KOMPARATIVNA ANALIZA KOMPJUTERSKOG KRIMINALA U ZAKONODAVSTVIMA REPUBLIKE SRBIJE I NEKIH STRANIH ZEMALJA

Apstrakt: U radu je napravljen pristup, sa pravnog aspekta, rešavanju problema kompjuterskog kriminala. Pisan je sa ciljem da omogući zakonodavcu, kao i stručnjacima iz oblasti kompjuterske tehnologije kako se nositi sa brojnim zloupotrebama u domenu ove nove sfere kriminala. Ono što je neophodno u suzbijanju te pojave jeste utemeljen i stabilan pravni sistem sa jakom zakonskom regulativom. Takav sistem bi doprineo IKT zaštiti od raznih vidova zloupotreba i ojačao poverenje u pravni sistem, a IKT stručnjaci bi mogli uvoditi nove metode i tehnike zaštite, znajući da su zakonski pokrivene. Bazira se na stanju u našem pravnom sistemu, metodima i regulativama, ali i osvrtu na zakonodavstvo u stranim pravosudnim sistemima i njihov pristup u rešavanju ovog ozbiljnog i rasprostranjenog vida kriminala. Namenjen je, pre svega, pravosudnim organima i ustanovama, koje imaju akcenat na borbu protiv kompjuterskog kriminala.

Ključne reči: Kompjuterski kriminal, zakonodavac, pravni sistem, zakonska regulativa, IKT zaštita, pravosudni organi

1. UVOD

Živimo u modernom informacionom dobu, gde su računari jeftin, a ipak moćan alat koji se može koristiti u sprovođenju brojnih kriminalnih aktivnosti. Kompjuterski kriminal je pojava novijeg vremena. Predstavlja oblik kriminalnog ponašanja, kod koga se korišćenje kompjuterske tehnologije i informacionih sistema ispoljava kao način izvršenja krivičnog dela ili se upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka, u krivično -pravnom smislu, relevantna posledica.

U uslovima nagle ekspanzije i razvoja informaciono - komunikacione tehnologije (IKT), posebno Internet tehnologija, otvoreni su i brojni putevi za potencijalne opasnosti za informacionu imovinu (informacije i druge resurse IKT sistema) pravnih i političkih subjekata. Evidentno je da mogućnost pristupa i upotrebe računara, sa kriminalnim namerama, nesumnjivo može stvoriti bogatstvo vrednih dokaza. U realnom okruženju ne postoji apsolutna zaštita IKT sistema, bilo da su u pitanju napadi sa Interneta, uključujući brojne maliciozne programe ili se radi o napadima ljudskog faktora, poput hakera, krakera, vandala ili kompjuterskih terorista. Dakle, realno ne postoji IKT sistem koji je apsolutno siguran i otporan na kriminalne aktivnosti, jer je ekonomski neopravdan, nerentabilan ili se tako procenjuje.

Kompjuterski kriminal je postao deo našeg svakodnevnog života, iako često nismo ni svesni da se sa njim susrećemo, ili čak u njemu učestvujemo. Danas, gotovo sve informatički razvijene zemlje, kao i one koje to pretenduju da budu, formiraju posebne organe, komisije, komitete, ili radne grupe eksperata koji prate i istražuju kompjuterski kriminal na nacionalnom i međunarodnom planu. Zbog svog specifičnog karaktera, velike društvene opasnosti i visoke stope rasta, u sve većoj meri postaje veoma ozbiljan društveni problem s kojim se treba suočiti društvo u celini, kao i pravni subjekti - organizacije i korporacije. Sve to zaslužuje pažnju države, njenih organa, ali i cele međunarodne zajednice.

Neophodan je odgovarajući zakonski i pravni okvir koji će pravno onemogućiti svaki vid slučajnog, ili namernog narušavanja ili sprečavanja funkcionisanja IKT sistema, kao i uništenje, neovlašćeno menjanje ili korišćenje podataka i informacija. Dakle, reč je o sponi pravne i informacione oblasti, koje zajedničkom saradnjom mogu doprineti uspešnom rasvetljavanju slučaja iz oblasti kompjuterskog kriminaliteta i sankcionisanju počinilaca. U suprotnom, nepostojanje zakonske

regulative predstavlja posebnu teškoću, jer nameće istražnim organima ponekad i pretešku obavezu da slučajeve kompjuterskog podvode pod standarde forme klasičnog kriminala.

2. KOMPJUTERSKI KRIMINAL U ZAKONODAVSTVU REPUBLIKE SRBIJE 2.1. Vrste kompjuterskog kriminala

Krivičnim zakonikom Republike Srbije 2005 godine, u naš pravni sistem uvedena su kompjuterska krivična dela [3]. U Glavi XXVII pomenutog Zakonika predviđena su krivična dela protiv bezbednosti računarskih podataka. Time se ujedno i naša zemlja pridružila nizu zemalja koje se odgovarajućim preventivnim i represivnim merama pokušavaju suprotstaviti različitim oblicima i vidovima zloupotrebe kompjutera.

2.1.1. Oštećenje računarskih podataka i programa

Predviđeno je kažnjavanje za svako lice koje neovlašćeno izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljenim računarski podatak[1] ili računarski program.[2] Delo se može učiniti samo u odnosu na računarski podatak ili program koji pripada nekom fizičkom licu - pojedincu (kao napadni objekt) i to sa više alternativno predviđenih delatnosti. Zapravo, cilj preduzimanja ovih delatnosti je onesposobljavanje za korišćenje, u potpunosti ili delimično, računarskih podataka (jednog ili više njih) ili programa. Posledica se sastoji u povredi zaštićenog dobra. Može ga učiniti svako lice, koje će se kazniti novčanom kaznom ili kaznom zatvora do jedne godine, a u pogledu vinosti[3] potreban je umišljaj.[4]

Zakonom je predviđeno kažnjavanje za ovo krivično delo i to ukoliko je delom prouzrokovana šteta u iznosu koji prelazi četristopedeset hiljada dinara, učinilac će biti kažnjen kaznom zatvora od tri meseca do tri godine, a ukoliko je prouzrokovana šteta u iznosu koji prelazi milion i petsto hiljada dinara učinilac će se kazniti zatvorom od tri meseca do pet godina.

„Računarski podatak"predstavlja informaciju, znanje, činjenicu, koncept ili naredbu, koja se unosi, obrađuje ili pamti ili je uneta, obrađena ili zapamćena u računaru ili računarskoj mreži „Računarskiprogram "je uređen skup naredbi koji služi za upravljanje radom računara, kao i za izvršavanje određenih zadataka pomoću računara
„Vinost" (krivica) postoji ako je učinilac u vreme kada je učinio krivično delo bio uračunljiv i postupao sa umišljajem, a bio je svestan ili je bio dužan i mogao biti svestan da je njegovo delo zabranjeno „Umišljaj" pretpostavlja da je učinilac bio svestan svog dela i hteo njegovo izvršenje ili kada je učinilac bio svestan da može učiniti delo pa je na to pristao

2.1.2. Računarska sabotaža

Krivično delo računarske sabotaže predviđa kažnjavanje kaznom zatvora od šest meseci do pet godina za svako lice koje unese, uništi, izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program i uništi, 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. Objekt napada je dvojako određen. Prvo, to je računarski podatak ili program, ali i računar odnosno drugi uređaj za elektronsku obradu ili prenos podataka. Drugo, objekti moraju da pripadaju državnom organu, javnoj službi ili drugim pravnim licima kao što su ustanove, preduzeća ili druge organizacije.

2.1.3. Pravljenje i unošenje računarskih virusa

Predstavlja vrstu krivičnog dela koje ima osnovni i teži oblik. Osnovni oblik čini lice koje napravi računarski virus[5] u nameri da ga unese u tuđi računar ili računarsku mrežu.[6] Radnja izvršenja je sačinjavanje, pravljenje virusa. Šta su to virusi, kako se prave, koje su njihove vrste ili karakteristike, svrha i sadržina, predstavljaju pitanja koja sudsko veće mora da reši u svakom konkretnom slučaju kao faktičko pitanje. U tome im stručnu pomoć pružaju lica sa posebnim znanjima i veštinama - u pitanju su veštaci informatičke struke. Delo je svršeno samim momentom pravljenja virusa u nameri da se unese u tuđi računar ili sistem bez obzira da li je takva namera i

ostvarena u konkretnom slučaju ili ne, a predviđena kazna je novčana ili kazna zatvora do šest meseci Ukoliko je ipak tako sačinjeni virus i unet, čime je prouzrokovana bilo imovinska bilo neimovinska šteta, radi se o težem obliku krivičnog dela, za koje je predviđena odgovarajuća novčana kazna ili kazna zatvora do dve godine.

2.1.4. Računarska prevara

U zavisnosti od visine pribavljene imovinske koristi za učinioca ili neko drugo lice, Zakon razlikuje dva oblika krivičnog dela. Osnovni oblik čini svako lice koje unese netačan podatak, propusti unošenje tačnog ili na neki drugi način prikrije ili lažno prikaže podatak, čime utiče na rezultat obrade i prenosa podataka u cilju pribavljanja imovinske koristi ili nanošenja imovinske štete drugome. Predviđena kazna je novčana ili kazna zatvora do tri godine. Postoji odredba po kojoj će se učinilac kazniti kaznom zatvora od jedne do osam godina ukoliko pribavljena korist prelazi iznos od četristopedeset hiljada dinara, odnosno kaznom zatvora od dve do deset godina ukoliko prelazi iznos od milion i petsto hiljada dinara. Učinilac koji ima nameru da drugog ošteti snosiće ili novčanu ili kaznu zatvora do šest meseci. Poseban oblik računarske prevare postoji kada je radnja krivotvorenja, prikrivanja ili lažnog prikazivanja podataka preduzeta u nameri da se drugom licu nanese kakva šteta. Ta šteta ne mora da nastupi u konkretnom slučaju, ali mora da bude pobuda, odnosno unutrašnji pokretač učinioca za preduzimanje radnje izvršenja. Može se raditi o imovinskoj, ali i o drugim vidovima neimovinske štete. Ono što karakteriše kompjuterske prevare jeste činjenica da daleko dopiru zbog veličine Interneta kao tržišta, da se brzo šire,

„Računarski virus" je računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu, koji je napravljen da 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 „Računarska mreža" je skup međusobno povezanih računara koji komuniciraju razmenjujući podatke

kao i izuzetno niski troškovi izvođenja takvih vrsta prevara. Kompjuterski prevaranti zloupotrebljavaju upravo one karakteristike Cyber-prostora koje doprinose rastu elektronske trgovine: anonimnost, distanca između prodavca i kupca i trenutna priroda transkacija. Uz to, koriste prednost činjenice da prevara preko Interneta ne zahteva pristup do nekog sistema za isplatu, kao što to zahteva svaka druga vrsta prevare i što je digitalno tržište još uvek nedovoljno uređeno i kao takvo konfuzno za potrošače, što predstavlja skoro idealne uslove za prevaru.

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

Delo ima osnovni i dva teža oblika ispoljavanja. Osnovni oblik čini lice koje kršeći mere zaštite neovlašćeno pristupi računaru ili računarskoj mreži. Dakle, radnja izvršenja jeste pristupanje, ulazak, upad u tuđi računar ili mrežu. Bitno je d a j e radnja preduzeta neovlašćeno, kršenjem predviđenih mera zaštite, a okolnosti moraju biti obuhvaćene umišljajem učinioca dela. Prvi teži oblik čini lice koje upotrebi podatak koji je pribavio, do koga je došao neovlašćenim pristupom zaštićenom računaru ili mreži. Ako je, pak, usled preduzete radnje došlo do nastupanja teških posledica za drugog radi se o najtežem krivičnom delu ove vrste za koji je zakon propisao kaznu. Bitno je da je posledica, i to teška, nastupila za drugog i da između nje i preduzete radnje upada u zaštićeni računarski sistem postoji uzročno - posledična veza. Krivičnim zakonikom je predviđena novčana ili kazna zatvora do šest meseci za svako lice koje kršeći mere zaštite, neovlašćeno uključi računar ili mrežu ili pristupi elektronskoj obradi podataka. Za lica koja upotrebe dobijene podatke na ovaj način predviđena je novčana ili kazna zatvora do dve godine, a ukoliko je usled dela došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili mreže učinilac će se kazniti zatvorom do tri godine.

2.1.6. Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži

U pitanju je krivično delo gde je objekt napada javna računarska mreža. Ima osnovni i teži oblik. Osnovni oblik čini lice koje neovlašćeno sprečava ili ometa pristup javnoj računarskoj mreži, a predviđena kazna je novčana ili kazna zatvora do jedne godine. U slučaju da se kao učinilac javi