PRILAGOĐAVANJE PRAVNE REGULATIVE AKTUELNIM TRENDOVIMA U REGIONU

Priredio: Redovni profesor dr Milorad Bejatović

ADAPTING LEGAL REGULATIONS TO CURRENT TRENDS IN THE REGION

Edited by: Full Professor Milorad Bejatović, PhD

Pravni fakultet za privredu i pravosuđe
Univerzitet Privredna akademija Novi Sad
Faculty of Law for Business and Justice
University Business Academy Novi Sad

Novi Sad 2015.

Zbornik referata sa međunarodnog naučnog skupa održanog
od 24. – 26. septembra 2015. godine u Novom Sadu
u organizaciji Pravnog fakulteta za privredu i pravosuđe
Univerziteta Privredna akademija u Novom Sadu.

Izdavač:
Pravni fakultet za privredu i pravosuđe
Univerziteta Privredna akademija u Novom Sadu,
Geri Karolja br. 1, telefon: 021 400 – 499
Web: www.pravni-fakultet.info

Recezenti:
Prof. dr Milorad Bejatović
Prof. dr Mirko Kulić
Prof. dr Dragan Mrkšić
Prof. dr Bora Čejović
Prof. dr Miroslav Vitez
Prof. dr Milan Počuča
Prof. dr Milutin Đuričić
Prof. dr Zoran Pavlović
Prof. dr Ivan Joksić
Doc. dr Predrag Mirković

Za izdavača:
Prof. dr Marko Carić

Urednik:
Prof. dr Milorad Bejatović

Štampa:
Štamparija FELJTON, Novi Sad

Tiraž: 150

ISBN 978-86-6019-058-3

Štampanje Zbornika podržao
Sekretarijat za nauku i tehnološki razvoj AP Vojvodine

Članovi Programskog odbora:

Prof. dr Marko Carić
Dekan Pravnog fakulteta za privredu i pravosuđe u Novom Sadu,
Univerziteta Privredna akademija, Republika Srbija
Prof. dr Milorad Bejatović
Profesor Pravnog fakulteta za privredu i pravosuđe u Novom Sadu, Republika Srbija
Akademik prof. dr Miodrag Simović
Potpredsednik Ustavnog suda Bosne i Hercegovine
Prof. dr Borce Davitovski
Ss. Cyril nad Methodeus University, Republic of Macedonia
Prof. dr Kostadin Pušara
Predsednik Udruženja Lobista Crne Gore
Profesor Univerziteta Alfa u Beogradu, Republika Srbij**a**
Prof. dr Bora Čejović
Predsednik Krivičara Srbije
Prof. dr Miroslav Vitez
Ekonomski fakultet u Subotici, Republika Srbija
Prof. dr Dragan Mrkšić
Fakultet tehničkih nauka u Novom Sadu, Republika Srbija
Prof. dr Branko Vučković
Predsednik Osnovnog suda u Kotoru, Republika Crna Gora
Čedomir Backović
Pomoćnik ministra pravde Republike Srbije
Doc. dr Mirko Smoljić
Veleučilište „Lavoslav Ružička" u Vukovaru, Republika Hrvatska
Prof. dr Rok Lampe
Research Institute of European Faculty of Law in Nova Gorica, Republic of Slovenia
Sebastian Spinei
Faculty of Law, University „Lucian Blaga", Sibiu, Romania
Igor Denisov Yurevich
Vice President for Development at the Federal State Educational Institution of
Higher Professional Education, Omsk State Institute of Service, Russia

Članovi Organizacionog odbora:
Prof. dr Milorad Bejatović
Prof. dr Mirko Kulić
Doc. dr Predrag Mirković
Doc. dr Darko Golić
Dr. Dragan Grahovac

Sekretar skupa:
Msr Nenad Stefanović

UDK: 004.042(497.11)

Dr Ivan Joksić / Ivan Joksic, PhD
Vanredni profesor na Pravnom fakultetu za privredu i pravosuđe
Univerzitet Privredna akademija u Novom Sadu
Associate Professor at Faculty of Law, University Business Academy in Novi Sad
E – mail: ijoksic@hotmail.rs

Mr Vidoje Mitrić / Vidoje Mitric, LL.M.
Sudija Višeg suda / Superior Court Judge
E – mail: vidoje.mitric@gmail.com

Dr Vesna Rajaković / Vesna Rajakovic, PhD
Pravni fakultet za privredu i pravosuđe
Univerzitet Privredna akademija u Novom Sadu
Faculty of Law, University Business Academy in Novi Sad
E – mail: vesnarajakovic@yahoo.com

BEZBEDNOST RAČUNARSKIH PODATAKA U KRIVIČNOM ZAKONODAVSTVU REPUBLIKE SRBIJE

Security of Computer Data in Criminal Legislation of the Republic of Serbia

A p s t r a k t

Informacione tehnologije predstavljaju važno područje društvenog i ličnog života svakog čoveka. Prednosti koje pruža visok nivo razvoja informacionih tehnologija, u čijem se središtu nalaze računarski podaci, omogućavaju efikasniji način komuniciranja i prenošenja podataka. Nagli razvoj interneta omogućio je čitavu lepezu mogućnosti na planu ličnog usavršavanja i razvijanja poslovnih, naučnih, medijskih i drugih sadržaja. Međutim, iskazane prednosti informacionih tehnologija uslovile su pojavljivanje različitih vrsta zloupotreba čija su meta pojedinci, pravna lica a na kraju i same državne institucije. Otuda dolazi do nastanka posebne vrste kriminaliteta poznatije kao sajber kriminalitet.

S obzirom da je krivično pravo najpozvanije da pruži efikasnu zaštitu društva od kriminaliteta pojavila se potreba za uvođenjem posebne vrste odnosno grupe krivičnih dela kojima se štiti bezbednost računarskih podataka. U krug ovih krivičnih dela ulaze naoko raznorodna krivična dela koja povezuje jedinstvo grupnog objekta zaštite. Reč je o krivičnim delima kojima se propisuje šira inkriminaciona zona u čijim okvirima se narušava bezbednost računarskih podataka. Stoga je važno ukazati na grupna i pojedinačna obeležja ovih krivičnih dela uvažavajući pritom njihove specifičnosti.

Ključne reči: *informacione tehnologije, računarski podaci, program, virus.*

Abstract:

Information technology represents an important area of social and personal life of every man. Benefits provided by the high level of development information technology, in the center of which are computer data, enabling a more efficient way of communicating and transmitting data. The rapid development of the Internet has enabled a whole range of possibilities in the field of personal development and the development of business, scientific, media and other content. However, the reported benefits of information technologies have caused the appearance of different types of abuse that targeted individuals, legal entities and finally the very state institutions. Hence comes to the formation of special type of crime known as cyber crime.

Since criminal law gives the main responsibility to provide effective protection of society against crime there was a need for the introduction of specific types or groups of criminal acts against the security of computer data. The circle of these crimes are included seemingly diverse offenses that connects the unity of group facility protection. It is about the crimes that prescribe wider zone incrimination within which undermines the security of computer data. Therefore, it is important to point out group and individual characteristics of these offenses taking into account all their specific features.

Keywords: *information technology, computer data, program, virus.*

UVODNA RAZMATRANJA

Pojava i razvoj računara se vezuje za drugu polovinu prošlog veka. To se, pre svega, odnosi na prva tehnička otkrića koja u sebi sadrže upotrebu tzv. "pametnih uređaja". Oni su omogućavali, do tada, neslućene mogućnosti obrade tehničkih podataka kojima se vremenski skraćuje postupak obrade podataka ručnim putem. Vest o prednostima novih mašina koje zamenjuju rad velikog broja ljudi brzo se širila u naučnom i poslovnom svetu. Otuda, u istorijskom smislu posmatrano, celokupan razvoj računara i informacionih tehnologija možemo podeliti u tri osnovne faze, koje se vezuju za vremenske periode njihovog pojavljivanja i upotrebe.

Prva faza razvoja obuhvata upotrebu računara velikih dimenzija čije korišćenje je bilo rezervisano za mali broj stručnih ljudi. U ovoj fazi je korišćen prvi elektronski kompjuter opšte namene, poznatiji kao ENIAC (*Electronic Numerical Integrator and Computer*). Ovu fazu odlikuje odsustvo šire upotrebe računara usled njihovih velikih dimenzija, visoke cene, izostanka masovnije proizvodnje i malog broja ljudi koji ih mogu koristiti.

Druga faza počinje sa pojavljivanjem ličnih računara koji su bili dostupni malom broju korisnika. Njih čine fizički značajno smanjeni aparati uz istovremeno povećanje softverskih kapaciteta u delu koji se odnosi na prostor za skladištenje podataka i brzinu njihove obrade. Ova faza traje sve do pojave interneta sa kojim kreće hipermasovna upotreba ličnih računara na poslu i kod kuće.

Treća faza obuhvata savremeno doba koje možemo označiti kao vreme tehnike u svim sferama društvenog života, počev od profesionalnog angažovanja, održavanja komunikacija, zabave i različitih vrsta zloupotreba računara u kriminalne svrhe. Otuda se pod objedinjenim nazivom "računari" smatraju: tzv. PC računari, mobilni telefoni (androidi), tableti, laptopovi i dr.

Posebnost masovne upotrebe računara i informacionih tehnologija otvara pitanje njihovog daljeg razvoja. Međutim, odgovor nije jednostavno dati jer tzv. pametni uređaji, u kojima su integrisani računari odnosno procesori, osvajaju svetsko tržište robe. Reč je o uređajima za kućnu upotrebu (televizori, frižideri, štednjaci i dr.) koji imaju ugrađene višefunkcionalne displeje. Interesantno je zapaziti da trend upotrebe računara seže u samo korišćenje poslovnih objekata i stanova, koji su audio-vizuelno iskontrolisani uz mogućnost programiranog uključenja gotovo svih uređaja. Na taj način se postiže ušteda i energije i vremena za obavljanje osnovnih operacija kojima ranije nije bilo moguće upravljati bez prisustva samog čoveka.

Koristi koje sa sobom donosi masovna upotreba računara u svim sferama ličnog, porodičnog i društvenog života počela je da uzima svoj danak. To se ogleda u zloupotrebi računara i informacionih tehnologija zarad ostvarenja ličnih, a ponegde i državnih odnosno nacionalnih interesa. Ovim postupcima se počinju ostvarivati višestruke koristi izražene u milionskim iznosima na strani onih koji narušavaju bezbednost računarskih podataka fizičkih i pravnih lica. To je posebno izraženo u sferi elektronskog plaćanja u privredi i bankarstvu gde su prevare bile najprisutnije. Otuda se u našem krivičnom zakonodavstvu uvode prve inkriminacije kojima se štiti bezbednost računarskih podataka.

OPŠTA OBELEŽJA KRIVIČNIH DELA PROTIV BEZBEDNOSTI RAČUNARSKIH PODATAKA

Krivična dela kojima se inkriminišu postupci kojima se narušava bezbednost računarskih podataka premijerno su uvedena u naše krivično zakonodavstvo promenama Krivičnog zakona Srbije iz 2003. godine.[1] Ovim krivičnim delima nije u potpunosti obuhvaćeno područje na kome se preduzimaju radnje protiv bezbednosti računarskih podataka, uključujući i različite oblike zloupotrebe informacionih tehnologija. Uporedo sa daljim razvojem računara i proširenjem broja njihovih korisnika, pojavom socijalnih mreža (fejsbuk, tviter i dr.), dolazi do ozbiljnijeg narušavanja bezbednosti računarskih podataka pravnih i fizičkih lica. Otvaraju se nove tehničke mogućnosti, kako za vršenje postojećih, tako za pojavu novih krivičnih dela koja se vrše zloupotrebom interneta. Otuda je kriminalitet, koji se vrši uz pomoć interneta, moguće definisati kao "izvršenje krivičnih djela

1 Zakon o izmenama i dopunama Krivičnog zakona Republike Srbije, Službeni glasnik RS, br. 39/03.

koje za svoj subjekat i objekat imaju Internet kao Globalnu računarsku mrežu i koja čine informatički obučena lica u cilju izazivanja štetnih posljedica ili pribavljanja protivpravne imovinske koristi".[2]

Donošenjem novog Krivičnog zakonika Srbije iz 2005. godine, krivičnopravna scena je obogaćena novim inkriminacijama na području bezbednosti računarskih podataka. Pored postojećih, uvode se nova krivična dela u okviru posebne glave XXVII važećeg Krivičnog zakonika Srbije, pod nazivom "Krivična dela protiv bezbednosti računarskih podataka".[3] S obzirom da je u pitanju specifična pravna materija, radi lakšeg razumevanja osnovnih pojmova, zakonodavac je u članu 112. KZS dao njihovo autentično značenje. Reč je o više različitih pojmova koji se jedino koriste u inkriminacijama ovih krivičnih dela, što ukazuje na složenost visokotehnološkog kriminaliteta, u smislu kompleksnosti i komplikovanosti ove materije, koja zahteva dodatna znanja.[4] Pod tim se podrazumevaju sledeći pojmovi:

- Pokretnom stvari se smatra i svaka proizvedena ili sakupljena energija za davanje svetlosti, toplote ili kretanja, telefonski impuls, kao i računarski podatak i računarski program (član 112. stav 16. KZS),

- 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 (član 112. stav 17. KZS),

- Računarskom mrežom smatra se skup međusobno povezanih računara, odnosno računarskih sistema koji komuniciraju razmenjujući podatke (član 112. stav 18. KZS),

- Računarskim programom smatra se uređeni skup naredbi koji služe za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara (član 112. stav 19. KZS),

- 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 (član 112. stav 20. KZS),

- Računar je svaki elektronski uređaj koji na osnovu programa automatski obrađuje i razmenjuje podatke (član 112. stav 33. KZS),

2 Stamenković, B. et al. (2014). Visokotehnološki kriminal (praktični vodič kroz savremeno krivično pravo i primjere iz prakse), Podgorica, OEBS Misija u Crnoj Gori, str. 4.

3 Krivični zakonik Republike Srbije, Službeni glasnik RS, br. 85/05-121/12.

4 Vidi: Čejović, B., Kulić, M., (2014). Krivično pravo, Novi Sad, Privredna akademija, str. 504.

- 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 (član 112. stav 34. KZS).

Pored Krivičnog zakonika, u odredbama Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, dat je opšti pojam ove vrste kriminaliteta.[5] Prema odredbi člana 2. ovog Zakona, visokotehnološki kriminal "predstavlja vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku. Pod proizvodima u elektronskom obliku posebno se podrazumevaju računarski programi i autorska dela koja se mogu upotrebiti u elektronskom obliku". Ostali izrazi, koji se koriste u ovom Zakonu, imaju značenje koje im daje Krivični zakonik u prethodno citiranim odredbama člana 112.

Posebnost visokotehnološkog kriminaliteta, pa samim tim i krivičnih dela kojima se štiti bezbednost računarskih podataka, ogleda se u otežanom načinu njegovog suzbijanja. Tako se neki od problema sa kojima se policija susreće na području ovog kriminaliteta odnose na:[6]

– Tehničku opremljenost i osposobljenost policijskih službenika vezanih za otkrivanje izvršilaca u *On-line* okruženju.

– Pravnu regulativu koja nije u skladu sa savremenim oblicima izvršenja krivičnih dela iz oblasti visokotehnološkog kriminala, pri čemu se vrlo često javlja potreba za usklađivanjem postojećih zakonodavnih rešenja pravnim propisima koji bi pratili promene u tehničkoj strukturi i savremene tokove u razvoju informacionog društva.

– Nedostatak operacionalnih obuka koje bi omogućile da policijski službenici koji se bave sprečavanjem visokotehnološkog kriminala budu dovoljno obučeni i tehnički opremljeni za vršenje ovih zadataka.

– Veoma velike poteškoće u otkrivanju izvršilaca krivičnih dela koji koriste lažne identitete u *On-line* okruženju, posebno kada se u obzir uzme činjenica da je u velikom broju slučajeva međunarodna policijska saradnja loša, a da u nekima čak i ne postoji.

– Poteškoće u otkrivanju tačne lokacije izvršenja krivičnog dela, pošto se ova krivična dela vrše sa mnogih mesta širom sveta, a u velikom broju slučajeva izvršioci krivičnih dela koriste mreže sa javnim pristupom.

5 Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala Republike Srbije, Službeni glasnik RS, br. 61/05 i 104/09.

6 Prema: Urošević, V. et al., (2015). Policija i visokotehnološki kriminal – primeri iz prakse i problemi u radu MUP-a Republike Srbije u: Slobodan R. Petrović (urednik) Zloupotreba informacionih tehnologija i zaštita, Beograd, Udruženje sudskih veštaka za informacione tehnologije IT Veštak, str. 358.

Uvođenju inkriminacija kojima se štiti bezbednost računarskih podataka prethodilo je donošenje Konvencije Saveta Evrope o kompjuterskom kriminalitetu (*cyber crime*) iz 2001. godine. Konvencijom se predviđa uvođenje: krivičnih dela kojima se štite računarski podaci, krivičnih dela vezanih za dečiju pornografiju i dr. Pored odgovornosti za svršena krivična dela, predviđena je odgovornost i za podstrekavanje i pokušaj. Zajednički imenitelj ove grupe krivičnih dela odnosi se na korišćenje kompjuterske tehnologije i informacionih sistema kao sredstva njihovog izvršenja. Otuda ovu grupu krivičnih dela karakteriše specifičan način i sredstvo izvršenja, jer se ona vrše upotrebom računara, ili uz pomoć računara ili posredstvom računara.[7]

Ovu grupu čini ukupno osam krivičnih dela i to: oštećenje računarskih podataka i programa (član 298. KZS); računarska sabotaža (član 299. KZS); pravljenje i unošenje računarskih virusa (član 300. KZS); računarska prevara (član 301. KZS); neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (član 302. KZS); sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 303. KZS); neovlašćeno korišćenje računara ili računarske mreže (član 304. KZS); pravljenje, nabavljanje i davanje sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka (član 304a KZS). Svako od navedenih krivičnih dela podrazumeva korišćenje računara i računarske mreže radi narušavanja bezbednosti računarskih podataka. Međutim, ova krivična dela se razlikuju prema načinu izvršenja, konkretno korišćenom sredstvu, obliku krivice (negde se traži prisustvo posebne namere kod učinioca), svojstvu učinioca i dr. Zato je neophodno ukazati na osnovne karakteristike svakog od pojedinačno navedenih krivičnih dela.

Oštećenje računarskih podataka i programa (član 298. KZS)

Ovo krivično delo ima više oblika od kojih jedan pripada osnovnom a druga dva težim oblicima. Pritom se teži oblici razlikuju od osnovnog po visini nastupele štete.

Osnovni oblik ovog krivičnog dela vrši onaj ko neovlašćeno izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program (stav 1.). Da bi krivično delo bilo učinjeno dovoljno je (neovlašćeno) preduzeti jednu od više alternativno postavljenih radnji izvršenja.

Prvi *teži oblik* krivičnog dela se sastoji u prouzrokovanju štete u iznosu koji prelazi četiristopedeset hiljada dinara (stav 2). Drugi *teži oblik* se sastoji u prouzrokovanju štete u iznosu koji prelazi milion i petsto hiljada dinara (stav 3.).

Zakonodavac je predvideo da se uređaji i sredstva, kojima je učinjeno krivično delo, oduzimaju ako su u svojini učinioca. Reč je o sredstvima koja su omogućila učiniocu da izvrši ovo krivično delo što se, po prirodi stvari, odnosi na

7 Babić, M., Marković, I., (2013). Krivično pravo-posebni dio, Banja Luka, Pravni fakultet, str. 262.

upotrebljenu računarsku tehniku. U krug izvršilaca ovog krivičnog dela može se uvrstiti svako lice.

Računarska sabotaža (član 299. KZS)

Ovo krivično delo ima samo jedan oblik. Može se izvršiti na više različitih načina, tako što učinilac: 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. Radnja izvršenja mora biti preduzeta 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. U pogledu oblika krivice predviđen je umišljaj, uz postojanje posebne namere, dok krivično delo može učiniti bilo koje lice.

Pravljenje i unošenje računarskih virusa (član 300. KZS)

U samom nazivu krivičnog dela možemo uočiti dva oblika njegovog izvršenja. Oni se razlikuju u delu koji se odnosi na preduzimanje radnje izvršenja u određenoj nameri ili pak ostvarenju ove namere i prouzrokovanju štete.

Prvi oblik se sastoji u pravljenju odnosno proizvodnji računarskih virusa u nameri da se isti unese u tuđ računar ili računarsku mrežu. Pod računarskim virusom možemo označiti poseban tip računarskih programa, koji mogu sebe reprodukovati, koji se šire tajno, koji *inficiraju* druge programe, kao bi se na taj način izvršio cilj koji je unapred postavio tvorac virusa. Reč je o stručnom terminu pod kojim se podrazumevaju određeni podaci koje učinilac krivičnog dela, rukovođen različitim pobudama, ubacuje u tuđ računar ili računarsku mrežu čime se izazivaju poremećaji u njihovom funkcionisanju.[8]

Drugi oblik obuhvata samo unošenje računarskog virusa u tuđ računar ili računarsku mrežu čime se prouzrokuje šteta. Ovde je za postojanje svršenog krivičnog dela neophodno da je do štete zaista došlo, tj. da je šteta nastupila. Šteta može nastati kako za drugog, tako i na samom računaru i računarskoj mreži, s tim što je bez značaja o kakvoj se šteti radi.[9]

Iako se načelno smatra da izvršilac ovog krivičnog dela može biti svako lice, činjenica je da se krug njegovih mogućih izvršilaca kreće u kategoriji vrsnih poznavalaca računarskih i internet tehnologija. Što se tiče oblika krivice predviđeno je postojanje umišljaja uz postojanje posebne namere koja se razlikuje kod dva njegova osnovna oblika.

8 Lazarević, Lj., (2011). Komentar Krivičnog zakonika, Beograd, Pravni fakultet Union, str. 882-883.

9 Ibid., str. 883.

Računarska prevara (član 301. KZS)

Ovo krivično delo u sebi sadrži jedan osnovni, dva teža i jedan poseban oblik. Sve njih povezuje prevarno postupanje učinioca koje se različito tretira u zavisnosti od konkretno predviđenih oblika.

Osnovni oblik krivičnog dela postoji kada se 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. Bitno je da je učinilac preduzeo neku od alternativno propisanih radnji u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist i time prouzrokuje imovinsku štetu. Za postojanje osnovnog oblika se ne određuje visina ostvarene koristi ili nastupele štete.

Teži oblici ovog krivičnog dela se razlikuju po visini protivpravno pribavljene imovinske koristi. U *prvom slučaju* se traži da je visina ostvarene koristi prešla iznos od četiristo pedeset hiljada dinara dok je u *drugom slučaju* reč o iznosu koji prelazi milion i petsto hiljada dinara. Najzad, zakonodavac je predvideo poseban (privilegisani) oblik ovog krivičnog dela, kada se ono učini samo u nameri da se drugi ošteti. Dakle, kod ovog oblika se ne traži postojanje koristoljubive namere kod učinioca već njegovo štetno postupanje prema drugome.[10]

Neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (član 302. KZS)

Ovo krivično delo ima osnovni oblik i dva teža oblika. Teži oblici se razlikuju u odnosu na osnovni oblik po načinu izvršenja i nastupeloj posledici.

Osnovni oblik krivičnog dela postoji kada se učinilac, kršeći mere zaštite, neovlašćeno uključi u računar ili računarsku mrežu, ili neovlašćeno pristupi elektronskoj obradi podataka. Radnja izvršenja se iscrpljuje samim neovlašćenim pristupom računaru ili računarskoj mreži, bez obzira da li je došlo do nastupanja konkretne posledice, u smislu oštećenja, krađe podataka i sl.

Prvi *teži oblik* ovog krivičnog dela se sastoji u snimanju ili upotrebi podataka dobijenih izvršenjem osnovnog oblika krivičnog dela. Pritom nije od značaja u koju svrhu i na koji način je taj podatak upotrebljen (to može biti od značaja kod odmeravanja kazne).[11]

10 Ovo krivično delo treba razlikovati od naoko „srodnih" krivičnih dela poput: prevara (član 208. KZS) i prevara u osiguranju (član 208a. KZS). Naime, ova krivična dela se, takođe, mogu izvršiti korišćenjem računarske tehnologije, s tim da se i u takvim okolnostima oba krivična dela bitno razlikuju od računarske prevare. Matijašević, J., (2013). Krivičnopravna regulativa računarskog kriminaliteta, Novi Sad, Privredna akademija, str. 107.

11 Stojanović, Z., (2012). Komentar Krivičnog zakonika, Beograd, Službeni glasnik, str. 828.

Drugi *teži oblik* ovog krivičnog dela, po pravilu, zahteva nastupanje konkretnih posledica. One se sastoje u zastoju ili ozbiljnom poremećaju funkcionisanja elektronske obrade i prenosa podataka ili mreže, ostavljajući mogućnost nastupanja i drugih težih posledica. "Teške posledice se ne odnose samo na direktne posledice koje su nastale na računaru, računarskoj mreži, odnosno drugom uređaju za elektronsku obradu podataka već obuhvataju sve posledice do kojih je došlo usled neovlašćenog pristupa".[12]

Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 303. KZS)

Ovo krivično delo ima jedan osnovni oblik i jedan teži oblik koji se razlikuju po svojstvu mogućeg izvršioca. Tako se *osnovni oblik* krivičnog dela može izvršiti neovlašćenim sprečavanjem ili ometanjem pristupa javnoj računarskoj mreži. Zakonodavac je u članu 112. stav 18. KZS odredio pojam računarske mreže kojoj može pristupati neograničeni broj ljudi (internet). *Teži oblik* ovog krivičnog dela može izvršiti samo službeno lice u vršenju službene dužnosti. Po prirodi stvari, može biti reč samo o onom službenom licu, koje u vršenju svoje službene dužnosti, ima mogućnost da spreči ili ograniči pristup javnoj računarskoj mreži. Oba oblika ovog krivičnog dela se mogu izvršiti samo sa umišljajem.

Neovlašćeno korišćenje računara ili računarske mreže (član 304. KZS)

Ovo krivično delo ima samo osnovni oblik koji se sastoji u neovlašćenom korišćenju računara ili računarske mreže. Radnja dela se ispoljava kao krađa internet vremena od lica koja uredno plaćaju ovo vreme ovlašćenim firmama (provajderu). Reč je o provaljivanju pristupne šifre (lozinke) kojom se legalni korisnik uloguje kako bi koristio zakupljeno vreme na internetu. S obzirom da je ovo krivično delo lako krivično gonjenje se preduzima po privatnoj tužbi. U praksi je prisutna velika tamna brojka kod ovog krivičnog dela. Razlozi se odnose na nemogućnost pravovremenog reagovanja na različite oblike neovlašćenog korišćenja računara ili računarske mreže. Tome doprinosi više nego vešt način upravljanja od strane lica koja poseduju visok nivo znanja iz oblasti računara i interneta (hakeri).

Pravljenje, nabavljanje i davanje sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka (član 304a. KZS)

Izmenama Krivičnog zakonika iz 2009. godine grupa krivičnih dela protiv bezbednosti računarskih podataka obogaćena je novim krivičnim delom. Ovo krivično delo ima samo jedan oblik čija se radnja izvršenja sastoji u pravljenju, nabavljanju i davanju sredstava za izvršenje krivičnih dela protiv bezbednosti

12 Ibid., str. 828.

računarskih podataka. Razlozi za uvođenje ovog krivičnog dela se tiču donošenja Zakona o potvrđivanju Konvencije o visokotehnološkom kriminalu.[13] Međutim, kod ovog krivičnog dela, nije potrebno da je preduzimanjem njegove radnje izvršeno neko krivično delo protiv bezbednosti računarskih podataka. Otuda se radnja izvršenja iscrpljuje na nivou pravljenja, nabavljanja i davanja sredstava za izvršenje krivičnih dela iz ove grupe. Predviđena je mera bezbednosti oduzimanja predmeta.

ZAVRŠNI OSVRT

Bezbednost računarskih podataka predstavlja područje koje uživa posebnu vrstu pravne zaštite, uključujući i domene krivičnog prava. Skorijim izmenama našeg ranijeg Krivičnog zakona iz 2003. godine, kao i donošenjem važećeg Krivičnog zakonika iz 2005. godine, povećan je broj krivičnih dela kojima se određuje inkriminaciona zona u čijim okvirima se narušava bezbednost računarskih podataka. Ona se kreće od tipičnih dela, poput oštećenja računarskih podataka i programa, računarske sabotaže, prevare, neovlašćenog pristupa mreži, pa sve do krađe internet vremena, kao dela koje se goni po privatnoj tužbi oštećenog pravnog (provajder) ili fizičkog (korisnik) lica.

Posebnost ove vrste krivičnih dela ogleda se u korišćenju stručnih izraza, iz oblasti informacionih tehnologija i računarstva, u njihovim dispozicijama, usled čega je potrebno koristiti zakonsko određenje pojedinih pojmova iz člana 112. KZS. Veći broj krivičnih dela sadrži, pored osnovnih, i teže oblike koji se razlikuju prema radnji izvršenja i nastupeloj posledici u obliku pretrpljene materijalne štete. Iako se eksplicitno ne traži posebno svojstvo učinioca, osim kod nekih težih oblika, činjenica je da ova krivična dela mogu vršiti samo lica sa prethodnim znanjem iz oblasti računarstva i informatike. Kod propisivanja radnje izvršenja prisutno je njihovo alternativno određivanje, tako što se navode tipične radnje i ostavlja mogućnost izvršenja krivičnog dela nekom drugom radnjom, kojom se može proizvesti zabranjena posledica.

Na kraju, važno je naglasiti da je Srbija na području zaštite bezbednosti računarskih podataka dostigla standarde predviđene Konvencijom o visokotehnološkom kriminalu. Međutim, u praksi se susrećemo sa nizom prepreka na polju pravovremenog otkrivanja i procesuranja učinilaca ove vrste krivičnih dela. Tome doprinosi, još uvek, veliki broj nelegalnih softvera kod individualnih korisnika računara, koji koriste krekovane operativne sisteme i programe, čime narušavaju bezbednost sopstvenih ali i tuđih računarskih podataka.

13 Odredbe ove Konvencije su sistematizovane kroz četiri poglavlja: I Upotreba termina; II Mere koje treba da se preduzmu na nacionalnom nivou; III Međunarodna saradnja; IV Završne odredbe. Vidi: Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, Službeni glasnik RS, br. 19/09.

LITERATURA :

1. Babić, M., Marković, I., (2013). Krivično pravo-posebni dio, Banja Luka, Pravni fakultet.
2. Čejović, B., Kulić, M., (2014). Krivično pravo, Novi Sad, Privredna akademija.
3. Lazarević, Lj., (2011). Komentar Krivičnog zakonika, Beograd, Pravni fakultet Union.
4. Matijašević, J., (2013). Krivičnopravna regulativa računarskog kriminaliteta, Novi Sad, Privredna akademija.
5. Stamenković, B. et al. (2014). Visokotehnološki kriminal (praktični vodič kroz savremeno krivično pravo i primjere iz prakse), Podgorica, OEBS Misija u Crnoj Gori.
6. Stojanović, Z., (2012). Komentar Krivičnog zakonika, Beograd, Službeni glasnik.
7. Urošević, V. et al., (2015). Policija i visokotehnološki kriminal – primeri iz prakse i problemi u radu MUP-a Republike Srbije u: Slobodan R. Petrović (urednik) Zloupotreba informacionih tehnologija i zaštita, Beograd, Udruženje sudskih veštaka za informacione tehnologije IT Veštak.

Propisi

1. Zakon o izmenama i dopunama Krivičnog zakona Republike Srbije, Službeni glasnik RS, br. 39/03.
2. Krivični zakonik Republike Srbije, Službeni glasnik RS, br. 85/05-121/12.
3. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala Republike Srbije, Službeni glasnik RS, br. 61/05 i 104/09.
4. Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, Službeni glasnik RS, br. 19/09.

CIP - Каталогизација у публикацији
Библиотека Матице српске, Нови Сад

340.134(497)(082)

МЕЂУНАРОДНИ научни скуп "Прилагођавање правне регулативе актуелним трендовима у региону" (2015 ; Нови Сад)
[Zbornik referata sa Međunarodnog naučnog skupa "Prilagođavanje pravne regulative aktuelnim trendovima u regionu", 24-26. septembar 2015, Novi Sad] / [priredio Milorad Bejatović]. - Novi Sad : Pravni fakultet za privredu i pravosuđe, 2015 (Novi Sad : Feljton). - 825 str. : ilustr. ; 24 cm

Tiraž 150. - Bibliografija uz svaki rad. - Rezime na engl. jeziku uz većinu radova.

ISBN 978-86-6019-058-3

а) Правна регулатива - Усаглашавање - Балкан - Зборници
COBISS.SR-ID 299340807