Autori: *(1) Prof. dr. Dragan Jovašević, redovni profesor; (2) Doc. dr.. Marina M. Simović, docent*
Institucija: *(1) Pravni fakultet Univerziteta u Nišu; (2) Fakultet pravnih nauka, Univerzitet "Apeiron", Banja Luka*

BEZBJEDNOST RAČUNARSKIH SISTEMA U SRBIJI I EVROPSKI STANDARDI

Sažetak

U novom krivičnom zakonodavstvu Republike Srbije od 2005. godine propisana je krivična odgovornost i kažnjivost za više krivičnih djela protiv bezbjednosti računarskih podataka. To su računarska ili kompjuterska krivična djela koja učinilac vrši zloupotrebom računara čime prouzrokuje imovinsku ili neimovinsku štetu drugim fizičkim ili pravnim licima. U osnovi ovih inkriminacija se nalaze evropski standardi utvrđeni u Konvenciji o kibernetičkom (sajber) kriminalu i Dodatnom protokolu uz ovu konvenciju, kao i nizu drugih evropskih dokumenata. U radu se analiziraju osnovne karakteristike računarskih krivičnih djela u Srbiji i stepen njihove usaglašenosti sa evropskim standardima.

Ključne riječi: zloupotreba računara, evropski standardi, kriminal, odgovornost, sankcija.

1. Uvod

Savjet Evrope je donošenjem Konvencije o kibernetičkom (sajber) kriminalu (Convention on Cybercrime, ETS 185), od 23. novembra 2001. godine[i], pokušao da postavi osnove jedinstvenog evropskog sistema materijalnog i procesnog krivičnog prava u oblasti neophodne saradnje država članica u suzbijanju različitih oblika i vidova računarskog (kibernetičkog) kriminala. Pri tome je sama Konvencija (čl. 2-13) propisala pet krivičnih djela ove vrste koja su upravljena protiv tajnosti, cjelovitosti i dostupnosti računarskih podataka i sistema. Ovim su postavljene osnove za pojedina nacionalna zakonodavstva da preciznije odrede obilježja i karakteristike pojedinih računarskih krivičnih djela, njihove osnovne, lakše ili teže oblike, te da propišu krivične sankcije za njihove učinioce (fizička ili pravna lica).

Uz ovu konvenciju je usvojen i Dopunski protokol o kriminaliziranju akata rasističke i ksenofobične prirode koja su učinjena posredstvom računarskih sistema. I ovaj protokol u čl. 3-7 propisuje takođe krivičnu odgovornost i kažnjivost za zloupotrebu računara u vršenju krivičnih djela iz rasističkih i ksenofobičnih pobuda (motiva).

Osim pomenute konvencije, veliki značaj ima i Direktiva 2013/40/EU Evropskog parlamenta i Vijeća Evropske unije od 12. avgusta 2013. godine o napadima na informacijske sisteme i o zamjeni Okvirne odluke Vijeća 2005/222/PUP.[ii] Imajući u vidu utvrđene obaveze za države članice Savjeta Evrope, bilo je logično očekivati da će i u krivičnom zakonodavstvu Republike Srbije (tada Državnoj zajednici Srbija i Crna Gora) uslijediti, prvo, na zakonodavnom planu, pa potom i u praksi efikasna, kvalitetna i zakonita borba sa računarskim kriminalitetom i njihovim izvršiocima. Prihvatajući navedenu konvenciju, izmjenama i dopunama Krivičnog zakona Republike Srbije iz aprila 2003. godine u krivičnopravni sistem je uvedeno više računarskih krivičnih djela (u glavi 16a), pod nazivom „Krivična djela protiv bezbjednosti računarskih podataka“[iii]. Identična krivična djela su uvedena i u Krivičnom zakoniku Crne Gore od 2003. godine (u glavi 28 pod istim nazivom[iv]).

2. Evropski standardi zaštite računarskih sistema

U osnovi Konvencije o kibernetičkom kriminalu, kao obavezujućem međunarodnom dokumentu koji je donijet od strane najznačajnije i najmasovnije evropske regionalne organizacije, nalazi se više prethodno donijetih preporuka kao što su: (1) Preporuka broj R (85) 10 o praktičnoj primjeni Evropske konvencije o uzajamnoj pomoći u krivičnim predmetima u pogledu pružanja međunarodne krivičnopravne pomoći pri presretanju komunikacija, (2) Preporuka broj R (88) 2 o piratstvu na polju autorskih i srodnih prava, (3) Preporuka broj R (87) 15 koja propisuje upotrebu ličnih podataka u oblasti djelatnosti policije, (4) Preporuka broj R (95) 4 o zaštiti ličnih podataka na području telekomunikacionih usluga sa posebnim osvrtom na ulogu telefonije, (5) Preporuka broj R (89) 9 o računarskom kriminalu koja daje smjernice nacionalnim organima u pogledu definisanja pojedinih računarskih krivičnih djela i (6) Preporuka broj R (95) 13 o problemima krivičnog procesnog prava koji su vezani za informatičku tehnologiju.

Konvencija o kibernetičkom kriminalu predviđa niz pravnih sredstava, mjera i postupaka koji su nužni radi odvraćanja lica od radnji koje su usmjerene protiv tajnosti, cjelovitosti i dostupnosti računarskih, sistema, mreža i računarskih podataka, kao i za odvraćanje od njihove zloupotrebe u bilo kom vidu. Na taj način se olakašava otkrivanje, istraživanje i krivični progon tih djela i njihovih učinilaca na domaćem i međunarodnom nivou i osigurava efikasna i brza međunarodna saradnja. U članu 1 Konvencije se definišu osnovni pojmovi računarskog (kibernetičkog, sajber) kriminaliteta, kao što su: računarski sistem, računarski

[i] Vidi Pavišić, 261-265.
[ii] Directive 2013/40/EU of the European Parliament and of the Council of the European Union, of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.
[iii] Vidi Jovašević, 2003, 351-361.
[iv] Zakonik je objavljen u “Službenom listu RCG” br. 70/03, 13/04 i 47/06 i “Službenom listu CG” br. 40/08, 25/10, 32/11, 40/03 i 56/13. Vidi Lazarević, Vučković, Vučković, 816-824.

podatak, davalac usluga ili podaci o prometu. Ovim je dato uputstvo nacionalnom zakonodascu da u ovom duhu tretira ove zaštićene vrijednosti kao objekte krivičnopravne zaštite.[v]

U drugom poglavlju Konvencije, pod nazivom "Kazneno materijalno pravo" u više odredbi su dati pojam i karakteristike pojedinih krivičnih djela koje treba inkriminisati u nacionalnim pravnim sistemima država članica Savjeta Evrope. To su sljedeća krivična djela: (1) krivična djela protiv tajnosti, cjelovitosti i dostupnosti računarskih podataka i sistema (čl. 2-6): nezakoniti pristup, nezakonito presretanje, ometanje podataka, ometanje sistema i zloupotreba uređaja, (2) računarska krivična djela (čl.7 i 8): računarsko falsifikovanje i računarska prevara, (3) krivična djela u vezi sa sadržajem (član 9) – krivična djela vezana za dečju pornografiju i (4) krivična djela povrede autorskih i srodnih prava (član 10). Od posebnog značaja su odredbe Konvencije koje izričito zahtijevaju od država članica da se kazni i za pokušaj ovih krivičnih djela, kao i za oblike saučesništva u vidu podstrekavanja i pomaganja, te da se, pored odgovornosti fizičkih lica, za ova djela predvidi i krivična odgovornost pravnih lica. Sve navedene standarde je novo krivično zakonodavstvo Srbije u potpunosti implementiralo u svoj pravni sistem obezbjeđujući vrstu i mjeru kazne za pojedina krivična djela, kao i formirajući u okviru policije, javnog tužilaštva i Višeg suda u Beogradu posebne organizacione jedinice za borbu protiv visokotehnološkog kriminala.

3. Opšte karakteristike krivičnopravne zaštite računarskih podataka

Objekt zaštite ovih krivičnih djela jeste bezbjednost računarskih (kompjuterskih) podataka i sistema, odnosno računarske mreže.[vi] Iako je danas uobičajeno da se ova krivična djela obuhvataju pojmom kompjuterski kriminalitet, zakonodavac Republike Srbije za njih je ipak upotrijebio termin računarski kriminalitet. Međutim, pored ovog naziva za krivična djela sistematizovana na ovom mjestu, zakonodavstvo Republike Srbije upotrebljava i pojam visokotehnološki kriminal.[vii] Pod ovim se pojmom podrazumijeva vršenje krivičnih djela kod kojih se kao objekat ili kao sredstvo izvršenja krivičnih djela javljaju računari, računarske mreže, računarski podaci, računarski sistemi, kao i njihovi proizvodi u materijalnom ili elektronskom obliku.[viii]

Pri tome je Krivični zakonik Republike Srbije[ix] (KZ) od 2005. godine u članu 112 odredio pojam i karakteristike: računarskog podatka, računarske mreže, računarskog programa, računarskog virusa, računara i računarskog sistema u smislu objekta napada kod ovih krivičnih djela. Računarski podatak je svako predstavljanje činjenica, informacija ili koncepta u obliku koji je podesan za njihovu obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski sistem obavlja svoju funkciju (stav 17). Računarska mreža predstavlja skup međusobno povezanih računara, odnosno računarskih sistema koji komuniciraju, razmjenjujući podatke (stav 18). Računarski program je uređeni skup naredbi koji služi za upravljanje radom računara, kao i za rješavanje određenog zadatka pomoću računara (stav 19). Računarski virus je računarski program ili drugi skup naredbi koji je unijet u računar ili računarsku mrežu, koji je napravljen da sam sebe umnožava i djeluje na druge programe ili podatke u računaru ili računarskoj mreži - dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka (stav 20). Računar je svaki elektronski uređaj koji na osnovu programa automatski obrađuje i razmjenjuje podatke (stav 33). I konačno, računarski sistem je svaki uređaj ili grupa međusobno povezanih ili zavisnih uređaja od kojih jedan ili više njih, na osnovu programa, vrši automatsku obradu podataka (stav 34).

Kompjuter (računar) predstavlja jednu od najznačajnijih i najrevolucionarnijih tekovina tehničko-tehnološkog razvoja na kraju 20. vijeka. Međutim, pored prednosti koje računar nosi sa sobom i ogromne koristi za čovječanstvo, on je ubrzo postao i sredstvo zloupotrebe nesavjesnih pojedinaca ili grupa. Tako

---

[v] Vidi Kareklas, 94-97.

[vi] Vidi Brvar, B. (1982). *Pojavne oblike zlorabe računalnika.* Ljubljana: Revija za kriminalistiko in kriminologijo, (2), 27-32 i Vodinelić, V. (1990). *Metodika otkrivanja, razjašnjenja i dokazivanja računarskog kriminaliteta*. Zagreb: Priručnik, (4), 330-337.

[vii] Pojam, karakteristike, organi krivičnog gonjenja i postupak za krivična djela visokotehnološkog kriminala uređeni su odredbama Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Službeni glasnik Republike Srbije" broj 61/05).

[viii] Vidi Jovašević, D. (2003). *Krivičnopravna zaštita bezbjednosti računarskih podataka*. Beograd: Pravni informator, (6), 53-58.

[ix] "Službeni glasnik Republike Srbije" br. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13 i 108/14.

nastaje računarski kriminalitet, kao poseban i specifičan oblik savremenog kriminaliteta. Zahvaljujući ogromnoj moći računara u memorisanju i brzoj obradi velikog broja podataka, automatizovani informacioni sistemi postaju sve brojniji i nezamjenjivi pratilac cjelokupnog ljudskog i društvenog života fizičkih i pravnih lica. Različite forme primjene računara u svim oblastima života, privrede i drugih društvenih djelatnosti nisu ostale nezapažene od strane nesavjesnih i zlonamjernih pojedinaca ili grupa koji (ne birajući sredstva i načine) pokušavaju da pribave za sebe ili drugog protivpravnu imovinsku korist ili da drugome nanesu kakvu štetu.[x] Tako računar postaje sredstvo, oruđe za izvršenje krivičnih djela. Za različite oblike i vidove zloupotrebe računara u teoriji se upotrebljavaju različiti nazivi: zloupotreba računara, delikti uz pomoć računara, informatički kriminalitet, računarski kriminalitet, sajber kriminalitet, tehno kriminalitet itd.

Pod pojmom računarskog kriminaliteta podrazumijeva se sveukupnost različitih oblika, vidova i formi ispoljavanja protivpravnih ponašanja upravljenih protiv bezbjednosti računarskih, informacionih i kompjuterskih sistema u cjelini ili njihovih pojedinih dijelova na različite načine i različitim sredstvima u namjeri da se sebi ili drugom pribavi korist (imovinske ili neimovinske prirode) ili da se drugome nanese šteta. Iz ovako određenog pojma računarskog kriminaliteta proizilaze njegove karakteristike: (1) objekt zaštite je bezbjednost računarskih podataka ili informacionog sistema u cjelini ili njegovog pojedinog dijela (segmenta), (2) poseban, specifičan karakter i priroda protivpravnih djelatnosti pojedinaca, (3) posebna znanja i specijalizacija na strani učinioca ovih krivičnih djela koja isključuje mogućnost da se svako, bilo koje lice nađe u ovoj ulozi, (4) poseban način i sredstvo preduzimanja radnje izvršenja – uz pomoć ili upotrebom (zloupotrebom) računara i (5) namjera učinioca kao subjektivni elemenat u vrijeme preduzimanja radnje koja se ogleda u namjeri pribavljanja za sebe ili drugog koristi ili nanošenja štete drugom fizičkom ili pravnom licu.[xi]

Računarski kriminalitet karakteriše velika dinamika i izuzetna šarolikost pojavnih oblika, formi i vidova ispoljavanja.[xii] To je i razumljivo jer se radi o novoj tehnologiji, sa velikim mogućnostima primjene u širokoj sferi ljudske, društvene i privredne djelatnosti, te su i mogućnosti zloupotrebe računara svaki dan sve veće. Pored novih pojavnih oblika, ranije već poznatih krivičnih djela koja pod uticajem zloupotrebe kompjutera mijenjaju tradicionalni, klasični način i modus ispoljavanja, javljaju se i novi oblici protivpravnog ponašanja koji ne poznaju granice između država. Štetne posljedice računarskih krivičnih djela su velike i ispoljavaju se u nastupanju imovinske štete za fizička ili pravna lica (ponekad i za cijelu državu), u gubitku poslovnog ugleda, gubitku povjerenja u sigurnost i istinitost računarskog poslovanja i uopšte računarskih podataka, opasnosti od zloupotrebe za slobode i prava čovjeka, na razne načine odavanje lične, poslovne i drugih vidova tajni i sl.

Izvršioci ovih krivičnih djela predstavljaju specifičnu kategoriju lica. Radi se, uglavnom, o nedelinkventnim i socijalno prilagodljivim, nenasilnim ličnostima. Oni za vršenje krivičnih djela putem računara moraju da posjeduju određena specijalna, stručna i praktična znanja i vještine u domenu informatičke i računarske tehnike i tehnologije. Pored toga, radi se o licima kojima su ovakva tehnološka sredstva dostupna u fizičkom smislu. Ova se krivična djela vrše prikriveno, često bez vidljive prostorne i vremenski bliske povezanosti između učinioca djela i oštećenog (pasivnog subjekta). U praksi postoji veća ili manja vremenska razlika između preduzete radnje izvršenja i trenutka nastupanja posljedice. Ova se djela teško otkrivaju, a još teže dokazuju, dugo ostaju praktično neotkrivena, sve dok oštećeni ne pretrpi štetu u domenu informatičkih i računarskih podataka ili sistema. Radi se o kriminalitetu koji brzo i lako mijenja forme i oblike ispoljavanja, granice među državama, kao i vrstu oštećenog. U pogledu krivice, ova se djela vrše isključivo sa umišljajem.

4. Pojedina računarska krivična djela

KZ je u verlikoj mjeri preuzeo niz utvrđenih evropskih standarda koji predviđa navedena evropska konvencija kako bi u potpunosti stvorio osnove za efikasnu, kvalitetnu, zakonitu i blagovremenu

[x] Vidi Petrović, S. (1994). *Kompjuterski kriminalitet*. Beograd: Bezbjednost, (1), 32-40.
[xi] Vidi Đokić, Z., Živanović, S. (2005). *Kompjuterski kriminal kao obilježje progresivnog kriminaliteta*. Zbornik radova „Kazneno zakonodavstvo – progresivna ili regresivna rješenja. Beograd, 305-318.
[xii] Vidi Kitarović, N. (1998). *Kompjuterski kriminalitet*. Beograd: *Bilten sudske praske Vrhovnog suda Srbije*, (2-3), 52-56.

krivičnopravnu zaštitu računarskih podataka, sistema i drugih zaštićenih vrijednosti. U odnosu na prvobitna rješenja, u septembru 2009. godine je dodato novo krivično djelo propisano u članu 304a KZ. Tako, danas sistem krivičnih djela protiv bezbjednosti računarskih podataka čine sljedeća krivična djela[xiii]: (1) Oštećenje računarskih podataka i programa (član 298 KZ), (2) Računarska sabotaža (član 299 KZ), (3) Pravljenje i unošenje računarskih virusa (član 300 KZ), (4) Računarska prevara (član 301 KZ), (5) Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (član 302 KZ), (6) Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 303 KZ), (7) Neovlašćeno korišćenje računara ili računarske mreže (član 304 KZ) i (8) Pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih djela protiv bezbjednosti računarskih podataka (član 304a KZ).

4.1. Oštećenje računarskih podataka i programa

Krivično delo iz člana 298 se sastoji u neovlašćenom brisanju, izmjeni, oštećenju, prikrivanju ili na drugi način činjenju neupotrebljivim računarskog podatka ili programa. Objekt zaštite je bezbjednost računarskih podataka ili računarskih programa, a objekt napada je računarski podatak ili program. Računarski podatak je svako predstavljanje činjenica, informacija ili koncepta u obliku koji je podesan za njihovu obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski sistem obavlja svoju funkciju. Računarski program je uređeni skup naredbi koji služi za upravljanje radom računara, kao i za rješavanje određenog zadatka pomoću računara.

Radnja izvršenja je alternativno određena[xiv] i sastoji se u preduzimanju sljedećih djelatnosti: 1) brisanju, 2) izmjeni, 3) oštećenju, 4) prikrivanju i 5) činjenju neupotrebljivim računarskog podatka ili programa. Za postojanje ovog djela je bitno da se radnja preduzima neovlašćeno, dakle od strane neovlašćenog lica, na način i u postupku koji nisu dozvoljeni i u skladu sa zakonom.

Brisanje je uklanjanje računarskih podataka u cjelini ili djelimično ili računarskog programa. Izmjena je delimična promjena postojećih podataka ili unošenje novih podataka na način, od strane lica i u postupku koji nije predviđen odgovarajućim propisima ili po odgovarajućoj proceduri. Oštećenje je privremeno, djelimično ili kratkotrajno onesposobljenje korišćenja računarskog podatka ili programa izazivanjem kvarova ili kidanjem pojedinih dijelova, veza ili sklopova, tako da se računarski podatak ili program ne mogu koristiti za određeno vrijeme za svrhu za koju su namijenjeni.

Prikrivanje je premještanje podatka ili programa sa mjesta na kome je bio pohranjen ili sadržan i sklanjanje na drugo, najčešće nepoznato mjesto. Činjenje neupotrebljivim na drugi način je svako drugo onesposobljenje za kraće ili duže vrijeme ili onemogućavanje u većoj ili manjoj mjeri korišćenja računarskog podatka ili programa. Posljedica djela je povreda zaštićenog dobra – računarskog podatka ili programa koji pripada fizičkom ili pravnom licu u smislu njegove upotrebljivosti, korisnosti uopšte ili za određeno vrijeme, na određenom mjestu ili za određenu namjenu.

Izvršilac djela može da bude svako lice, a u pogledu krivice potreban je umišljaj. Za ovo je djelo propisana novčana kazna ili kazna zatvora do jedne godine. Sud učiniocu djela obavezno izriče mjeru bezbjednosti oduzimanja uređaja i sredstava ako su ispunjena dva uslova: 1) da se radi o sredstvima i uređajima kojima je krivično djelo učinjeno i 2) da su sredstva i uređaji u svojini učinioca djela.

Ovo djelo ima dva teža oblika. Prvi teži oblik djela postoji ako je preduzetom radnjom izvršenja osnovnog djela prouzrokovana šteta u iznosu preko 450.000 dinara. Visina pričinjene imovinske štete (u vrijeme izvršenja djela u zakonom utvrđenom iznosu) predstavlja kvalifikatornu okolnost. Za ovo je djelo propisana kazna zatvora od tri mjeseca do tri godine. Drugi teži oblik djela, za koji je propisana kazna zatvora od tri mjeseci do pet godina, postoji ako je preduzetom radnjom osnovnog djela prouzrokovana imovinska šteta u iznosu preko 1.500.000 dinara.

[xiii] Vidi Đurđić, Jovašević, 215-217.
[xiv] Vidi Lazarević, Vučković, Vučković, 816 i 817.

4.2. Računarska sabotaža

Ovo djelo iz člana 299 KZ čini lice koje unese, uništi, izbriše, izmijeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program ili uništi ili ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka u namjeri da onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državni organ, javnu službu, ustanovu, preduzeće ili druge subjekte.[xv]

Objekt zaštite je dvojako određen kao: 1) računarski podatak ili program i 2) računar i drugi uređaj za elektronsku obradu i prenos podataka. Bitno je da ovi uređaji i sredstva pripadaju, odnosno da su od značaja za državni organ, javnu službu, ustanovu, preduzeće ili drugog subjekta.

Radnja izvršenja[xvi] je alternativno određena kao: 1) unos, 2) uništenje, 3) brisanje, 4) izmjena, 5) oštećenje, 6) prikrivanje i 7) činjenje neupotrebljivim na drugi način računarskog podatka ili programa, odnosno uništenje ili oštećenje računara ili drugog uređaja za elektronsku obradu i prenos podataka.

Unos je upisivanje ili pohranjivanje novog do tada nepostojećeg podatka ili izmjena već postojećeg računarskog ili drugog podatka u računarskom programu. Uništenje je potpuno i trajno razaranje supstance ili oblika određenog predmeta tako da više uopšte ne može da se koristi za svrhu, namjenu za koju je ranije korišćen. Brisanje je uklanjanje, najčešće mehaničkim ili drugim putem, u cjelini ili djelimično, računarskog podatka ili programa. Izmjena je djelimično mijenjanje postojećih podataka u smislu njihove sadržine, mjesta gdje se nalaze ili njihove prirode ili unošenje drugih neistinitih podataka u računarski sistem. Oštećenje je privremeno, djelimično ili kratkotrajno onesposobljenje računarskog podatka, programa, računara ili drugog uređaja za svrhu za koju su inače namijenjeni. Prikrivanje je sklanjanje podatka ili predmeta sa mjesta na kome se do tada nalazio i koje je svima bilo poznato i premještanje na drugo, najčešće skriveno mjesto, tako da se sa njihovom sadržinom ne mogu upoznati druga lica uopšte ili za određeno vrijeme. Činjenje neupotrebljivim računarskog podatka ili programa predstavlja svaku djelatnost kojom se u većoj ili manjoj mjeri utiče na upotrebljivost računarskih podataka ili programa.

Zavisno od objekta napada prema kome je upravljena radnja izvršenja ovog krivičnog djela, razlikuju se dva njegova oblika. To su: 1) uništenje ili oštećenje računarskog podatka ili programa i 2) uništenje i oštećenje računara ili drugog uređaja za elektronsku obradu i prenos podataka. Ono što je bitno za postojanje oba oblika djela jeste: a) da se radnja izvršenja preduzima u odnosu na objekte koji pripadaju državnom organu, javnoj službi, ustanovi, preduzeću ili drugom subjektu (pravnom licu sa posebnim ovlašćenjima)[xvii]; b) da na strani učinioca u vrijeme preduzimanja radnje postoji određena namjera - da se onemogući (u potpunosti i trajno) ili znatno omete (otežа) postupak elektronske obrade i prenosa podataka. Nije od značaja da li je ova namjera u konkretnom slučaju i ostvarena. Posljedica djela je povreda računarskog podatka, programa, računara ili uređaja za automatski prenos ili obradu podataka u smislu njihove upotrebljivosti i korisnosti.

Izvršilac djela može da bude svako lice, a u pogledu krivice potreban je direktni umišljaj koji karakteriše navedena namjera. Za ovo je djelo propisana kazna zatvora od šest mjeseci do pet godina.

4.3. Pravljenje i unošenje računarskih virusa

Specifično krivično djelo iz člana 300 KZ se sastoji u pravljenju računarskog virusa u namjeri njegovog unošenja ili njegovom unošenju u tuđi računar ili računarsku mrežu. Objekt zaštite je bezbjednost računara i računarske mreže od virusa različite vrste i prirode, a objekt napada je računarski virus. To je računarski program ili neki drugi skup naredbi unijet u računar ili računarsku mrežu koji je napravljen da sam sebe umnožava i djeluje na druge programe ili podatke u računaru ili računarskoj mreži -dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka.

[xv] Vidi Kitarović, Kompjuterski kriminalitet, op. cit., 52-56.
[xvi] Vidi Jovašević, 2003, 354 i 355.
[xvii] Dakle, svojstvo oštećenog predstavlja elemenat bića ovog krivičnog djela.

Radnja izvršenja se sastoji u:

(1) pravljenju - stvaranju računarskog virusa koji je podoban, dovoljan, u mogućnosti da prouzrokuje određene promjene, oštećenja u korišćenju ili upotrebljivosti računara ili računarske mreže u (cjelini ili djelimično). Za postojanje ove radnje izvršenja je potrebno da učinilac postupa sa namjerom (kao subjektivnim elementom) da tako stvoreni računarski virus unese u tuđi računar ili računarsku mrežu. Namjera mora da postoji na strani učinioca u vrijeme preduzimanja radnje, bez obzira na to da li je u konkretnom slučaju ona i ostvarena;

(2) unošenju računarskog virusa, neposredno ili posredno, u tuđi računar ili računarsku mrežu, bez obzira na to ko je ovaj virus napravio.

Izvršilac djela može da bude svako lice, a u praksi su to lica koja posjeduju posebna, specijalna znanja iz oblasti računarstva i informatike. U pogledu krivice potreban je direktni umišljaj koji karakteriše navedena namjera. Za ovo je djelo propisana novčana kazna ili kazna zatvora do šest mjeseci. Uređaji i sredstva kojima je učinjeno djelo se obavezno oduzimaju - primjenom mjere bezbjednosti oduzimanja predmeta.

Teži oblik djela, za koji je propisana novčana kazna ili kazna zatvora do dvije godine, postoji ako je ovako stvoreni virus unijet u tuđi računar ili računarsku mrežu čime je prouzrokovana šteta. Za postojanje djela je bitno da je učinilac svjestan, da zna u vrijeme preduzimanja radnje – rada na računaru, da na takav način upravo unosi računarski virus u tuđi računar ili računarsku mrežu. Šteta koja je na ovaj način prouzrokovana, može biti imovinskog ili neimovinskog karaktera. Bitno je da ovako prouzorokovana šteta predstavlja rezultat preduzete radnje osnovnog djela i da u odnosu na nju učinilac postupa sa nehatom.

4.4. Računarska prevara

Računarska prevara iz člana 301 KZ se sastoji u unošenju netačnog podatka, propuštanju unošenja tačnog podatka ili na drugi način prikrivanju ili lažnom prikazivanju podatka čime se utiče na rezultat elektronske obrade i prenosa podataka u namjeri da se sebi ili drugom pribavi protivpravna imovinska korist i time prouzrokuje imovinska šteta drugom licu.[xviii] Objekt zaštite je bezbjednost računarskih sistema od unošenja netačnih, neistinitih podataka i povjerenje u ove sisteme.

Radnja izvršenja[xix] se sastoji iz dvije alternativno predviđene djelatnosti. To su: (1) prikrivanje i (2) lažno prikazivanje računarskog podatka. Prikrivanje je neunošenje nekog podatka od strane lica koje je obavezno da taj podatak unese u računar ili računarsku mežu. Može se raditi o bilo kakvom podatku. Lažno prikazivanje računarskog podatka postoji kada se u računarskoj mreži prikazuje, objavljuje, unosi ili koristi neistiniti podatak (bilo da je u potpunosti ili djelimično neistinit). Obje djelatnosti moraju biti preduzete u odnosu na podatak koji je po svom značaju, prirodi, karakteru, vremenu unošenja ili upotrebe takav da je podoban da utiče na rezultat (tok i postupak) elektronske obrade i prenosa podataka u računarskom sistemu.

Bilo koja od ovih djelatnosti, u smislu krivičnog djela, mora biti preduzeta na zakonom određeni način: (1) unošenjem netačnog (neistinitog) podatka u cjelini ili djelimično, (2) propuštanjem da se unese, neunošenjem, neupisivanjem kakvog važnog podatka (znači ne bilo kakvog podatka, već samo onog koji je u konkretnom slučaju važan) ili (3) na drugi način. Sve djelatnosti, u smislu radnje izvršenja ovog krivičnog djela, moraju biti preduzete u određenoj namjeri – namjeri da učinilac za sebe ili drugog pribavi protivpravnu imovinsku korist. Ta namjera mora da postoji na strani učinioca u vrijeme preduzimanja radnje, ali ona u konkretnom slučaju ne mora biti i ostvarena. Posljedica djela je povreda koja se ogleda u prouzrokovanju imovinske štete za drugog. Može se raditi o šteti u bilo kom iznosu koja je u uzročno-posledičnoj vezi sa preduzetom radnjom izvršenja, bez obzira na to da li je oštećeni vlasnik ili korisnik računarske mreže.

[xviii] Vidi Turković et al., 345 i 346.
[xix] Vidi Jovašević, Obilježja kompjuterskog kriminaliteta, op. cit., 56-62.

Izvršilac djela može da bude svako lice, a u pogledu krivice je potreban direktni umišljaj koji kvalifikuje navedena namjera. Za ovo djelo je propisana novčana kazna ili kazna zatvora do tri godine. Lakši oblik djela postoji kada je učinilac preduzeo radnju izvršenja – prikrivanje ili lažno prikazivanje podatka u računaru ili računarskoj mreži na zakonom predviđeni način sa namjerom da se drugome nanese šteta, dakle, da se drugo fizičko ili pravno lice ošteti. Maliciozna namjera učinioca da se drugome nanese imovinska ili neimovinska šteta - predstavlja privilegujuću okolnost za koju je zakon propisao novčanu kaznu ili kaznu zatvora do šest mjeseci.

Ovo djelo ima dva teža oblika. Prvi teži oblik djela, za koji je propisana kazna zatvora od jedne do osam godina, postoji ako je usljed preduzete radnje izvršenja osnovnog djela pribavljena imovinska korist (za učinioca ili drugo lice) u iznosu preko 450.000 dinara. Visina pribavljene imovinske koristi predstavlja kvalifikatornu okolnost. Ona se mora nalaziti u uzročno-posljedičnoj vezi sa preduzetom radnjom izvršenja. Drugi teži oblik djela postoji ako je preduzetom radnjom izvršenja učinilac za sebe ili drugog pribavio protivpravnu imovinsku korist u iznosu preko 1.500.000 dinara. Za ovo je djelo propisana kazna zatvora od dvije do deset godina.

4.5. Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka

Sljedeće računarsko djelo iz člana 302 KZ se sastoji u neovlašćenom uključivanju u računar ili računarsku mrežu ili u neovlašćenom pristupu elektronskoj obradi podataka kršenjem mjera zaštite.[xx] Objekt zaštite je bezbjednost računara ili računarske mreže, odnosno sistema elektronske obrade podataka koji su zaštićeni posebnim tehničkim i drugim mjerama zaštite.

Radnja izvršenja je neovlašćeno uključivanje u računar ili računarsku mrežu ili pristup elektronskoj obradi podataka.[xxi] To je ulazak, prodiranje, pristup u zaštićeni sistem računarskih podataka, u sistem elektronske obrade ili prenosa podataka, kao i u računarsku mrežu u cjelini ili njen pojedini dio. Bitno je da se radi o računaru, računarskom sistemu ili sistemu elektronske obrade podataka koji su zaštićeni posebnim mjerama zaštite. Stoga se radnja izvršenja preduzima na određeni zakonom predviđeni način: 1) neovlašćeno i 2) kršenjem mjera zaštite (postupanjem protivno svim propisanim mjerama ili samo pojedinim mjerama, i to činjenjem ili nečinjenjem).

Izvršilac dela može da bude svako lice koje posjeduje određena znanja iz oblasti zaštite računara ili računarskih sistema. U pogledu krivice potreban je umišljaj. Za ovo je djelo propisana novčana kazna ili kazna zatvora do šest mjeseci. Djelo ima dva teža oblika.

Prvi teži oblik djela postoji u slučaju snimanja ili upotrebe računarskog podatka koji je dobijen neovlašćenim uključivanjem u tuđi računar ili računarsku mrežu ili tuđi sistem elektronske obrade podataka pod uslovom da je to učinjeno kršenjem mjera zaštite. Za ovo je djelo propisana novčana kazna ili kazna zatvora do dvije godine. Bez značaja je u kom cilju ili u kojoj namjeri je upotrijebljen na ovaj način pribavljen (snimljen) računarski podatak.

Drugi teži oblik djela, za koji je propisana kazna zatvora do tri godine, postoji ako je neovlašćenim uključivanjem u tuđi računar ili računarsku mrežu ili tuđi sistem elektronske obrade podataka (kršenjem mjera zaštite) pribavljen računarski podatak (jedan ili više njih) koji je potom upotrijebljen usljed čega je došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili mreže ili su nastupile druge teške posljedice za drugo (fizičko ili pravno) lice. Teže posljedice mogu biti imovinske ili neimovinske prirode, ali moraju biti u uzročno-posljedičnoj vezi sa upotrebom podatka do koga se došlo neovlašćenim uključivanjem ili pristupom. Za postojanje ovog težeg djela je bitno da je došlo do nastupanja teže posljedice povrede u vidu zastoja ili ozbiljnog poremećaja funkcionisanja elektronske

[xx] Vidi Jovašević, 2003, 359 i 360.
[xxi] Vidi Turković et al., 341 i 342.

obrade i prenosa podataka ili mreže ili da su nastupile druge teške posljedice. Koje su to teške posljedice, predstavlja faktičko pitanje koje sud rješava u konkretnom slučaju.

4.6. Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži

Krivično delo iz člana 303 KZ se sastoji u neovlašćenom sprečavanju ili ometanju pristupa javnoj računarskoj mreži.[xxii] Objekt zaštite je javna računarska mreža i slobodan pristup toj mreži od strane individualno neodređenog broja lica. Motiv ove inkriminacije je sprečavanje monopola u korišćenju javne računarske mreže.

Radnja izvršenja je sprečavanje ili ometanje slobodnog pristupa javnoj računarskoj mreži.[xxiii] Sprečavanje je onemogućavanje u potpunosti, trajno ili za određeno kraće vrijeme, pristupa drugom licu javnoj računarskoj mreži. To može biti učinjeno fizičkim sprečavanjem, postavljanjem određenih uslova ili prepreka, odnosno zahtijevanjem ispunjenja određenih pretpostavki. Ometanje je djelimično usložavanje, otežavanje, činjenje nedostupnim ili uslovljavanje drugom licu da nesmetano, slobodno, po svom nahođenju pristupi ili koristi javnu računarsku mrežu. Bitno je da se radi o radnji izvršenja koja je preduzeta neovlašćeno (od neovlašćenog lica, mimo uslova i pretpostavki i van postupka koji su zakonom ili drugim propisima iz ove oblasti predviđeni) u odnosu na javnu računarsku mrežu.

Izvršilac djela može da bude svako lice, a u pogledu krivice potreban je umišljaj. Za ovo je djelo propisana novčana kazna ili kazna zatvora do jedne godine. Teži oblik djela, za koji je propisana kazna zatvora do tri godine, postoji ako je radnju izvršenja preduzelo službeno lice u vršenju službe. Svojstvo učinioca djela i način preduzimanja radnje izvršenja - kršenjem ili zloupotrebom službene dužnosti, predstavljaju kvalifikatorne okolnosti za koje zakon propisuje strožije kažnjavanje.

4.7. Neovlašćeno korišćenje računara ili računarske mreže

Krivično djelo iz člana 304 KZ se sastoji u neovlašćenom korišćenju računarske usluge ili računarske mreže u namjeri da se sebi ili drugom licu pribavi protivpravna imovinska korist.[xxiv]

Objekt zaštite je zakonitost i savjesnost u korišćenju računarskih sistema - usluga ili mreže od svih oblika zloupotrebe i nesavjesnosti. Radnja izvršenja je neovlašćeno korišćenje, dakle upotreba, iskorišćavanje podataka koji su pribavljeni ili pohranjeni u računaru ili računarskoj mreži u koristoljubivoj namjeri – namjeri da na ovaj način učinilac za sebe ili drugo fizičko ili pravno lice pribavi protivpravnu (ne bilo kakvu) korist. Ova namjera mora da postoji na strani učinioca u vrijeme preduzimanja radnje izvršenja, ali ona ne mora u konkretnom slučaju da bude i ostvarena.

Izvršilac djela može da bude svako lice, a u pogledu krivice potreban je direktni umišljaj koji karakteriše navedena namjera. Za ovo je djelo propisana novčana kazna ili kazna zatvora do tri mjeseca.

4.8. Pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih djela protiv bezbjednosti računarskih podataka

Ovo je novo računarsko krivično djelo (član 304a KZ) koje je uvedeno novelom KZ iz 2009. godine. Zapravo, ovdje se radi o kažnjivim pripremnim radnjama za izvršenje nekog od računarskih krivičnih djela. Samo djelo se sastoji u posjedovanju, pravljenju, nabavljanju, prodaji ili davanju drugome na upotrebu računara, računarskog sistema, računarskog podatka ili programa za izvršenje nekog od krivičnih djela protiv bezbjednosti računarskih podataka.[xxv] Za ovo je djelo propisana kazna zatvora od šest mjeseci do tri godine, pri čemu se obavezno od učinioca oduzimaju predmeti izvršenja djela - primjenom posebne mjere bezbjednosti oduzimanja premeta.

[xxii] Vidi Jovašević, Obilježja kompjuterskog kriminaliteta, op. cit., 56-62.
[xxiii] Vidi Kitarović, Kompjuterski kriminalitet, op. cit., 52-56.
[xxiv] Vidi Jovašević, 2003, 360 i 361.
[xxv] Vidi Simić, Trešnjev, 213 i 214.

Objekt zaštite je i u ovom slučaju bezbjednost računarskih sistema i podataka, ali koja se obezbjeđuje na specifičan način - prije neposrednog preduzimanja radnje krivičnog djela.

Radnja izvršenja je višestruko alternativno određena. Ona se sastoji u: posjedovanju, pravljenju, nabavljanju, prodaji ili davanju drugome na upotrebu predmeta. Posjedovanje je sama državinska vlast izvršioca nad predmetima, neposredno ili posredno, što uključuje njegovu mogućnost njihovog korišćenja. Pravljenje je izrada novog ili prepravljanje, preinaka postojećeg predmeta. Nabavljanje je dolaženje u posjed, u državinu predmeta. Prodaja je zamjena predmeta za domaći ili strani novac, a davanje na upotrebu drugome je radnja pomaganja kojom se stvaraju uslovi da drugo lice neposredno upotrijebi ove predmete. Bitno je da se radnja izvršenja preduzima: 1) u odnosu na zakonom tačno određene predmete kao što su: računar, računarski sistem, račnarski podatak ili program i 2) u određenoj namjeri - za izvršenje nekog od krivičnih djela protiv bezbjednosti računarskih podataka.

5. Zaključak

Prihvatanjem odredbi niza relevantnih evropskih dokumenata, koji su konačno inaugurisani usvajanjem Konvencije o kibernetičkom kriminalu, u nacionalnim zakonodavstvima država članica Sav,eta Evrope je stvorena pravna osnova za uvođenje posebne vrste „računarskih, kompjuterskih" krivičnih djela koja imaju za cilj da obezbijede efikasno, kvalitetno, zakonito, bezbjedno i uz povjerenje obavljanje različitih poslova i usluga putem računara.

Zapravo, uvođenjem posebnih krivičnih djela obezbjeđuje se bezbjednost računarskih sistema i podataka u nacionalnim i međunarodnim razmerama. Tako je i u Republici Srbiji, počev od 2003. godine, u krivičnopravni sistem uvedeno više krivičnih djela ove vrste pri čemu je zakonodavac, poštujući utvrđene evropske standarde, obezbijedio krivične sankcije za pojedine oblike i vidove ispoljavanja propisanih računarskih krivičnih djela.

Slična krivična djela su sastavni dio i novodonijetog KZ iz 2005. godine. Na taj način, uz odgovarajuće procesne pretpostavke (formiranje posebnih organa za suzbijanje visokotehnološkog kriminala u okviru policije, javnog tužilaštva i suda) stvorene su pretpostavke za efikasnu borbu Republike Srbije sa ovim savremenim oblicima i vidovima kriminaliteta koji ne poznaje granice između država.

6. Literatura

Đurđić, V., Jovašević, D. (2010). *Krivično pravo, Posebni dio.* Beograd: Nomos.

Jovašević, D. (2003). *Komentar Krivičnog zakona Republike Srbije sa sudskom praksom*. Beograd: Nomos.

Kareklas, S.E. (2009). *Priručnik za krivično pravo Evropske unije*. Beograd: Institut za uporedno pravo i Mladi pravnici.

Lazarević, Lj., Vučković, B., Vučković, V. (2004). *Komentar Krivičnog zakonika Crne Gore*, Obod, Cetinje: Obod.

Pavišić, B. (2006). *Kazneno pravo Vijeća Evrope.* Zagreb: Tehnička knjiga.

Simić, I., Trešnjev, A. (2010). *Krivični zakonik s kraćim komentarom*. Beograd: Ing pro.

Turković, K., et al. (2013). *Komentar Kaznenog zakona.* Zagreb: Narodne novine.

Authors: *Dragan Jovašević, PhD; Marina M. Simović, PhD*
Institutions: *(1) Facultfay of Law of University of Niš; (2) Faculty of Law, University „Apeiron" of Banja Luka*

SAFETY OF COMPUTER SYSTEMS IN SERBIA AND EUROPEAN STANDARDS

Abstract

The Republic of Serbia, in its new criminal legislation passed in 2005, provides for criminal responsibility and punishment for several criminal offences against safety of computer data. Those are computer criminal offences done by the perpetrator by computer abuse, thereby causing material or non-material damage to other natural or legal persons. The basis of those incriminations are European standards prescribed under the Convention on Cyber Criminal and Additional Protocol to this Convention, as well as many other European documents. The paper analyses basic characteristics of computer criminal offences in Serbia and the degree of their compatibility with European standards.

Keywords: computer abuse, european standards, crime, responsibility, sanction.