KRIVIČNOPRAVNA ZAŠTITA BEZBEDNOSTI RAČUNARSKIH PODATAKA

prof.dr Dragan Jovašević
Pravni fakultet u Nišu

Tarik Hašimbegović
Poreska uprava Republike Srbije
Beograd

Uvod

Usvajanjem novog krivičnog zakonodavstva 2003. godine u Državnoj zajednici Srbija i Crna Gora po prvi put su u sistem krivičnog prava uvedana posebna računarska ili kompjuterska krivična dela koja su imala za cilj da obezbede efikasnu, kvalitetnu i potpunu zaštitu bezbednosti računarskih podataka odnosno računarskog sistema.

Tako je Zakon o izmenama i dopunama Krivičnog zakona Republike Srbije (KZ RS)[1] iz aprila 2003. godine odnosno Krivični zakonik Republike Crne Gore (KZ RCG)[2] iz decembra 2003. godine u sistem krivičnog prava naše zemlje uvedeno je više računarskih (kompjuterskih) krivičnih dela[3] i to, u glavi 16a. KZ RS odnosno glavi 28. KZ RCG predvidjena su krivična dela protiv bezbednosti računarskih podataka. Na taj način se i naša zemlja pridružila nizu zemalja koje se na različite načine (preventivnim i represivnim merama) pokušavaju suprotstaviti različitim oblicima i vidovima zloupotrebe kompjutera odnosno računara. S obzirom da se radi o novim inkriminacijama koje pobudjuju pažnju ne samo stručne već i opšte javnosti u našem pravnom sistemu u nastavku ćemo ukazati na osnovne fenomenološke i krivično pravne karakteristike računarskih krivičnih dela[4] .

Pojam kompjuterskog (računarskog) kriminaliteta

Iako je u svetu uobičajeno da se krivična dela protiv bezbednosti podataka u savremenim informatičkim sistemima nazivaju kompjuterska krivična dela (kompjuterski kriminalitet) naš je zakondavac za ova dela upotrebio termin računarski kriminalitete. Inače radi se o dva sinonimna pojma pa ćemo ukazati na osnovne teorijske definicije pojma kompjuterskog kriminaliteta. Kompjuter (računar) u svakom slučaju predstavlja jednu od najznačajnijih i najrevolucionarnijih tekovina razvoja tehničko – tehnološke civilizacije. No, pored svih prednosti koje sobom nosi i ogromne koristi čovečanstvu kompjuter je brzo postao i sredstvo zloupotrebe nesvesnih pojedinaca, grupa čak i organizacija.Tako nastaje kompjuterski kriminalitet kao poseban i specifičan oblik savremenog kriminaliteta po strukturi, obimu i osobenostima. Sve to zaslužuje pažnju države i njenih organa pa i cele medjunarodne zajednice.

Zahvaljujući ogromnoj moći komopjutera u memorisanju i brzoj obradi velikog broja podataka, automatizovani informacioni sistemi postaju sve brojniji i gotovo nezamenjivi

[1] Službeni glasnik Republike Srbije broj 39/2003
[2] Službeni list Republike Crne Gore broj 70/2003
[3] Dragan Jovašević, Komentar Krivičnog zakona Republike Srbije, Nomos, Beograd, 2003. godine, str.257
[4] Dragan Jovašević, Leksikon krivičnog prava, Službeni list SRJ, Beograd, 2002.godine, str.689

deo celokupnog društvenog života svih subjekata (fizičkih,ali i pravnih lica) na svim nivoima. Tako kompjuter postaje svakodnevni i nezaobilazni deo, segment svih sfera društvenog života od proizvodnje, prometa, vršenja usluga pa do nacionalne odbrane i bezbednosti u najširem smislu. No, sve ove raznolike forme neposredne primene kompjutera u svim oblastima života nisu ostale nezapažene od strane nesavesnih i neodgovornih pojeidnaca i grupa koji ne birajući sredstva i način protivpravnim ponašanjem pokušavaju da sebi ili drugom pribave protivpravnu imovinsku korist.

Tako kompjuter postaje sredstvo vršenja različitih oblika nedozvoljenih, protivpravnih i društveno opasih delatnosti. Naravno, kompjuterski kriminalitet pod čijim zbirnim nazivom su obuhaćeni svi ovi raznoliki oblici i forme ponašanja vezani za zloupotrebu kompjutera i informacionih sistema uopšte iako štetna i opasna negativna društvena pojava modernog doba nema opšte usvojenu definiciju. Tako se u krivičnopravnoj literaturi za ove raznolike oblike kompjuterskog kriminaliteta upotrebljavaju različiti termini kao što su :

1. zloupotreba kompjutera (computer abuse),
2. kompjuterska prevara (computer fraud),
3) delikti uz pomoć kompjutera (crime by computer),
4) informatički kriminalitet,
5) računarski kriminalitetr i
6) tehno kriminalitet. [5]

Ovaj vid kriminaliteta za razliku od drugih ne predstavlja još uvek zaokruženu fenomenološku kategoriju te ga je nemoguće definisati jednistvenim i precizno pojmovnim odredjenjem. Kompjuterski kriminalitet je samo opšta forma kroz koju se ispoljavaju različiti oblici kriminalne delatnosti. Naime, to je kriminalitet koji je upravljen protiv bezbednosti informacionih (kompjuterskih, računarskih) sistema u celini ili u njenom pojedinim delu na različite načine i različitim sredstvima u nameri da se sebi ili drugom pribavi kakva korist ili da se drugome nanese kakva šteta .

No, u teoriji krivičnog prava se mogu naći različita pojamna odredjenja kompjuterskog kriminaliteta. Tako Don Parker odredjuje kompjuterski kriminalitet kao zloupotrebu kompjutera u smislu svakog dogadjaja koji je u vezi sa upotrebom kompjuterske tehnologije u kome žrtva trpi ili bi mogla da trpi gubitak,a učinilac deluje u nameri da sebi pribavi ili bi mogao da pribavi korist[6] . August Bequaia definiše kompjuterski kriminalitet kao vršenje krivičnih dela kod kojih se računar pojavljuje kao orudje ili objekt zaštite odnosno kao upotreba kompjutera pri vršenju prevare,utaje ili zloupotrebe čiji je cilj prisvajanje novca ili usluge ili vršenje političke ili poslovne manipulacuije uključujući i radnje uperene protiv samog računara[7] .

Bogo Brvar daje sledeću definiciju kompjuterskog kriminaliteta. To su krivična dela kod kojih se kompjuter pojavljuje kao sredstvo (orudje), predmet ili objekt napada za čije je vršenje ili pokušaj neophodno izvesno znanje iz računarstva ili informatike[8] . Konačno Djordje Ignjatović pod kompjuterskim kriminalitetom pak smatra poseban vid inkriminisanih ponašanja kod kojih se računarski sistem (shvaćen kao jedinstvo hardvera i

[5] Vidi : Slobodan Petrović, Kompjuterski kriminal, MUP Srbije, Beograd, 2002. godine
[6] Don Parker, Computer abuse, Springfield, 1973. godine, str.70
[7] August Bequai, Computer crime,Lexington,1978.godine,str.4
[8] Bogo Brvar, Pojavne oblike zlorabe računika, Revija za kriminalistiko in kriminologijo,Ljubljana,broj 2/1982. godine,str.29

softvera) pojavljuje ili kao sredstvo izvršenja ili kao objekt krivičnog dela ukoliko se delo na drugi način ili prema drugom objektu uopšte ne bi moglo izvršiti ili bi ono imalo drugačije karakteristike[9] .

Iz navedenih definicija nesumnjivo se mogu izvući osnovne karakteristike ili obeležja pojma kompjuterskog kriminaliteta .To su sledeća obeležja :

- društveno opasna, protivpravna ponašanja za koja zakon propisuje krivične sankcije,
- specifičan način i sredstvo vršenja krivičnih dela – uz pomoć ili posredstvom kompjutera,
- poseban objekt zaštite – bezbednost računarskih podataka ili informacionog sistema u celini ili pojediniog segmenta (dela),
- namera učinioca da sebi ili drugom na ovaj način pribavi kakvu korist (imovinsku ili neimovinsku) ili da drugome nanese kakvu štetu.

U teoriji krivičnog prava se u oblast kompjuterskog kriminaliteta svrstavaju različiti oblici protivpravnog, nedozvoljenog ponašanja kao što su :

1. kompjuterska prevara,
2. finansijske kradje, prevare i zloupotrebe,
3. kradja dobara,
4. falsifikovanje podataka i dokumenata,
5. vandalizam,
6. sabotaža,
7. hakerisanje,
8. kompjuterska špijunaža i
9. kradja vremena.

Velike praktične mogućnosti koje pruža savremena visoko sofisticirana kompjuterska i informatička tehnologija sa sobom nose i opasnosti od širenja i masovne upotrebe elektronskog prisluškivanja, kradje poslovnih i drugih tajni kao i različitih oblika intelektualne svojine, zatim ozbiljnog narušavanja privatnosti i drugih ljudskih sloboda i prava kao i ličnog integriteta a u poslednje vereme prisutna je i realna opasnost od talasa terorističkih akata raznih vsta (tzv. tehno ili sajber terorizam). Jedna novija američka studija iz ove oblasti ukazuje na činjenicu da se informatički kriminalitet dešava čak 40 puta češće od klasičnog, opšteg, tradicionalnog kriminaliteta, a da 90 % informatičkih zločina ostaje praktično neotkriveno (dakle u zoni tamne brojke kriminaliteta). Ova vrsta kriminaliteta se razvija takvom brzinom da praktično nema presedana u praksi .

Karakteristike kompjuterskog (računarskog) kriminaliteta

Kompjuterski (računarski) kriminalitet se pre svega karakteriše velikom dinamikom i izuzetnim bogatstvom svojih pojamnih formi i vidova ispoljavanja. To je i razumljivo jer se radi o novoj tehnologiji sa velikom mogućnosti i primenom u skoro svim oblastim društvenog,privrednog pa i ličnog života te su i mogućnosti za zloupotrebu kompjutera svakim danom sve veće. Pored novih pojavnih oblika ranije već poznatog kriminaliteta

[9] Djordje Ignjatović,Pojmovno odredjivanje kompjuterskog kriminaliteta, Anali Pravnog fakulteta u Beogradu,Beograd,broj 1-3/1991.godine,str.142

koje pod uticajem kompjutera menja svoj tradicionalni način i modus ispoljavanja,sada se javljaju i novi, znatno opasnijij oblici kriminalnog ponašanja koji do sada nisu bili poznati u kriminalističkoj praksi , a koji ne poznaju granice izmedju država pa i izmedju kontinenata.

Štetne posledice kompjuterskog kriminaliteta su izuzetno velike. One se mogu ispoljti i u nastupanju imovinske štete za pravno ili fizičko lice (ponekad i za celu državu), u gubitku poslovnog ugleda, gubitku poverenja u sigurnost i istinitost kompjuterskog poslovanja i uopšte kompjuterskih informacija,opasnosti od zloupotrebe po slobode i prava čoveka uopšte na razne načine i u raznim oblicima. I sami učinioci krivičnih dela u vezi sa zloupotrebom kompjutera predstavljaju posebnu često specifičnu kategoriju ljudi. Ovde se najčešće radi o nedelikventnim, nenasilnim, socijalno prilagodljivim pojedincima.

To su po pravilu lica koja ipak moraju da poseduju posebna stručna i praktična znanja i veštine u domenu visoke informatičke, računarske i kompjuterske tehnologije i kojima su ovakva tehnološka sredstva dostupna. Ova se krivična dela vrše prikriveno, često bez neke vidljive i bliske prostorne povezanosti učinioca dela i žrtve (oštećenog). Najčešće se teško otkrivaju a još teže dokazuju, a dugo vremena ostaju praktično neotkriveni sve dok oštećeni ne pretrpi neku štetu koja je vidljiva u sistemu računarskih informacija. To je kriminalitet koji brzo menja forme i oblike ispoljavanja,granice medju državama kao i vrstu oštećenog.

Tako je Interpol još 1980. godine konstatovao sledeće : "Danas u savremenom svetu postoji još jedan veliki usavršeni front koji je prisutan u svetskim razmerama.Veliki kriminalitet, organizacije kriminalaca sve više se orijentišu na akcije pljački u kojima je objekt kompjuter. Elektronika se zloupotrebljava. Ne beleži se pad klasičnih pljački ali se iz godine u godinu povećava nova vrsta kriminaliteta u kome se elektronika koristi kao sredstvo da se kriminalci domognu milionskih svota novca[10] .

Savremena informaciona i kompjuterska tehnologija unela je nove i drastične promene u sve sfere društvenog života. Te promene su pored pozitivnih i korisnih novina donele i niz problema vezanih za pojavu i širenje kompjuterskog kriminaliteta različitih oblika, formi i vidova ispoljavanja. Sve te promene se mogu svesti na sledeće :

- nove forme vrednosti,
- koncentracija podataka,
- novi ambijent delovanja,
- nove metode i tehnike delovanja,
- sužavanje vremenske skale delovanja,
- širenje geografskog prostora delovanja,
- pokretljivost,
- stabilnost rizika[11] .

Kompjuterski kriminalitet u uporednom krivičnom pravu

Budući da preventivne mere (opšteg i specijalnog karaktera) često nisu dovoljne niti jedine mere kojima se društvo suprostavlja naraslim i nabujalim oblicima i vidovima zloupotrebe komjutera u razlicite svrhe to je logično da sva savremena krivična

[10] Nikola Kitarović, Kompjuterski kriminal,Bilten Vrhovnog suda Srbije,Beograd,broj 2-3/1998.godine,str. 52-53

[11] Slobodan Petrović,op.cit.str.17

zakonodavstva u sistemu inkriminacija poznaju jedno ili više kompjuterskih (računarskih ili informatičkih ili tehno) krivičnih dela za koja su propisane različite vrste i mere krivičnih sankcija.

Tako iako Nemački krivični zakonik[12] ne poznaje kompjuterska krivična dela to ne znaci da ova protivpravna, nedopuštena ponašanja nisu inkriminisana. Naime, u Nemačkoj je 1986.godine donet poseban Krivični zakon za suzbijanje privrednog kriminaliteta koji predvidja niz kompjuterskih krivičih dela i to : kompjutersku špijunažu u čl. 202a., kompjutersku prevaru u čl.263a., falsifikovanje podataka u čl. 269., obmanu u pravnom prometu pri obradi podataka u čl. 270., promenu podataka u cl. 302a. i kompjutersku sabotaža u čl. 303a.

Krivični zakonik Austrije[13] predvidja kompjutersko krivično delo u čl. 126a. pod nazivom oštećenje podataka.

U Velikoj Britaniji je 1990. godine donet poseban Zakonik o zloupotrebi kompjutera. Ovaj zakonik predvidja niz krivičnih dela vezanih za zloupotrebu kompjutera i drugih informacionih sistema za koja se propisane veoma stroge kazne[14] .

I Krivični zakonik Makedonije[15] poznaje u čl. 251. kompjutersko krivično delo pod nazivom " Upad u kompjuterski sistem".

Na sličan način postupa i Krivični zakonik Republike Srpske[16] koji poznaje identično krivično delo pod nazivom : Upad u kompjuterski sistem u čl.260.

Krivični zakonik Republike Slovenije[17] poznaje sledeća krivična dela i to : Protivzakoniti ulaz u zaštićenu računarsku bazu podataka u čl. 225 i Upad u računarski sistem u čl.242.

Krivični zakon Republike Hrvatske[18] u čl.223. poznaje krivično delo pod nazivom : Oštečenje i upotreba tudjih podataka (koje se odnosi na automatski obradjene podatke ili računarske programe).

I konačno Krivični zakonik Ruske federacije[19] poznaje više kompjuterskih krivičnih dela u posebnoj glavi 23. koja nosi naziv: Krivična dela u sferi kompjuterske informacije. Ovde su propisana sledeća krivična dela : Protivpravni pristup kompjuterskoj informaciji u čl.272., Pravljenje,korišćenje i širenje štetnih računarskih programa u čl.273. i Povreda propisa o eksploataciji računara, računarskih sistema ili njihovih mreža u čl.274.

Računarska (kompjuterska) krivična dela u Krivičnom zakonu Srbije

[12] Vidi : Schonke-Schroder, Strafgesetzubuch ,Kommentar,Munchen,1978. godine
[13] Vidi : E.Foregger- E.Serini, Strafgesetzbuch, Wien,1989.godine
[14] Martin Wasik,The Computer misuse act, The Criminal review,1990.godine,str. 767
[15] Služben vesnik na Republika Makedonija, Skoplje,broj 37/1996.godine
[16] Službeni glasnik Republike Srpske,Banja Luka,broj 22/2000.godine ; Više :Miloš Babić,Komentar Krivičnog zakonika Republike Srpske,Banja Luka,2002.godine
[17] Vidi : Boštajn Penko-Klaudije Strolig,Kazenski zakonik Republike Slovenije,Ljubljana,1999.godine
[18] Narodne novine Republike Hrvatske,Zagreb,broj 110/1996.godine
[19] Vidi : J.I.Skuratov- V.M.Lebedov,Kommentarii k Ugolovnomu kodeksu Rossijskoj federaciji, Norma, Moskva, 1996.godine

I naš pravni sistem, posle novele Krivičnog zakona Republike Srbije iz aprila 2003.godine poznaje više krivičnih dela vezanih za zloupotrebu kompjutera (računara). Ova su krivična dela predvidjena u posebnoj Glavi 16a. koja nosi naslov:" Krivična dela protiv bezbednosti računarskih podataka". U ovoj glavi je predvidjeno sedam krivičih dela koja imaju zajednički objekt zaštite – bezbednost računarskih podataka odnosno informacionih sistema u celini i poverenja u istinitost ovih podataka. To su sledeća krivična dela :

1. neovlašćeno korišćenje računara i računarske mreže u čl. 186a. ,
2. računarska sabotaža u čl. 186b.,
3. pravljenje i unošenje računarskih virusa u čl. 186v.,
4. računarska prevara u cl. 186g.,
5. ometanje funkcionisanja elektronske obrade i prenosa podataka i računarske mreže u čl. 186d.,
6. neovlašćeni pristup zaštićenom računaru ili računarskoj mreži u čl. 186dj.,
7. sprečavanje i ograničavanje pristupa javnoj računarskoj mreži u čl. 186e20 .

Prvo krivično delo ove vrste u našem pravu jeste : **Neovlašćeno korišćenje računara i računarske mreže** iz čl.186a. Delo ima osnovni i dva teža oblika. Osnovno delo se sastoji u oštećenju, prikrivanju, neovlašćenom brisaju, izmeni ili na drugi način činjenju neupotrebljivim računarskih podataka ili programa. Delo se dakle može učiniti samo u odnosu na računarski podatak ili program koji pripada nekom fizičkom licu – pojedincu (kao napadni objekt) i to sa više alternativno predvidjenih delatnosti. Cilj preduzimanja ovih delatnosti je onesposobljenje za korišćenje u potpunosti ili delimično računarskih podataka (jednog ili više njih) ili programa. Posledica se dakle sastoji u povredi zaštićenog dobra. Delo može učiniti svako lice a u pogledu vinosti potreban je umišljaj. Za ovo je delo propisana novčana kazna ili zatvor do tri meseca.

Prvi teži oblik ovog krivičnog dela postoji ako je preduzetom radnjom prouzrokovana šteta za neko lice u iznosu preko 100.000 dinara. Visina prouzrokovane štete je kvalifikatorna okolnost za koju zakon propisuje kaznu zatvora od tri meseca do tri godine. Najteži oblik ovog krivičnog dela za koji je propisana kazna zatvora od šest meseci do pet godina postoji ako je preduzetom radnjom prouzrokovana šteta u iznosu preko 600.000 dinara.

Računarska sabotaža je drugo kompjutersko krivično delo u našem pravu za koje je propisana kazna zatvora od jedne do osam godina. Delo čini lice koje uništi, izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program ili ošteti računar ili drugi uredjaj za elektronsku obradu prenos podataka koji je od značaja za državni organ, javnu službu, ustanovu, preduzeće ili drugu organizacioju. Objekt napada kod ovog dela je dvojako odredjen. To je prvo. računarski podatak ili program (kao i kod prethodnog krivičnog dela) ali i računar odnosno drugi uredjaj za elektronsku obradu ili prenos podataka. No, ovde se mora raditi i o posebnom svojstvu oštećenog. Naime, ovi objekti moraju da pripadaju državnom organu, javnoj službi ili drugim pravnim licima kao što su ustanove,preduzeća ili druge organizacije. Inače u pogledu radnje izvšenja i ostalih obeležja bića ovog dela nema razlike u odnosu na prethodno krivično delo.

[20] Vidi : Ljubiša Jovanović-Vojislav Djurdjić-Dragan Jovašević,Krivično pravo,Posebni deo, Službeni glasnik,Beograd,2004.godine ; Vojislav Djurdjić-Dragan Jovašević,Praktikum za krivično pravo,Posebni deo,Službeni glasnik,Beograd,2003.godine

Pravljenje i unošenje računarskih virusa je krivično delo predvidjeno u čl. 186v. Delo ima osnovni i teži oblik. Osnovno delo čini lice koje napravi računarski virus u nameri da ga uense u tudji računar ili računarsku mrežu. Radnja izvršenja je samo sačinjavanje, pravljenje virusa. Šta su to virusi, kako se prave, koje su njihove vrste ili karakteristike, svrha i sadržina predstavljaju pitanja koje sudsko veće mora da reši u svakom konkretnom slučaju kao faktičko pitanje. U tome im stručnu pomoć moraju da pruže lica sa posebnim znanjima i veštinama – veštaci informatičke struke. Delo je svršeno samim momentom pravljenja ovakvog virusa u nameri da se on unese u tudji računar ili računarski sistem bez obzira da li je takva namera i ostvarena u konkretnom slučaju ili ne. Za ovo je delo propisana novčana kazna ili zatvor do jedne godine.

Ako je pak ovako sačinjeni,napravljeni virus i unet u tudji računar ili računarsku mrežu čime je prouzrokovana šteta (bilo imovinska ili neimovinska i to bez obzira u kom iznosu) radi se o težem obliku ovog krivičnog dela za koji je propisana kazna zatvora od tri meseca do tri godine.

Sledeće je krivično delo predvidjeno u čl.186g. To je **računarska prevara**. Delo ima jedan osnovni, jedan posebni i dva teža, kvalifikovana oblika. Osnovno delo čini lice koje unese netačan podatak ili ne unese kakav važan podatak ili ko na drugi način prikrije ili lažno prikaže podatak i tako utiče na rezultat elektronske obrade ili prenosa podataka. Bitno je da je ova radnja falsifikovanja,krivotvorenja, dovodjenja u zabludu oštećenog preduzeta u nameri da se sebi ili drugom pribavi protivpravna imovinska korist odnosno da se drugome nanese kakva imovinska šteta. Za postojanje krivičnog dela dovoljno je da je radnja izvršenja preduzeta u navedenoj nameri. Tog trenutka je delo svršeno. Nije potrebno da je u konkretnom slučaju u nastupila imovinska šteta za neko lice. Za ovo je delo propisana kazna zatvora od šest meseci do pet godina.

Poseban oblik računarske prevare za koji je propisana novčana kazna ili zatvor do dve godine postoji kada je radnja krivotvorenja podataka ili prikrivanja ili lažnog prikazivanja računarskih podataka preduzeta u nameri da se na ovaj način drugom licu nanese kakva šteta. Ta šteta ne mora da nastupi u konkretnom slučaju, ali ona mora da bude pobuda, unutrašnji pokretač učinioca na preduzimanje radnje izvršenja. Može se raditi o imovinskoj,ali i drugim vidovima neimovinske štete.

Zavisno od visine pribavljene protivpravne imovinske koristi za učinioca ili neko drugo lice zakon razlikuje dva teža, kvalifikovana oblika ovog krivičnog dela. Prvi teži oblik za koji je propisana kazna zatvora od dve do deset godina postoji kada je pribavljena imovinska korist u iznosu preko 100.000 dinara. Ako je pak na ovaj način pribavljena protivpravna imovinska korist u iznosu preko 600.000 dinara radi se o najtežem obliku računarske prevare za koji je propisana kazna zatvora od dve do dvanaest godina.

Ometanje funkcionisanja elektronske obrade i prenosa podataka i računarske mreže je krivično delo predvidjeno u čl. 186d. Krivičnog zakona Republike Srbije. Delo ima dva oblika ispoljavanja . Osnovni i teži oblik. Osnovno delo se sastoji u neovlašćenom (dakle protivpravnom) pristupu (upadu) elektronskoj obradi podataka ili računaskoj mreži čime je izazvan zastoj ili poremećeno funkcionisanje elektronske obrade i prenosa podataka ili same mreže. Za postojanje dela nije dovoljno samo da neko lice neovlašćeno, nepozvano upadne u tudji računarski sistem. Potrebno je da usled tako preduzete delatnosti dodje do posledice u vidu povrede koja se manifestuje ili zastoj ili poremećenje u funkcionisanju, obradi ili prenosu računarskih podataka ili pak cele mreže. Delo se može preduzeti u bilo

kojoj nameri ali njeno postojanje na strani učinioca nije elemenat bića krivičnog dela. Učinilac može biti svako lice, a u pogledu vinosti potreban je umišljaj. Za ovo je delo propisana novčana kazna ili zatvor do dve godine.

Teži oblik ovog krivičnog dela za koji je propisana kazna zatvora od šest meseci do pet godina postoji ako su usled preduzete radnje izvršenja osnovnog dela nastupile teške posledice. Koje su to teške posledice po računarski sistem, prenos ili obradu podataka ili njegovo funkcionisanje predstavlja faktičko pitanje koje sud mora da reši u svakom konkretnom slučaju na bazi svih objektivnih i subjektivnih okolnosti učinjenog dela i ličnosti učinioca. Bitno je da su posledice teške, znači u većem obimu ili iznosu odnosno u dužem trajanju.

Neovlašćeni pristup zaštićenom računaru ili računarskoj mreži je krivično delo predvidjeno u čl. 186dj. koje ima osnovni i dva teža oblika ispoljavanja. Osnovno delo čini lice koje kršeći mere zaštite (preventivno – tehničke i druge mere) neovlašćeno pristupi računaru ili računarskoj mreži. Radnja izvršenja je pristupanje, ulazak, upad u tudji računar ili računarsku mrežu. Bitno je da je ova radnja preduzeta neovlašćeno, dakle protivpravno i drugo kršenjem predvidjenih mera zaštite. Ove okolnosti moraju biti obuhvaćene umišljajem učinioca dela. Za ovo je delo propisana novčana kazna ili zatvor do jedne godine.

Prvi teži oblik za koji je propisana novčana kazna ili zatvor do tri godine čini lice koje upotrebi podatak koji je pribavio, do koga je došao neovlašćenim pristupom zaštićenom računaru ili računarskoj mreži. Ova upotreba može biti u bilo kojoj nameri ili za bilo koju svrhu ili cilj. Ako je pak usled preduzete radnje upotrebe na ovaj način pribavljenog računarskog podatka došlo do nastupanja teških posledica za drugog (drugo fizičko ili pravno lice) radi se o najtežem krivičnom delu ove vrste za koje je zakon propisao kaznu zatvora od šest meseci do pet godina. Bitno je da je posledica i to teška (a to je faktičko pitanje za sudsko veće) nastupila za drugog i da izmedju nje i preduzete radnje upada u zaštićeni računarski sistem postoji uzročno-posledična veza.

Poslednje računarsko krivično delo u našem pravnom sistemu uvedeno novelom republičkog krivičnog zakona iz aprila 2003.godine je : **Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži**. Ovo je delo propisano u odredbi čl.186e. Delo ima osnovni i teži oblik. Objekt napada u ovom slučaju je javna računarska mreža. Osnovno delo čini lice koje neovlašćeno (dakle protivno postojećim propisima, protiovzakonito) sprečava ili ometa pristupo javnoj računarskoj mreži. Za ovo je delo propisana novčana kazna ili zatvor do jedne godine. U slučaju da se kao učinilac javi službeno lice u vršenju službe tada se radi o kvalifikovanom obliku ovog dela za koji je propisana kazna zatvora do tri godine. Ovde se zapravo radi o posebnom, specijalnom obliku krivičnog dela zloupotrebe službenog položaja službenog lica[21] koje sprečava ili ometa drugome fizičkom ili pravnom licu nesmetani pristup i korišćenje javne računarske mreže.

I Krivični zakonik Republike Crne Gore iz decembra 2003. godine u glavi 28. pod naslovom "Krivična djela protiv bezbjednosti računarskih podataka" predvidja više računarskih krivičnih dela za kojaa su propisane stroge kazne zatvora i mera bezbednosti oduzimanja uredjaja i sredstava. To su

[21] Vidi : Dragan Jovašević,Komentar Krivičnog zakona SR Jugoslavije,Službeni glasnik, Beograd,2002.godine

- Oštećenje računarskih podataka i programa u čl. 349.,
- Računarska sabotaža u čl. 350.,
- Pravljenje i unošenje računarskih virusa u čl. 351.,
- Računarska prevara u čl. 352.,
- Neovlašćeno korišćrenje računara ili računarske mreže u čl. 353.,
- Ometanje funkcionisanja elektronske obrade i prenosa podataka i računarske mreže u čl. 354.,
- Neovlašćeni pristup zaštićenom računaru i računarskoj mreži u čl. 355. i
- Sprječavanje i ograničavanje pristupa javnoj računarskoj mreži u čl. 356.

Zaključak

Iako je danas nemoguć život i funkcionisanje ni gradjana ni drugih poslova pa ni države u celini bez upotrebe računara i savremene informatičke tehnologije sazrela je svest da se ova korisna i nadasve potrebna sredstva mogu koristiti za nedopuštene, protivpravne ciljeve u prvom radu za pribavljanje protivpravne imovinske koristi za neko lice ili za nanošenje štete drugima. Budući da je naša stvarnost poslednjih godina zabeležila brojne sučajeve zloupotrebe kompjutera u kriminalne svrhe to je bilo krajnje vreme da se i država ne samo preventivnim merama već i sistemom krivičnih sankcija uhvati u koštac za ovakvim neodgovornim pojedincima i grupama.

To je bio osnovni motiv da se i naša zemlja pridruži velikom broju zemalja koji u svom sistemu krivičnog zakonodavstva predvidjaju različite oblike i vidove kompjuterskog kriminaliteta za koje su propisane stroge krivične sankcije – kazne zatvora u dugom trajanju, u pojedinim slučajevima preko pet čak do 12 godina .U sistemu ovih inkriminacija preovladjuju različiti slučajevi protivpravnog neovlašćenog upada u tudje računare i računarske sisteme drugih lica (fizičkih lica,pravnih lica ili državnih organa ili javnih službi).

Takve nedopuštene delatnosti mogu biti različite : od izmene, uništenja, oštećenja do korišćčenja i upotrebe neovlašćeno pribavljenih podataka. Najčešće se ova dela preduzimaju sa posebnim prishičkim elementom na strani učinioca – namerom da se sebi ili drugom pribavi kakva korist (imovinska ili druga) odnosno da se drugome nanese kakva šteta. Ako je takva korist pribavljena ili pak je takva šteta naneta radi se o težim, kvalifikovanim oblicima za koja je zakon predvideo strože kažnjavanje.

Nadamo se da će primena ovih zakonskih rešenja u velikoj meri suzbiti i predupreditи brojna protivpravna postupanja u odnosu na računar ili posredstvom računara čime će zaštita ljudskih i društvenih dobara i vrednosti, sigurnost i poverenje u računarske sisteme kao i zaštita ljudskih sloboda i prava dobiti kvalitetno viši nivo.