FBIM Transactions
DOI 10.12709/fbim.08.08.01.12

KRIVIČNA DELA PROTIV BEZBEDNOSTI RAČUNARSKIH PODATAKA

CRIMINAL ACTS AGAINST SECURITY OF COMPUTER DATA

Živanka Miladinović Bogavac
Poslovni i pravni fakultet, Univerzitet „Union – Nikola Tesla“, Beograd, Srbija

JEL kategorija rada: **K14**

Apstrakt

Krivični zakonik Republike Srbije u glavi dvadeset i sedmoj propisuje krivična dela koja za svoj zaštitni objekat imaju računarske podatke. Shodno navedenom u ovoj glavi regulisana su sledeća krivična dela: oštećenje računarskih podataka i programa, računarska sabotaža, pravljenje i unošenje računarskih virusa, računarska prevara, neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka, sprečavanje i ograničavanje pristupa javnoj računarskoj mreži, neovlašćeno korišćenje računara ili računarske mreže, i pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka. Ova krivična dela su uvedena u krivično zakonodavstvo Republike Srbije 2003 godine, izmenama i dopunama KZS, izmenama i dopunama KZS, tako što su prihvaćena rešenja iz Nacrta KZ SR Jugoslavije iz februara 2000.godine. Republika Srbija je 2005 godine potpisala Konvenciju o sajber kriminalu Saveta Evrope. U skladu sa preuzetim obavezama, u cilju suzbijanje kompjuterskog kriminaliteta, pored odredbi u Krivičnom Zakoniku Republike Srbije, od značaja su odredbe Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala kojim se, između ostalog predviđa i formiranje specijalizovanih odeljenja u tužilaštvu i MUP-u. U radu će biti analizirana krivična dela protiv bezbednosti računarskih podataka, međusobno razlikovanje i specifičnosti istih, čime će se skrenuti pažnja da li je Republika Srbija u svom zakonodavstvu svoje odredbe prilagodila potpisanoj Konvenciji o sajber kriminalu.

Ključne reči: *krivična dela, bezbednost računarskih podataka, Krivični zakonik Republike Srbije, pravna regulative*

Abstract

The Criminal Code of the Republic of Serbia, in part twenty-seven, prescribes criminal offenses that have computer data for their protective object. Pursuant to this chapter, the following offenses are regulated: damage to computer data and programs, computer sabotage, creation and introduction of computer viruses, computer fraud, unauthorized access to a secure computer, computer network and electronic data processing, preventing and organizing access to a public computer network,

Adresa autora:
Živanka Miladinović Bogavac
zivankamiladinovic@gmail.com

unauthorized use of a computer or computer network, and making, procuring and providing other means of committing criminal offenses against computer data security. These criminal offenses were introduced into the criminal legislation of the Republic of Serbia in 2003, as amended by the CCS, as amended by the CCS, by adopting the decisions of the Draft CC of the Federal Republic of Yugoslavia of February 2000. In 2005, the Republic of Serbia signed the Council of Europe Convention on Cybercrime. In accordance with the undertaken obligations, in order to combat computer crime, in addition to the provisions of the Criminal Code of the Republic of Serbia, the provisions of the Law on Organization and Competence of State Bodies for Combating High-Tech Crime, which, among other things, provide for the establishment of specialized departments in the prosecution and Police. The paper will analyze criminal offenses against the security of computer data, their differentiation and their specificities, which will draw attention to whether the Republic of Serbia has in its legislation adapted its provisions to the signed Convention on Cybercrime.

Keywords: *criminal offenses, computer data security, Criminal Code of the Republic of Serbia, legal regulation*

1 OŠTEĆENJE RAČUNARSKIH PODATAKA I PROGRAMA

U glavi dvanaest Krivičnog zakonika koja nosi naziv ,,značenje izraza" definisani su pojmovi ,,računarski podatak" i ,,računarski program". S tim u vezi, 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, dok se računarskim programom smatra uređeni skup naredbi koji služe za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara. (Krivični zakonik, čl. 112 st. 17 i 19). Upravo, računarski podatak i računarski program su predmet krivičnopravne zaštite u članu 298 Krivičnog zakonika. Radnja izvršenja krivičnog dela oštećenja računarskih podataka se sastoji u brisanju, izmeni, oštećenju, prikrivanju ili na drugi način činjenju neupotrebljivim računarskog podatka ili računarskog programa. Irelevantno je koja je od navedenih radnji izvršenja dovela do posledice ovog krivičnog dela tj. da računarski podaci i programi ne služe svojoj nameni.

Oštećenje računarskog podatka ili programa može biti učinjeno putem uticaja na hardver ili softver računara. Prvi vid predstavlja fizičko delovanje na deo hardvera koji je nosilac predmetnog podatka ili programa. Drugi vid je softversko delovanje putem računara kojim se podatak ili program modifikuju ili brišu. (Miladinović Bogavac, Ž., 2018, str. 122).

Delo ima teži oblik ukoliko je prouzrokovana šteta u iznosu koji prelazi četiristo pedeset hiljada dinara (stav 2), dok najteži oblik (stav 3) postoji ukoliko ta šteta prelazi iznos od milion i petsto hiljada dinara. Za teži oblik zakonodavac je predvideo kaznu zatvorom od tri meseca do tri godine, a za najteži oblik učinilac će se kazniti zatvorom od tri meseca do pet godina.

Međutim, s obzirom na prirodu računarskih podataka ili programa, teško je utvrditi njihovu vrednost tj. štetu koja nastaje njihovim oštećenjem. Problem čini složenijim i činjenica da podatak ili program čija se vrednost utvrđuje više ne postoji, a njeno rekonstruisanje nije moguće. No, veštaci koji će se baviti ovom procenom će uzeti kao odlučujuće važnost podataka ili programa na privatni i profesionalni život oštećenog kao i štetu koja je načinjena u ovim aspektima života oštećenjem računarskog podatka ili programa.

Oštećenje računarskog podatka i programa pored toga što je predviđeno kao zasebno krivično delo, predstavlja i način izvršenja (modus operandi) drugih krivičnih dela. Tada će se neovlašćeno brisanje, izmena, oštećenje, prikrivanje ili na drugi način činjenje neupotrebljivim računarskog podatka ili programa biti tretirano kao način izvršenja drugog krivičnog dela (npr. falsifikovanje isprave),

Uređaji i sredstva kojima je učinjeno krivično delo, ako su u svojini učinioca, oduzeće se.

2 RAČUNARSKA SABOTAŽA

Računarska sabotaža je u Krivičnom zakoniku Republike Srbije definisana na sledeći način: " Ko unese, uništi, izbriše, izmeni, 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 sa namerom da onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte, kazniće se zatvorom od šest meseci do pet godina." (Krivični zakonik RS čl. 299).

Na prvi pogled, ne može se ne uočiti sličnost sa prethodno opisanim krivičnim delom "Oštećenje računarskih podataka ili programa". Zakonodavac je predvideo u oba slučaja kao radnju izvršenja brisanje, izmenu, oštećenje, prikrivanje ili na drugi način činjenje neupotrebljivim računarskog podatka ili programa. Uz to, u oba slučaja bilo koja od navedenih radnji se preuzima neovlašćeno, tj. bez saglasnosti vlasnika računarskog programa ili podatka. Diferencia specifica će u konkretnom slučaju biti namera učinioca. U slučaju računarske sabotaže zahteva se postojanje određene namere koja je usmerena prema državnim organima, javnoj službi, ustanovi, preduzeću ili drugom subjektu, dakle onim subjektima koji imaju poseban društveni značaj. Dakle, krivično delo računarske sabotaže odlikuje specifična namera učinioca krivičnog dela da onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte. S obzirom na nameru, ovo delo se može izvršiti samo sa direktnim umišljajem.

Unošenje, uništenje, brisanje, izmena, oštećenje, prikrivanje ili na drugi način činjenje neupotrebljivim računarskog podatka ili programa nije jedini način izvršenja krivičnog dela računarske sabotaže. U zakonskom tekstu kao drugi vid izvršenja ovog krivičnog dela navodi se uništenje ili oštećenje računara koji se u Zakonu o izmenama i dopunama Krivičnog zakonika, definiše kao svaki elektronski uređaj koji na osnovu programa automatski obrađuje i razmenjuje podatke. (2009, član 25) ili drugog uređaja za elektronsku obradu i prenos podataka.

Dakle ova dva vida izvršenja krivičnog dela računarske sabotaže se razlikuju s obzirom na objekt napada. Prvi oblik ovog krivičnog dela je usmeren na računarski podatak ili program, dok drugi oblik računarske sabotaže kao objekat ima računar ili drugi uređaj za elektronsku obradu i prenos podataka.

U poslednjem, radnja izvršenja se može sastojati u uništenju ili oštećenju računara ili drugog uređaja za elektronsku obradu i prenos podataka sa namerom da se onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove preduzeća ili druge subjekte. Pod uništenjem računara ili drugog uređaja za elektronsku obradu i prenos podataka treba razumeti potpuno menjanje njihovih svojstava u negativnom smislu, tako da oni faktički više i ne postoje, a pod oštećenjem takvo menjanje njihovih svojstava u negativnom smislu koje umanjuje mogućnosti njihove dalje upotrebe u svrhu kojoj su namenjeni. (Stojanović & Perić, 2009, str. 253- 254)

Kako zaključuju Stojanović i Perić, ovim krivičnim delom se pruža zaštita elektronskim sistemima i mrežama za elektronsku obradu i prenos podataka koji imaju poseban društveni značaj. (Stojanović & Perić, 2009, str. 253) Taj društveni značaj je upravo ono što se može postaviti kao specifičnost ovog dela u odnosu na druga kompjuterska krivična dela. Računarska sabotaža se vrši u cilju da se onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte.

Priroda krivičnog dela i objekat zaštite uslovili su i visinu sankcije za ovo krivično delo iz grupe krivičnih dela protiv bezbednosti računarskih podataka, te je predviđena sankcija za ovo krivično delo kazna zatvora od šest meseci do pet godina. Propisujući samo osnovni oblik, za razliku od prethodnog krivičnog dela izostavljeni su kvalifikatorni oblici istog, te i privilegujuće okolnosti koje ćemo razmatrati kod drugih krivičnih dela u okviru ove grupe krivičnih dela.

3 PRAVLJENJE I UNOŠENJE RAČUNARSKIH VIRUSA

Na samom početku analize ovog krivičnog dela neophodno je ukazati na definiciju računarskih virusa datu u članu 112 u delu "značenje izraza": „Računarski virus je računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih

programa ili podataka". (Krivični zakonik Republike Srbije, član 112, st. 20). Brojne su klasifikacije virusa s obzirom na način njihovog prenošenje, dejstva na računar, ciljnoj grupi i slično. U svakom slučaju zakonodavac je prilikom propisivanja ovog krivičnog dela imao na umu njihovo svakodnevno umnožavanje i usavršavanje, te posledice koje izazivaju od sasvim bezazlenih usporavanja rada računara, preko milionskih materijalnih gubitaka i špijunaže (Miladinović Bogavac, Ž, 2017, str. 239).

Osnovni oblik krivičnog dela pravljenje i unošenje računarskih virusa propisano je članom 300 Krivičnog zakonika Republike Srbije: „Ko napravi računarski virus u nameri njegovog unošenja u tuđ računar ili računarsku mrežu, kazniće se novčanom kaznom ili zatvorom do šest meseci". (Krivični zakonik, član 300).

Radnja izvršenja prvog oblika ovog krivičnog dela je samo pravljenje računarskog virusa. Delo je dovršeno kada je računarski virus napravljen u nameri da se unese u tuđ računar ili računarsku mrežu. Ovo delo se može izvršiti samo sa umišljajem.

Pored osnovnog oblika, u Krivičnom zakoniku je predviđen teži oblik u slučaju unošenja računarskog virusa u tuđ računar ili računarsku mrežu čime bi se prouzrokovala šteta. Prilikom izvršenja težeg oblika irelevantno je da li je izvršilac sam napravio računarski virus koji se unosi u računar ili je nabavio isti na drugi način. Ono na čemu kod ovog oblika zakonodavac insistira je nastala šteta, ali ne precizirajući kakvog karaktera. Tumačenje nas navodi da je i usporen rad računara i teškoće pri funkcionisanju računara kao štetna posledica unošenja virusa može biti odlučujuća za postojanje težeg oblika.

Za razliku od prvog oblika (pravljenje virusa) gde je propisana novčana kazna ili kazna zatvora do šest meseci a za teži oblik (širenje virusa) je propisana novčana kazna ili kazna zatvora do dve godine. U stavu 3 člana 300 koje reguliše krivično delo Pravljenja i unošenja računarskog virusa navodi se da će se uređaj i sredstva kojima je učinjeno krivično delo oduzeti.

4 RAČUNARSKA PREVARA

Krivično delo prevara je određeno u Krivičnom zakoniku Republike Srbije u okviru krivičnih dela protiv imovine: "Ko u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist dovede koga lažnim prikazivanjem ili prikrivanjem činjenica u zabludu ili ga održava u zabludi i time ga navede da ovaj na štetu svoje ili tuđe imovine nešto učini ili ne učini, kazniće se zatvorom od šest meseci do pet godina i novčanom kaznom". (član 208)

Međutim u okviru krivičnih dela protiv bezbednosti računarskih podataka zakonodavac definiše i računarsku prevaru kao poseban oblik prevare: „Ko unese netačan podatak, propusti unošenje tačnog podatka ili na drugi način prikrije ili lažno prikaže podatak i time utiče na rezultat elektronske obrade i prenosa podataka u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, kazniće se novčanom kaznom ili zatvorom do tri godine". (član 301 st. 1)

Razlog za zasebno definisanje nalazi se u izostavljanju „dovođenja i održavanja u zabludi nekog lica" kao radnje izvršenja krivičnog dela računarska prevara, za razliku od krivičnog dela prevare.

Prisutno je u laičkim krugovima da se krivično delo računarska prevara se identifikuje sa „Internet prevarama", što navodi na pogrešnu kvalifikaciju dela.

Naime, razne prevare koje su dostupne na Internetu, primera radi: nigerijske prevare, lutrijske prevare, ljubavne prevare i slično podležu regulativi krivičnog dela prevare, a ne računarske prevare. Budući da je kod tzv. Internet prevarama reč o „dovođenju i održavanju u zabludi nekog lica", što kao što smo videli predstavlja radnju izvršenja krivičnog dela prevare.

Radnja izvršenja krivičnog dela računarske prevare je unošenje netačnog podatka, propuštanje da se unese tačan podatak ili prikrivanje na drugi način tačnog podatka ili lažno prikazivanje podatka čime se utiče na rezultat elektronske obrade i prenosa podataka. Shodno navedenom, posledica ovog krivičnog dela će biti u izmenjenom rezultatu elektronske obrade podataka.

Za ovo krivično delo karakteristična je namera da se sebi ili drugome pribavi protivpravna imovinska korist i time drugome prouzrokuje imovinska šteta, te se može izvršiti samo sa umišljajem. Za

dovršeno krivično delo nije potrebno da je ova namera i ostvarena.

U slučaju računarske prevare, kao i kod krivičnog dela prevare, zakonodavac se odlučuje za iznos pribavljene imovinske koristi kao kvalifikatornu okolnost pri propisivanju ostalih oblika. S tim u vezi, teži oblik računarske prevare postoji u slučaju da je pribavljena imovinska korist koja prelazi iznos od četiristo pedeset hiljada dinara. Najteži oblik razlikuje se samo prema visini pribavljene imovinske koristi (milion i petsto hiljada dinara).U prvom slučaju propisana je kazna zatvora od jedne do osam godina, a u drugom zatvor od dve do deset godina.

Zakonodavac je pored osnovnog i 2 kvalifikatorna oblika predvideo i privilegovan oblik ovog krivičnog dela, što možemo uočiti i kod krivičnog dela prevare (čl. 208. st. 2). U oba slučaja, privilegujuću okolnost čini namera da se drugo lice ošteti, bez namere pribavljanja protivpravne imovinske koristi.

5 NEOVLAŠĆENI PRISTUP ZAŠTIĆENOM RAČUNARU

Radnja izvršenja osnovnog oblika je na sledeći način definisana: „Ko se, kršeći mere zaštite, neovlašćeno uključi u računar ili računarsku mrežu, ili neovlašćeno pristupi elektronskoj obradi podataka, kazniće se novčanom kaznom ili zatvorom do šest meseci.”(član 302, st1)

Dakle, radnja izvršenja osnovnog oblika se sastoji u neovlašćenom uključivanju u računar ili računarsku mrežu ili neovlašćeno pristupanje bilo kom drugom načinu elektronske obade podataka i to na taj način što je tom prilikom prekršena neka mera zaštite. Najčešće se mera zaštite ogleda u lozinki („password”) koja je neophodna da bi se pristupilo elektronskoj obradi podataka.

Učinilac ovog dela uglavnom je lice sa dobrim poznavanjem informacionih tehnologija, koje ima stečeno umeće da savlada mere zaštite koje poseduje određeni računar ili računarska mreža.

Subjektivno obeležje bića ovog krivičnog dela jeste umišljaj. Kod osnovnog oblika irelevantna je namera zbog koje vrši ilegalno pristupanje računaru, računarskoj mreži, odnosno elektronskoj obradi podataka.

Pored osnovnog oblika, zakonodavac predviđa i dva teža oblika.

Prvi teži oblik predviđen je u slučaju da se snimi ili upotrebi podatak dobijen prilikom neovlašćenog uključenja u računar ili računarsku mrežu, ili neovlašćenog pristupa elektronskoj obradi podataka. U tom slučaju učinilac će se kazniti novčanom kaznom ili zatvorom do dve godine.

Drugi teži oblik će postojati ako je prilikom izvršenja osnovnog oblika došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili mreže ili su nastupile druge teške posledice. Za najteži oblik ovog oblika krivičnog dela neovlašćenog pristupa zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka predviđena je kazna zatvora do tri godine.

6 SPREČAVANJE I ORGANIČAVANJE PRISTUPA JAVNOJ RAČUNARSKOJ MREŽI

Kako se putem informacionih tehnologija vrši komuniciranje i informisanje građana, cilj zakonodavca je da svojim odredbama ove aktivnosti učini neometanim. Da bi korisnik računara komunicirao i koristio računar za informisanje mora biti deo javne računarske mreže, tj. pristupiti istoj. Računarskom mrežom se smatra skup međusobno povezanih računara koji komuniciraju razmenjujući podatke (član 112 stav 18). Javna računarska mreža jeste ona računarska mreža koja je, pod određenim uslovima dostupna svakome. Ona može biti globalnog (internet), regionalnog ili lokalnog karaktera. Ovo krivično delo ima za cilj kako da zaštiti bezbednost računarskih podataka tako i da učini pristup na računarskoj mreži nepovredivim.

Radnja izvršenja ovog krivičnog dela je sprečavanje ili ometanje pristupa javnoj računarskoj mreži. U slučaju sprečavanja, korisnik javne računarske mreže nije u mogućnosti da ima pristup toj mreži, dok u slučaju ometanja taj pristup otežan. Krivično delo se može izvršiti samo sa umišljajem.

Teži oblik, kao i kod nekih krivičnih dela protiv sloboda i prava čoveka i građanina, postoji ukoliko delo izvrši službeno lice u vršenju svoje službe. Za razliku od osnovnog oblika gde je predviđena novčana kazna ili zatvor do jedne godine, za teži oblik ovog krivičnog dela propisan je zatvor do tri godine.

7 NEOVLAŠĆENO KORIŠĆENJE RAČUNARA ILI RAČUNARSKE MREŽE

Reč je o najčešće vršenom ali i najlakšem krivičnom delu iz grupe krivičnih dela protiv bezbednosti računarskih podataka. Radnja izvršenja ovog krivičnog dela jeste neovlašćeno korišćenje računarskih usluga ili računarske mreže. Ranije se ovo krivično delo manifestovalo putem tzv. krađe internet vremena, odnosno korišćenja Interneta bez plaćanja naknade ovlašćenom provajderu, a u novijem vremenu putem neovlašćenog korišćenja WF mreže. U tom smislu, pasivni subjekt ovog krivičnog dela su korisnici usluga internet-provajdera, a pasivni subjekt mogu biti i sami provajderi.

Na subjektivnom planu neophodan je umišljaj, kao i namera da se sebi ili drugome pribavi protivpravna imovinska korist.

U slučaju da izvršilac višekratno neovlašćeno koristi računarske usluge ili računarsku mrežu, postojaće samo jedno krivično delo. Međutim, u nekim slučajevima ovde neće ni biti potrebe za primenom konstrukcije produženog krivičnog dela jer će se raditi o prirodnom jedinstvu dela .

Nakon definisanja radnje izvršenja ovog krivičnog dela, zakonodavac u stavu 2 istog člana predviđa da se gonjenje za ovo delo, s obzirom na njegovu prirodu i značaj, preduzima se po privatnoj tužbi (stav 2).

8 PRAVLJENJE, NABAVLJANJE I DAVANJE SREDSTAVA ZA IZVRŠENJE KRIVIČNIH DELA

Ovo krivično delo je uvedeno nakon donošenja Zakona o potvrđivanju Konvencije o visokotehnološkom kriminalu (“Službeni glasnik RS” broj 19/09), koja u članu 6. predviđa obavezu strana ugovornica da u svom krivičnom zakonodavstvu kao krivično delo propišu niz radnji koje se odnose na uređaje, uključujući i računarske programe, koji su napravljeni ili prilagođeni prvenstveno u svrhu izvršenja nekog krivičnog dela protiv bezbednosti računarskih podataka predviđenih tom konvencijom.

Radnja izvršenja jeste proizvodnja, prodaja, nabavljanje radi upotrebe, uvoz, distribuiranje ili stavljanje na raspolaganje na drugi način određenih sredstava radi izvršenja krivičnih dela iz čl. 298 do 303 KZ (krivična dela protiv bezbednosti računarskih podataka). Stoga, subjektivni element mora pored umišljaja obuhvatiti i ovu nameru izvršioca da se izvrši krivično delo iz glave Krivična dela protiv bezbednosti računarskih podataka.

Kao predmet radnje izvršenja zakonodavac podrazumeva uređaje i računarske programe projektovane ili prvenstveno namenjene u svrhu izvršenja krivičnog dela kao i računarske šifre i slične podatke putem kojih se može pristupiti računarskom sistemu kao celini ili nekom njegovom delu sa namerom da bude upotrebljen u izvršenju nekog od krivičnih dela.

Osnovni oblik je definisan na sledeći način: „Ko proizvodi, prodaje, nabavlja radi upotrebe, uvozi, distribuira i na drugi način stavlja na raspolaganje:

1. uređaje i računarske programe projektovane ili prvenstveno u svrhe izvršenja nekog krivičnog dela iz čl. 298. do 303. ovog zakonika;
2. računarske šifre ili slične podatke putem kojih se može pristupiti računarskom sistemu kao celini ili nekom njegovom delu sa namerom da bude upotrebljen u izvršenju nekog od krivičnih dela iz čl. 298. do 303. ovog zakonika.“

Za osnovni oblik ovog krivičnog dela zakonodavac predviđa kaznu zatvora od šest meseci do tri godine.

Zakonodavac predviđa i privilegujući oblik ovog krivičnog dela u stavu 2 istog člana u slučaju posedovanja nekog od sredstava, u nameri da ih upotrebi u svrhu izvršenja nekog od krivičnih dela iz čl. 298. do 303. ovog zakonika. U tom slučaju predviđena je novčana kazna ili zatvor do jedne godine.

Mera bezbednosti oduzimanja predmeta propisana je kao obavezna (stav 3).

9 ZAKLJUČNA RAZMATRANJA

Međunarodna zajednica je zbog globalnog karaktera informacione tehnologije kao i ekspanzije njene zloupotrebe zainteresovana za suzbijanje nedozvoljenih ponašanja u ovoj oblasti. Od niza međunarodnih akata posebno treba istaći Konvenciju Saveta Evrope o kompjuterskom kriminalitetu (cyber crime) iz 2001.godine sa Dodatnim protokolom koji sadrži obavezu

kažnjavanja akata rasizma i ksenofobije učinjenih putem kompjutera iz 2003 godine.

Razlog donošenja Konvencije o sajber kriminalu je sprečavanja dela usmerenih protiv poverljivosti, integriteta i dostupnosti kompjuterskih sistema, mreža i kompjuterskih podataka, kao i sprečavanja zloupotrebe tih sistema, mreža i podataka na taj način što će se predvideti kaznene mere za takva činjenja i što će se usvojiti mere dovoljne za efikasnu borbu protiv takvih krivičnih dela, na taj način što će se na unutrašnjem i međunarodnom nivou olakšati otkrivanje, istraga i gonjenje takvih krivičnih dela i što će se obezbediti uslovi za brzu i pouzdanu međunarodnu saradnju; (Konvencija o sajber kriminalu).

Donošenje ove konvencije je uslovljeno potrebom da se obezbedi odgovarajući balans između potrebe za sprovođenjem zakona i poštovanja osnovnih ljudskih prava sadržanih u Konvenciji Saveta Evrope o zaštiti ljudskih prava i osnovnih sloboda iz 1950 godine, Međunarodnoj konvenciji o građanskim i političkim pravima Ujedinjenih Nacija iz 1966 godine, kao i drugim važećim međunarodnim ugovorima o ljudskim pravima koji reafirmišu pravo svakog pojedinca da ima sopstveno mišljenje bez ikakvog ometanja, kao i pravo na slobodu izražavanja, koje obuhvata slobodu da, bez obzira na granice, traži, prima i da sa drugima deli informacije i ideje svih vrsta, i prava koja se tiču privatnosti svakog pojedinca.

Konvencija o sajber kriminalu u prvom delu koje reguliše oblast materijalnog krivičnog prava, propisuje da svaka država članica treba da usvoji takve legislativne i ostale neophodne mere da bi se u njenom nacionalnom pravu okvalifikovala:

1. Krivična dela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema
2. Krivična dela u vezi sa kompjuterima
3. Krivična dela u odnosu na sadržaj
4. Krivična dela koji se odnose na kršenje autorskih i njima sličnih prava

U sastavu odeljka 1 koji propisuje krivična dela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i Sistema, navode se sledeća protivpravna ponašanja koje članice trebaju sankcionisati: nedozvoljeni pristup, nedozvoljeno presretanje, ometanje podataka, ometanje sistema, i zloupotreba uređaja.

U drugom odeljku Konvencije o sajber kriminalu navedena su krivična dela u vezi sa kompjuterima koje su članice u obavezi da sankcionišu: falsifikovanje koje je u vezi sa kompjuterima i prevare koje su u vezi sa kompjuterima.

Krivična dela u odnosu na sadržaj koje države članice moraju predvideti i obezbediti sankcionisanje se pre svega odnose na krivična dela vezana za dečiju pornografiju.

Poslednja kategorija krivičnih dela su krivična dela koji se odnose na kršenje autorskih i njima sličnih prava koje države članice trebaju da usvoje kroz legislativne i ostale mere.

U oblasti sankcionisanja Konvencija upućuje da „Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se omogućilo da krivična dela ustanovljena podležu efikasnim, proporcionalnim i odvraćajućim sankcijama koje obuhvataju i lišenje slobode".

Republika Srbije je potpisala ovu konvenciju 2005 godine, a do ratifikacije još nije došlo. Ova vrsta krivičnih dela su prvi put uvedena u krivično zakonodavstvo 2003. godine izmenama i dopunama KZS, tako što su prihvaćena rešenja iz Nacrta KZ SR Jugoslavije iz februara 2000.godine.

Krivična dela protiv bezbednosti računarskih podataka propisana su na taj način da uglavnom odgovaraju obavezama iz te konvencije. Na adekvatan način su propisana i sadržana u tekstu Krivičnog zakonika: krivična dela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema krivična dela u vezi sa kompjuterima, krivična dela u odnosu na sadržaj i krivična dela koji se odnose na kršenje autorskih i njima sličnih prava.

Može se zaključiti da jedino na adekvatan način nije sprovedena odredba člana 3 Konvencije o sajber kriminalu koja se odnosi na nedozvoljeno presretanje: „Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se u njenom nacionalnom pravu kao krivično delo okvalifikovalo bespravno presretanje prenosa kompjuterskih podataka koji nisu javne prirode, ka kompjuterskom sistemu, od njega ili unutar samog sistema, u šta spada i elektromagnetska emisija iz kompjuterskih sistema kojom se prenose takvi podaci, a kad je učinjeno sa namerom i uz pomoć tehničkih uređaja. Članica može usloviti da delo

mora biti učinjeno sa nečasnim namerama, ili učinjeno u vezi sa kompjuterskim sistemom koji je povezan sa drugim kompjuterskim sistemom."

Od značaja za suzbijanje kompjuterskog kriminaliteta je i Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Službeni glasnik RS", broj 61/05 i 104/09) kojim se, između ostalog predviđa i formiranje specijalizovanih odeljenja u tužilaštvu i MUP-u.

CITIRANA DELA

Krivični zakonik ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr, 107/2005 - ispr, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 i 94/2016)

Konvencija o visokotehnološkom kriminalu (Budimpešta, 23.novembar 2001)

Miladinović Bogavac, Ž. (2017). Pojam, vrste i načini delovanja malicioznih programa kojima se sprovode internet prevare. Časopis za istraživanje medija i društva Medijski dijalozi, X(29), 239.

Miladinović Bogavac, Ž. (2018). Models of committing cyber-criminal offences. Međunarodna naučna konferencija ,,PRAVO 2018" Zbornik radova, Poslovni i pravni fakultet Univerzitet Union Nikola Tesla (str. 122-129). Beograd: ICIM Izdavački centar za industrijski menadžment.

Stojanović, Z., & Perić, O. (2009). Krivično pravo – posebni deo. Beograd.

Datum prve prijave: 07.10.2019.
Datum prijema korigovanog rada: 03.04.2020.
Datum prihvatanja članka: 07.04.2020.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Miladinović Bogavac, Ž. (2020, 04 15). Krivična dela protiv bezbednosti računarskih podataka. (Z. Čekerevac, Ur.) *FBIM Transactions, 8*(1), 119-126. doi:10.12709/fbim.08.08.01.12

*Style – **Chicago** Sixteenth Edition:*

Miladinović Bogavac, Živanka. 2020. „Krivična dela protiv bezbednosti računarskih podataka." Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 8 (1): 119-126. doi:10.12709/fbim.08.08.01.12.

*Style – **GOST** Name Sort:*

Miladinović Bogavac Živanka Krivična dela protiv bezbednosti računarskih podataka [Časopis] // FBIM Transactions / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2020. - 1 : T. 8. - str. 119-126.

*Style – **Harvard** Anglia:*

Miladinović Bogavac, Ž., 2020. Krivična dela protiv bezbednosti računarskih podataka. *FBIM Transactions,* 15 04, 8(1), pp. 119-126.

Style – **ISO 690** Numerical Reference:

Krivična dela protiv bezbednosti računarskih podataka. **Miladinović Bogavac, Živanka.** [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2020, FBIM Transactions, T. 8, str. 119-126.