiv je i pokušaj." Gonjenje se poduzima po prijedlogu, par. 303c.

Inkriminacija "kompjuterska sabotaža", glasi: "Tko neku obradu podataka koja je od bitne važnosti za jedan tuđi pogon, tuđe poduzeće ili državni organ omete time da izvrši djelo iz par. 303. 1. ili 2., uništi, ošteti, ukloni, izmjeni ili učini neupotrebljivim neki uređaj za obradu podataka ili neki nosioc podataka, kaznit će se lišenjem slobode do pet godina ili novčanom kaznom. (2) Kažnjiv je i pokušaj." Gonjenje se poduzima po prijedlogu, par. 303c.

Kao počinitelj inkriminacije "izmjena podataka" može se pojaviti svaka osoba koja neovlašteno manipulira sa podacima, da se sa iscrpnim opisom modaliteta radnje izvršenja djela pokriva široko područje manipulacija bez da se pri tome, nomotehnički propis i suviše veže na tehničke termine koji podliježu promjenama te da se u subjektivnom pogledu traži umišljaj ali i svijest da se radi o podacima koji su "tuđi", koji se ne odnose na počinitelja i njegove interese. Tako "brisanje" podataka znači njihov nepovratni gubitak u cijelosti i "uklanjanje" ili čini nedostupnim određenom krugu korisnika, dok "činjenje neupotrebljivim" znači onemogućavanje upotrebe prema njihovoj namjeri, "mijenjanje" znači remećenje

---

Gesetzes zur Bekämpfung der Wirtschaftskriminalität, Wistra, 6/82, 1/83, 2/83.
Möhrenschlager, M.: Das Zweite Gesetzes zur Bekämpfung der Wirtschaftskriminalität, (2.WIKG), Wistra, 4/86.

[40] Strafgesetzbuch, 32, Auflage, 1998. Beck-Texte im dtv., par. 303a, 303b.

njihovog informacijskog sadržaja. Posljedica radnje inkriminacije je da je došlo do promjene podataka.

Inkriminacija "kompjuterska sabotaža" uvedena je kao prvi delikt tzv. pogonske ili privredne sabotaže sa povećanim kaznenim okvirima u usporedbi sa inkriminacijom "izmjena podataka". Kao počinitelj ove inkriminacije može se pojaviti osoba koja pripada krugu namještenika nekog poduzeća ili službenika javnog organa kao i osoba koja ne pripada tome krugu, dok se element "obrada podataka", tumači u najširem smislu kao unos podataka, obrada, pohrana. Element "bitna važnost" te obrade za djelatnost nekog subjekta, treba shvatiti kao njegova egzistencijalna pretpostavka te da je zakonodavac predvidio dvije varijante radnje i to mijenjanje podataka i napad na sam uređaj za automatsku obradu podataka i njihove materijalne nosioce.

Posljedica radnje ove inkriminacije je u "ometanju" automatske obrade podataka tj. u takvom djelovanju ali ne i ugrožavanju na njezin tok koje se ne može otkloniti bez većih napora te utroška vremena i sredstava.

U subjektivnom pogledu djelo se može izvršiti s umišljajem a potrebna je i svijest o okolnosti da svojim napadom na obradu podataka, koja je od bitne važnosti za djelovanje nekog poduzeća ili državnog organa. [41]

Zakonodavstvo Republike Austrije

U Republici Austriji je donesen 25. 11. 1987.godine Zakon o izmjeni kaznenog zakonika - *das Strafrechtsänderungesetz* koji je stupio na snagu 01. 03. 1988.godine. Nacrt zakona bio je prvobitno predvidio više novih inkriminacija ali su ozakonjene samo dvije "oštećenja podataka" - par. 126a KZ, i "prijevarna zloupotreba obrade podataka" - par. 148a KZ. [42]

---

[41] Komentari inkriminacija, izmjena podataka i kompjuterska sabotaža, opširnije u H. Schmitz/D. Schmitz, Computerkriminalität , Forkel Verlag, Wiesbaden, 1990.

[42] Strafrechtsänderungesetz EDV & Recht, 1988. O austrijskom zakonodavstvu u ovoj oblasti, opširnije u: Bericht des Justizausschusses über den Antrag der Abgeordneten Dr. Ofner und Genossen betreffend ein Strafrechtsänderungesetz 1987., Sonderdruck 359 der Beilagen zu den Stenographischen Protokollen des Nationalrates XVII, GP, 1988.

Međutim, u raspravi oko izmjene kaznenog zakonodavstva u Republici Austriji, nalazile su se još dvije inkriminacije: "neovlašteno pribavljanje pohranjenih podataka" i "neovlašteno preinačavanje ili brisanje podataka" (koje nije rezultiralo imovinskom štetom), a koje nisu prihvaćene. Inkriminacija "oštećenja podataka" - *Datenbeschödigung*, par. 126a KZ, glasi: "Tko drugoga ošteti na način da podatke koji se obrađuju ili prenose uz automatsku podršku i s kojima nije ovlašten samostalno ili bez drugih osoba raspolagati, mijenja, briše ili na drugi način učini neupotrebljivim ili nedostupnim, kaznit će se kaznom zatvora do šest mjeseci ili novčanom kaznom do 360 dnevnih globa".

Spomenuta inkriminacija razlikuje se od njemačke "kompjuterska sabotaža"- par. 303b KZ (prethodno definirana i komentirana), time što je u spomenutoj inkriminaciji austrijskog kaznenog zakonika zauzeto jedno kriminalno političko stanovište po kojem objekt kaznenopravne zaštite treba ostati samo sigurnost i integritet podataka u automatskoj obradi dok se konstrukcija inkriminacije usko oslanja na delikt oštećenja tuđe stvari u opisu radnje u kaznenom okviru (par. 125 "oštećenja stvari" austrijskog KZ glasi: "Tko neku tuđu stvar uništi, ošteti, poremeti sastavne dijelove ili učini neupotrebljivom, kaznit će se lišenjem slobode do šest mjeseci ili novčanom kaznom do 360 dnevnih globa".) i kao posljedicu ustanovljava neposrednu štetu sa podacima. Time se razlikuje od njemačkog zakonodavstva koji u par. 303a Njemačkog KZ uopće ne spominje pojam oštećenja, pretpostavljajući da je već sadržan u opisanim modalitetima radnje izvršenja djela. Od delikta "oštećenja tuđe stvari" - par. 124 KZ, razlikuje se nova inkriminacija u austrijskom KZ po zaštitnom objektu (podaci osobnog i neosobnog karaktera te programi, par. 126a. st. 2.) te modalitetima radnje dok joj subjektivna strana ostaje ista.

Inkriminacija "prijevarna zloupotreba obrade podataka" - par. 148a KZ glasi: "Tko u namjeri da sebi ili drugome pribavi protupravnu imovinsku korist, nekoga u imovini ošteti utjecanjem na rezultat neke obrade podataka s automatskom podrškom i to programiranjem, unošenjem, izmjenama ili brisanjem podataka (par. 126a. st. 2. KZ) ili nekim drugim utjecanjem na tok postupka obrade podataka, kaznit će se zatvorom do šest mjeseci ili novčanom kaznom do 360 dnevnih globa. (2) Ukoliko je djelo vršeno obrtimice ili pričinjena šteta prelazi iznos od 250.000 šilinga, počinitelj će se kazniti lišenjem

slobode do tri godine, a ako je iznos štete veći od 50.000 šilinga, lišenjem slobode do deset godina."

Uspoređujući ovo kazneno djelo sa kaznenim djelom "kompjuterska prijevara"- par. 263a. njemačkog KZ (prethodno definirano i komentirano) nalazi se da je suština ove inkriminacije u njemačkom kaznenom zakoniku u naznaci kako utjecanje na tok obrade podataka, predstavlja ostvarenje počiniteljeve namjere da neovlaštenim uplitanjem u automatsku obradu podataka pribavi sebi ili drugom protupravnu imovinsku korist.

U zakonodavstvu Republike Austrije, "Zakon o zaštiti osobnih podataka" iz 1978. godine [43] sadrži dvije inkriminacije: "narušavanje tajnosti podataka", *Gehemnisbruch* - par. 48 i "neovlašteni zahvati u prometu podacima", *Unbefugte Eingiffe im Datenverkehr* - par. 49.

Inkriminacija "narušavanje tajnosti podataka" - par. 48 glasi: "Tko protupravno objavi ili upotrijebi podatke koji su mu povjereni ili do kojih je došao na temelju profesionalnog bavljenja obradom podataka i čije bi objavljivanje ili upotreba mogla povrijediti neki opravdani interes osobe na koji se odnose, kaznit će se zatvorom do jedne godine dana (ukoliko se za djelo po nekom drugom propisu ne može izreći stroža kazna)."

Inkriminacija "neovlašteni zahvati u prometu podacima" - par. 49 glasi. "Tko drugome u njegovim pravima namjerno pričini štetu time što sebi protupravno pribavi podatke iz automatske obrade, kaznit će se zatvorom do jedne godine dana." [44]

Summary

At the end of his short report about a very complex problem of computer delinquency, we cam point aut that the penal law wich does not have the legislative regulations concerning the computer

[43] Das neue Computer-Strafrecht, EDV & Recht, 1988., Datenschutzgesetz, BGB, 1978., Bundesgesetz vom 18. 10. 1978., BGB, 1978.

[44] Kienapfel, D.: Grundriss des Österreichischen Starfrechts, BTII, 2. Aufl., Delikte gegen Vermögenswerte, Manz, Wien, 1988. Foregger, E. / Serini, E. / Kodek, G.: Die Österreichischen Strafprozessordnung, Kurzkommentar, 4. Aufl. Manz, Wien, 1989.
O austrijskom kaznenom zakonodavstvu vidjeti u Strafsrchtliche Probleme der Gegenweart B cl. 25 1998., Bundesministerium Für Justiz, Wien, Fernmeldegestz 1997. Telekomunikationsgestez BG bl. Nº 100, 1997.

criminal acts, better say, concerning the criminal acts in connection with the illegal use of computers, internet, and in our legislature, it would be advisable to follow the practice of the criminal jurisdiction of the Socialist Republic of Germany and Austria, and to try to combine the German and the Austrian approach in construction of the new incriminations, for the reason that, in the above mentioned legislations, the protective objects of incrimination are completely denoted; the individual and social interests are determined with a high level of legislative accuracy in the definition of incrimination. The mentioned legislatures have completely penalized occurrence of the abuses by means of he application of computers.

KORIŠTENA LITERATURA

A.Bequai, How to Prevent Computer Crime - A. Guide for Managers, J. Wiley and Sons, Chiecester, 1983.
Bericht des Justizausschusses über den Antrag der Abgeordneten dr. Ofner und Genossen betreffend ein Strafrechtsänderungesetz 1987., Sonderdruck 359 der Beilagen zu den Stenographischen Protokollen des Nationalrates XVII, GP, 1987.
Bundesgesetz von 18. 10. 1978., BGB, 1978.
Computer-Related Crime: Analisis of Legal Policy in the OECD Area, Paris, 1984., DSTI/ICCP.
"Computer crime", Bureau of Justice Statistics, US Department of Justice, Washington, 1979.
Donn B. Parker/Susan Nykum/s. Stephen Oura, Computer Abuse Stanford Research Institute, Menlo Park, 1973.
Dokumenti UN-Rezolucija UN 45/121, UN Manual on Computer - Relad Crime, 1990.
Das neue Computer-Strafrecht, EDV & Recht, 1988.
Foregger, E. / Serini, E. / Kodek, G.: Die Österreichischen Strafprozessordnung, Kurzkommentar, 4. Aufl. Manz, Wien, 1989.
G. Schmölzer: Strafsrchtliche Probleme der Gegenwart B. cl. 25, 1998.
H. Gliss, Computerkriminalität-Erscheinungs sformen, Bedrohungspotentiäl und Wachstumstrends, 1985.
H. Schmitz/D. Schmitz, ComputerKriminalität , Forkel Verlag, Wiesbaden, 1990.
H. Sonoda, Das Neue Computerstrafrecht in Japan, Wistra, 1988.

Izvještaj Europskog komiteta za probleme kriminaliteta Computer-related crime" R (89)9 Council of Europe, Strasbourg, 1990.
J. Soyka: Computer Kriminalität, Fälle und Fakten, W.Heyne, München, 1986.
J. C. Lin: Computer Crime, Security and Privacy: Aselected, Bibliography, Monticello, 1979.
Jaburek, W. - Schmölzer, G.: Computer - Kriminalität, A. Orae, Wien, 1985.
Kienapfel, D.: Grundriss des Österreichischen Starfrechts, BTII, 2. Aufl., Delikte gegen Vermögenswerte, Manz, Wien, 1988.
Lenckner, Th.: Computerkriminalität und Vermögensdelikte, C. F. Müller, Karlsruhe, 1981.
M. Wasik: Crime and the Computer, Clarendon, Press., Oxford, 1991.-Section 301.2 of the Criminal Code.
Möhrenschlager, M.: Der Regierungsentwurf eines Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität, Wistra, 6/82, 1/83, 2/83.
Möhrenschlager, M.: Das Zweite Gesetzes zur Bekämpfung der Wirtschaftskriminalität, (2.WIKG), Wistra, 4/86.
M. Möhrenschlager: Der Regierungsentwart eines Zweiten Gesetzes zur Beleämpfung der Wirtschaftskriminalität, Wistra, 6/82, 1/83 i 2/83.
Strafgezetzbuch, 32. Auflage, Beck-Texte in dtv 1998.
R. T. Nimmer: The Law of Computer Technology, New York, J. Wiley, 1985.
R. von zur Mühlena: Computer-Kriminalität. Gefahren und Abwehrmassnahmen, Neuwied und Berlin, 1979.
R. A. H. von zur Mühlen, Computer-Kriminalität, 1972., Magazin "Chip", (SR Njemačka), br. 3. 1992.
S. Nora / A. Minc: Die Informatisierung der Gesellschaft, Frankfurt/M - New York 1979.
Sieber, U.: Informationstechnologie und Strafrechtsreform zur Reichwcite des künftigen Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität, Carl Heymanns Verlag, Köln, et. al. 1985.
Sieber, U: Informationsrecht und Recht der Informationstechnik, Neue juristische Wochenschrift 41, 1989.Tanović R., "Potreba krivičnopravne regulative, kompjuterski kriminalitet i neophodnost koncipiranja krivičnog djela kompjuterske zloupotrebe", Pravna misao 1-4/96, Sarajevo, 1996.
Tanović R.: Osnove precedentnog prava Common Law, DD "Informator", Zagreb, 1998.

U. S. Code, Tit. 18, pogl. 30 i 47. , U. S. Code, Tit. 18, Ch. 47, par. 1029, 5 U. S. Code par. 552a, 12 U. S. Code par. 3401-3422, 5 U. S. Code par. 552a, M. Wasik: Crime and the Computer, Clarendon, Press., Oxford, 1991.
V. Ferišaka: Osnove informatike , Informator, Zagreb,1985.
Wasik, M.: Crime and the Computer, Clarendon, Press, Oxford, 1991.
Zimmerli, E./Liebl, K.: Computermissbrauch, Computersicherheit: Fälle - Abwehr - Aufdeckung, Peter Hohl, Ingelheim, 1984.,
Ž. Horvatić: Novo hrvatsko kazneno pravo, Organizator, Zagreb, 1997.