

PRAVO I DIGITALNE TEHNOLOGIJE
Priredio: Dr Marko Carić, redovni profesor

LAW AND DIGITAL TECHNOLOGY
Edited by: Marko Carić, PhD, Full Professor

Univerzitet Privredna akademija u Novom Sadu
Pravni fakultet u Novom Sadu
University Business Academy Novi Sad
Faculty of Law in Novi Sad

Novi Sad 2019.

Zbornik referata sa XVI Međunarodnog naučnog skupa
„Pravnički dani - Prof. dr Slavko Carić”
26. – 28. septembar 2019. godine u Novom Sadu,
u organizaciji Univerziteta Privredna akademija u Novom Sadu
Pravni fakultet u Novom Sadu

Izdavač:

Univerzitet Privredna akademija u Novom Sadu,
Pravni fakultet u Novom Sadu
Geri Karolja br. 1, telefon: 021 400 – 499
Web: www.pravni-fakultet.info

Recenzenti:

Dr Marko Carić, redovni profesor Emeritus dr Milorad Bejatović Akademik dr Vesna Vučković, redovni profesor	Dr Darko Golić, vanredni profesor Dr Predrag Mirković, vanredni profesor
Dr Mirjana Knežević, redovni profesor Dr Vladimir Medović, vanredni profesor	Dr Mirko Smoljić, vanredni profesor Dr Marijana Mladenov, docent Dr Jelena Stojšić-Dabetić, docent Dr Joko Dragojlović, docent
Dr Vladimir Kozar, vanredni profesor	

Za izdavača:

Dr Marko Carić, redovni profesor

Urednik:

Dr Marko Carić, redovni profesor

Štampa:

Štamparija FELJTON, Novi Sad

Tiraž: 80

ISBN
978-86-6019-103-0

Programski odbor:

Dr MARKO CARIĆ, redovni profesor | Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet u Novom Sadu, Dekan | Republika Srbija
Emeritus dr MILORAD BEJATOVIĆ | Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet u Novom Sadu | Republika Srbija

Dr MIRKO KULIĆ, redovni profesor | Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet u Novom Sadu, Rektor | Republika Srbija

Akademik dr MIODRAG N. SIMOVIĆ, redovni profesor | Pravni fakultet Univerziteta u Banjoj Luci, Sudija Ustavnog suda Bosne i Hercegovine | Bosna i Hercegovina

Dr DUŠANKA ĐURĐEV, redovni profesor | Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet u Novom Sadu | Republika Srbija

Dr MILENKO KREĆA, redovni profesor u penziji | Pravni fakultet Univerziteta u Beogradu | Republika Srbija

Dr RODOLJUB ETINSKI, redovni profesor u penziji | Pravni fakultet Univerziteta u Novom Sadu, Urednik Sekcije za međunarodno pravo Kopaoničke škole prirodnog prava | Republika Srbija

Akademik dr RADOVAN VUKADINOVIĆ, redovni profesor | Pravni fakultet Univerziteta u Banjoj Luci | Bosna i Hercegovina

Dr MIRJANA KNEŽEVIĆ, redovni profesor | Univerzitet u Kragujevcu, Ekonomski fakultet | Republika Srbija

Akademik dr VESNA VUČKOVIĆ, redovni profesor | Univerzitet "Adriatik" – Bar, Sudija Vrhovnog suda Crne Gore | Republika Crna Gora

Dr MILE MATIJEVIĆ, redovni profesor | Univerzitet za poslovne studije, Fakultet pravnih nauka, Dekan | Bosna i Hercegovina

Dr MIRKO SMOLJIĆ, vanredni profesor | Sveučilište Sjever, Varaždin | Republika Hrvatska

Dr SLAVOMIR RUDENKO | Pravni fakultet, Panevropski univerzitet u Bratislavi | Republika Slovačka

Dr IVAN BULATOVIĆ, profesor strukovnih studija | Beogradska poslovna škola – Visoka škola strukovnih studija, Nacionalni savet za visoko obrazovanje | Republika Srbija

Mr KAMENKO KOZARSKI | Predsednik Prekršajnog suda u Novom Sadu | Republika Srbija

MIROSLAV ALIMPIĆ | v.f. predsednika Višeg suda u Šapcu, Sudija Apelacionog suda u Novom Sadu | Republika Srbija

Dr ILIJA ZINDOVIĆ | Sudija Apelacionog suda u Kragujevcu | Republika Srbija

Organizacioni odbor:

Dr MARKO CARIĆ, redovni profesor - Predsednik Organizacionog odbora

Emeritus dr MILORAD BEJATOVIĆ

Dr ŽELJKO BJELAJAC, redovni profesor

Dr VLADIMIR MEDOVIĆ, vanredni profesor

Dr VLADIMIR KOZAR, vanredni profesor

Dr DARKO GOLIĆ, vanredni profesor

Dr PREDRAG MIRKOVIĆ, vanredni profesor

Dr MARIJANA MLADENOV, docent

Dr JELENA STOJŠIĆ- DABETIĆ, docent

Dr JOKO DRAGOJLOVIĆ, docent

Sekretar:

Dr MAJA SUBOTIN, docent

Dr Maja Subotin, docent

Univerzitet Privredna akademija u Novom Sadu,

Pravni fakultet u Novom Sadu

e-mail: maja.subotin@pravni-fakultet.info

Dr Jelena Matijašević Obradović, vanredni profesor

Univerzitet Privredna akademija u Novom Sadu,

Pravni fakultet u Novom Sadu

e-mail: jelena@pravni-fakultet.info

KRIMINOLOŠKI I KRIMINALISTIČKI ASPEKT RAČUNARSKOG KRIMINALITETA

Apstrakt:

Ubrzan razvoj informacione i kompjuterske tehnologije unapredio je skoro sve oblasti života, ali je i otvorio mogućnosti za sve složenije i opasnije oblike zloupotreba. Specifične karakteristike računarskog kriminaliteta uticale su da se u teoriji sve više razmatraju mogobrojni aspekti ove društvene pojave, kao i da se menja legislativa u pravcu kvantitativno i kvalitativno boljeg regulisanja ove oblasti. Izuzetna fenomenološka kompleksnost, raznolikost i dinamika manifestovanja doprinela je njegovom otežanom definisanju i razumevanju kao posebnog oblika kriminaliteta. Razvoj, mogućnosti i izražena „tamna brojka” računarskog kriminaliteta koju prati nedovoljna obučenost odgovornih lica za njegovo suzbijanje, nametnula je potrebu za posvećenijim pristupom u pogledu analize kriminološkog i kriminalističkog aspekta ovog oblika kriminaliteta.

Ključne reči: računarski kriminalitet, kriminološki aspekt, kriminalistički aspekt

UVOD

Razvoj kompjuterske tehnologije u velikoj meri je doprineo poboljšanju i unapređenju privredne delatnosti, posebno kada je reč o proizvodnji, komunikaciji, finansijskom poslovanju i dr. Međutim, ovaj razvoj je, sa druge strane, doneo mnoge mogućnosti zloupotrebe i nove oblike kriminaliteta, a sve kriminalne pojave koje su u vezi sa zloupotrebom kompjuterskih tehnika i tehnologija predstavljaju upravo računarski kriminalitet.

Savremena informaciona i kompjuterska tehnologija unela je nove i drastične promene u sve segmente društva, odnosno društvenog života, a koje su pored pozitivnih i korisnih novina, donele i niz problema vezanih za pojavu i širenje računarskog kriminaliteta različitih oblika, formi i vidova ispoljavanja. Sve te promene se mogu svesti na sledeće: nove forme vrednosti, koncentracija podataka, novi ambijent delovanja, nove metode i tehnike delovanja, sužavanje vremenske skale delovanja, širenje geografskog prostora delovanja, pokretljivost, stabilnost rizika.¹

Dakle, računarski kriminalitet predstavlja savremeni oblik kriminaliteta kojeg karakteriše niz specifičnosti u pogledu strukture, osobenosti i zastupljenosti, odnosno rasprostranjenosti.

Kompjuter se u kriminalnoj delatnosti može koristiti kao objekt napada, sredstvo izvršenja, sredstvo za planiranje izvršenja krivičnog dela, kao i sredstvo za sprečavanje razjašnjavanja i dokazivanja krivičnih dela. U tom smislu, kompjuter se pokazao kao sredstvo kojim se mogu izvršavati raznovrsna složena krivična dela, kao što su pljačke, pronevere, finansijske malverzacije, špijunaža, terorizam, kao i različiti oblici zloupotreba.²

POJAM I KARAKTERISTIKE RAČUNARSKOG KRIMINALITETA

U cilju jasnijeg sagledavanja računarskog kriminaliteta neophodno je osvrnuti se na sam pojam računarskog kriminaliteta i njegova specifična obeležja, odnosno karakteristike. Fenomenologija ovog oblika kriminaliteta doprinela je tome da još uvek ne postoji njegovo jedinstveno i precizno pojmovno određenje.

Pojam računarskog kriminaliteta menjao se kroz istoriju prateći evoluciju načina upotrebe, odnosno zloupotrebe računara i ubrzano širenje područja primene računara.³ Imajući u vidu da se radi o relativno novom obliku kriminaliteta koji karakteriše izuzetna fenomenološka raznovrsnost uzrokovana dinamičnim razvojem kompjuterske tehnologije i za kojim kontinuirano zaostaje adekvatna pozitivna krivičnopravna legislativa, jasno je zbog čega je pitanje definisanja računarskog kriminaliteta praćeno brojnim nedoumicama i problemima.

Živojin Aleksić i Milan Škulić zastupaju jedno veoma prihvaćeno gledište vezano za pojam računarskog kriminaliteta: Kompjuterski kriminalitet predstavlja oblik kriminalnog ponašanja kod koga se korišćenje kompjuterske tehnologije i

1 Petrović, S. (2002). *Kompjuterski kriminal*, MUP Srbije, Beograd, str. 17.

2 Bošković, M. (2012). *Socijalna patologija*, Unija fakulteta Jugoistočne Evrope, Novi Sad, str. 69.

3 McEwen, T. J. (1988). *Dedicated Computer Crime Units*, Davis-Associates, p. 1. Preuzeto sa: <https://books.google.rs/books?id=qZBXcX0ZgZwC&lpq=PA1&ots=JEhU1FzGS&dq=computer%20criminal&pg=PR1#v=onepage&q=computer%20criminal&f=false> (27.06.2019.)

informatičkih sistema ispoljava kao način izvršenja krivičnog dela, ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivičnopravnom smislu relevantna posledica.⁴

U kontekstu pomenute definicije, autori su izneli i argumentaciju iste, ističući karakteristike same pojave koje se moraju imati u vidu, kao i osnovnih elemenata jedne definicije: „Određivanje pojma kompjuterskog kriminaliteta se ne može zasnivati na utvrđivanju u okviru njegove definicije, elemenata, koji nisu karakteristični za sve oblike ovog vida delinkvencije, kao što su npr. profil učinilaca, konkretna vrsta krivičnog dela, vrsta štetne posledice, motiv za kriminalno ponašanje, itd. Zato je prilikom definisanja kompjuterskog kriminaliteta neophodno imati veoma širok pristup. Tako se jedna sveobuhvatna i široka definicija kompjuterskog kriminaliteta mora zasnivati na tri osnovna elementa: načinu izvršenja, sredstvu izvršenja i posledici kriminalnog delovanja. Način izvršenja ovih delikata se zasniva na upotrebi kompjutera, pri čemu samo to korišćenje računara može biti ispoljeno kao celovit *modus operandi*, ili kao jedan njegov segment. Kompjuter može biti i osnovno sredstvo izvršenja ovih krivičnih dela, a potrebno je pored toga da je na takav način ostvarena i neka u krivičnopravnom smislu kažnjiva posledica, s tim što posledica može biti ispoljena i na samim kompjuterima, informatičkoj, ili komunikacijskoj mreži.”⁵

Dakle, računarski kriminalitet se može definisati kao kriminalitet koji je usko povezan sa korišćenjem računara i u tom smislu sam računar javlja se kao sredstvo izvršenja ili cilj izvršenja krivičnog dela, ili se njegovo korišćenje ispoljava kao način izvršenja krivičnog dela.

Imajući u vidu da se savremeno poslovanje ne može zamisliti bez tehnologije, odnosno računara, računarskih sistema, mreža i programa, jasno je da kompjuterski kriminalitet ima potencijal da parališe čitavu privredu, infrastrukturu, komunikacije, finansije i sl.

Šteta koja nastane kao posledica vršenja kompjuterskih krivičnih dela obično je znatno veća nego što se na prvi pogled čini, čak daleko nadmašuje iznos štete koja je prouzrokovana klasičnim krivičnim delima i procenjuje se na stotine miliona dolara.⁶

Shodno do sada rečenom, najbitnije osobine kompjuterskog kriminaliteta vezane su za:

1. Prostornu dimenziju kriminalnog delovanja;
2. Vremensku dimenziju kriminalnog delovanja;
3. Konstantno širenje na nove oblasti društvenog života;

4 Aleksić, Ž., Škulić, M. (2007). *Kriminalistika*, Pravni fakultet Univerziteta u Beogradu i Javno preduzeće „Službeni glasnik”, Beograd, str. 385.

5 *Ibid.*

6 Matijašević, J. (2013). *Krivičnopravna regulativa računarskog kriminaliteta*, Pravni fakultet za privredu i pravosuđe, Novi Sad, str. 23.

4. Specifičan profil učinioca;
5. Veliku tamnu brojku;
6. Način vršenja i otkrivanja kriminalnih radnji;
7. Težinu posledica i visinu štete;
8. Višestruku ulogu računarske tehnologije.⁷

KRIVIČNOPRAVNA REGULATIVA RAČUNARSKOG KRIMINALITETA

Krivična dela koja se odnose na bezbednost računarskih podataka propisana su u Glavi XXVII Krivičnog zakonika. Krivična dela protiv bezbednosti računarskih podataka čine oštećenje računarskih podataka i programa, računarska sabotaza, 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, pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka.⁸

Dakle, mogućnosti korišćenja računara za izvršenje krivičnog dela su mnogobrojne, a računar može biti sredstvo ili objekt izvršenja, sredstvo za planiranje ili prikrivanje krivičnog dela, sredstvo za omogućavanje izvršenja krivičnog dela i dr.

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnoškog kriminala⁹ predviđa osnivanje, organizaciju, nadležnost i ovlašćenja posebnih organa za borbu protiv ove vrste kriminala, odnosno za otkrivanje, krivično gonjenje i suđenje za krivična dela koja predviđa, u okviru postojeće sudske i tužilačke organizacije i Ministarstva unutrašnjih poslova. U okviru Višeg javnog tužilaštva u Beogradu obrazovano je Posebno tužilaštvo za borbu protiv visokotehnoškog kriminala, čijim radom rukovodi Posebni tužilac za visokotehnoški kriminal. U okviru Ministarstva nadležnog za unutrašnje poslove obrazovana je Služba za borbu protiv visokotehnoškog kriminala, koja postupa po zahtevima Posebnog tužioca za visokotehnoški kriminal, u cilju obavljanja poslova organa unutrašnjih poslova u vezi sa krivičnim delima iz ove oblasti. U okviru Višeg suda u Beogradu za postupanje u predmetima krivičnih dela iz ove oblasti, obrazovano je Odeljenje za borbu protiv visokotehnoškog kriminala, a sudije u ovo Odeljenje raspoređuje predsednik Višeg suda u Beogradu, pri tom prednost imaju sudije koje poseduju posebna znanja iz oblasti informatičkih tehnologija.¹⁰ U skladu sa odredbama Krivičnog zakonika, u članu 3, stav

7 Matijašević, J. (2013). *Krivičnopravna regulativa računarskog kriminaliteta*, op. cit., str. 18-25.

8 Krivični zakonik ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019), čl. 298-304a

9 Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnoškog kriminala („Sl. glasnik RS”, br. 61/2005 i 104/2009)

10 Matijašević, J. (2013). *Krivičnopravna regulativa računarskog kriminaliteta*, op. cit., str. 99-100.

1, Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnoškog kriminala svrstava navedena krivična dela u isključivu stvarnu nadležnost ovih organa.

Krivična dela poput pljačke, pronevere, prevare, terorizma, finansijskih malverzacija i raznih oblika zloupotreba, dobila su potpuno novu dimenziju korišćenjem kompjutera kao sredstva izvršenja. Ovakav savremeni način izvršenja ovih krivičnih dela ima niz specifičnosti i različitih oblika ispoljavanja, a predstavljaju upravo visokotehnoški kriminal.¹¹

Prema Zakonu o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnoškog kriminala, visokotehnoški kriminal se definiše kao vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja javljaju računari, računarski sistemi, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku.¹²

Osnovna primedba koja se upućuje Zakonu o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnoškog kriminala jeste izostanak odredbi koje bi predviđale obavezu specijalizacije kadrova Službe za borbu protiv visokotehnoškog kriminala, odnosno posedovanja posebnih znanja iz oblasti informatičkih tehnologija.¹³

Positivan korak ka unapređenju borbe protiv visokotehnoškog kriminala učinjen je donošenjem Strategije za borbu protiv visokotehnoškog kriminala za period 2019-2023. godine¹⁴ kroz koju se ukazalo na niz problema koje je neophodno otkloniti u cilju efikasnijeg suzbijanja ovog oblika kriminaliteta. U tom smislu ukazano je da postoji prostor za unapređenje normativnog i institucionalnog okvira, odnosno da je neophodno poboljšati uslove za rad u pogledu broja zaposlenih, tehničke opremljenosti i operativnih kapaciteta, kao i unaprediti saradnju na nacionalnom i međunarodnom nivou između državnih organa koji su prepoznati kao nosioci borbe protiv visokotehnoškog kriminala.

KRIMINOLOŠKI ASPEKT RAČUNARSKOG KRIMINALITETA

Savremena visoko sofisticirana kompjuterska i informatička tehnologija doprinela je razvoju velikog broja pojava oblika računarskog kriminaliteta, između kojih veoma često ne postoji jasna granica, već se međusobno ukrštaju, preklapaju ili vrše istovremeno kako bi se ostvario postavljeni cilj.

11 Randelović, D. M., Nikač, Ž., Stefanović, M. (2012). Softverski alati i pranje novca kao oblik visokotehnoškog kriminala, *Poslovna ekonomija*, vol. 6, br. 2, str. 97-98.

12 Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnoškog kriminala („Sl. glasnik RS”, br. 61/2005 i 104/2009), čl. 2, st. 1

13 Dimovski, D. (2010). Kompjuterski kriminalitet, *Zbornik radova Pravnog fakulteta u Nišu*, br. 55, str. 204.

14 Strategija za borbu protiv visokotehnoškog kriminala za period 2019-2023. godine („Sl. glasnik RS”, br. 71 od 25. septembra 2018. godine)

Praktične mogućnosti računarskih tehnologija uticale su na to da je danas sve izraženija opasnost od širenja i masovne upotrebe elektronskog prisluškivanja, krađe poslovnih i drugih tajni, kao i različitih oblika intelektualne svojine, zatim ozbiljnog narušavanja privatnosti i drugih ljudskih sloboda i prava, kao i ličnog integriteta, a u poslednje vreme prisutna je i realna opasnost od talasa terorističkih akata raznih vrsta.¹⁵

U skladu sa njihovom zastupljenošću u praksi, u teoriji se kao pojavni oblici računarskog kriminaliteta najčešće ističu: računarska prevara, računarska sabotaza, računarska špijunaža, računarske krađe, računarski terorizam, hakerisanje, računarske zloupotrebe, posebno zloupotrebe platnih kartica i računarske mreže, dečija pornografija i dr.

Kada je reč o uzrocima računarskog kriminaliteta, kao najznačajni faktor izdvaja se tehnološka razvijenost, rasprostranjenost informacionih tehnologija, dostupnost računara i interneta, a posebno internet zavisnost kao sve zastupljeniji pojavni oblik socijalne patologije koji u poslednje vreme dobija dimenziju epidemije.

Prema Boškoviću i Markoviću, uzroci računarskog kriminaliteta mogu se svrstati u:

- a) tehničke faktore, u koje spada laka pristupačnost i softverska nezaštićenost računarske tehnologije;
- b) tehničko-tehnološke faktore koje čine razućdenost i nesigurnost mreža koje omogućavaju pristup kompjuterskim sistemima u uslovima nestručnosti ili nedovoljne stručnosti njihovih korisnika, kao i izražena anonimnost delovanja;
- v) neadekvatna pravna regulativa;
- g) neefikasna prevencija, odnosno izuzetno teško otkrivanje i dokazivanje, neupućenost oštećenih (žrtava) u izvršeni delikt i nestručnost lica zaduženih za otkrivanje ove vrste krivičnih dela.¹⁶

Neophodno je precizno definisati i prepoznati profil izvršilaca krivičnih dela iz sfere kompjuterskog kriminala, s obzirom na to da se radi o informatičkim stručnjacima koji koriste svoje znanje u pogrešne svrhe. Iako se metodologija i motivi izvršilaca razlikuju, najčeći motiv jeste imovinska korist, mada je ponekad to samo dokazivanje u hakerskom svetu, slanje određene poruke društvu, pojedincu, vlasti i slično, analizom osnovnih osobenosti izvršilaca može se doprineti određivanju efikasnijih preventivnih aktivnosti u oblasti kompjuterskog kriminaliteta.¹⁷

15 Jovašević, D., Hašimbegović, T. (2004). Krivičnopravna zaštita bezbednosti računarskih podataka, *Naučno stručno savetovanje Ziteh*, str. 3.

Preuzeto sa: <https://singipedia.singidunum.ac.rs/izdanje/40081-krivicnopravna-zastita-bezbednosti-racunarских-podataka> (28.06.2019.)

16 Bošković, M., Marković, M. (2015). *Kriminologija sa elementima viktinologije*, Pravni fakultet za privredu i pravosuđe, Novi Sad, str. 308.

17 Matijašević, J. (2013). *Krivičnopravna regulativa računarskog kriminaliteta*, op. cit., str. 236.

Dakle, učinioci računarskih krivičnih dela bi se mogli uopšteno podeliti na zlonamerne koji deluju radi sticanja imovinske koristi ili radi nanošenja određene štete, kao i na učinioce koji jednostavno traže zadovoljstvo u neovlašćenom pristupu nekom dobro obezbeđenom informacionom sistemu. U praksi su se izdvojile određene osobine koje čine kriminalni profil učinioca računarskih delikata koji su motivisani koristoljubljem: 80% ovih delinkvenata čini delo po prvi put, 70% je zaposleno više od 5 godina u oštećenom preduzeću, njihovo starosno doba je u proseku između 19 i 30 godina, pretežno su muškog pola, veoma inteligentni, imaju uglavnom više godina radnog iskustva i smatraju se savesnim radnicima, često su tehnički kvalifikovaniji nego što to zahteva radno mesto na koje su raspoređeni, sebe ne smatraju kriminalcima.¹⁸

Ono što računarski kriminalitet čini primamljivim za potencijalne izvršioce krivičnih dela, jeste njegova prostorna neograničenost, izražena anonimnost i brzina izvršenja. U tom smislu, kao endogeni faktori ovog oblika kriminaliteta javlja se frustracija izazvana izuzetno velikim brojem informacija dostupnim na internetu, unutrašnja želja ka lakom i brzom bogaćenju, izolovanost i socijalna otuđenost koja se javlja kao posledica internet zavisnosti i različiti mentalni poremećaji.

KRIMINALISTIČKI ASPEKT RAČUNARSKOG KRIMINALITETA

Priroda informacionih tehnologija izuzetno otežava otkrivanje i dokazivanje, odnosno gonjenje učinilaca ovih krivičnih dela. Računari i računarski sistemi povezani su na globalnom nivou, što omogućava da se preduzimaju inkriminisane radnje iz jedne države u bilo kojoj drugoj državi, pod uslovom da sa obe strane postoji računar i internet konekcija. Visok stepen anonimnosti korisnika doprinosi otežanom otkrivanju izvora kriminalne aktivnosti od strane organa gonjenja, dok ih granice teritorijalne nadležnosti, u određenim slučajevima, sprečavaju u procesuiranju otkrivenih učinilaca ovih krivičnih dela.¹⁹

Upravo otežano otkrivanje, komplikovano dokazivanje i neefikasna prevencija podstiču potencijalne izvršioce ovih krivičnih dela na donošenje odluke o izvršenju.

Dakle, za računarski kriminalitet karakteristično je teško otkrivanje i teško pribavljanje dokaza, a sam postupak razjašnjavanja i dokazivanja zahteva poseban pristup, stručna znanja i multidisciplinarni aspekt sagledavanja ovih krivičnih dela, iz čega proizilazi potreba sticanja odgovarajućih znanja od strane operativnih radnika policije, javnih tužilaca, njihovih zamenika, istražnih sudija. Visok stepen poznavanja računara, njegovih mogućnosti i načina korišćenja

18 Aleksić, Ž., Škulić, M. (2007). *Kriminalistika, op.cit.*, str. 388-389.

19 Pisarić, M. (2013). Potrebni normativni odgovor na probleme otkrivanja i dokazivanja dela visokotehnološkog kriminala, *Zbornik radova Pravnog fakulteta*, Novi Sad, vol. 47, br. 1, str. 292.

predstavlja preduslov za otkrivanje, krivično gonjenje i suđenje učiniocima ovih krivičnih dela.²⁰

Specijalizovane jedinice državnih organa za suzbijanje kriminala predstavljaju neophodan segment u cilju suzbijanja kompjuterskog kriminaliteta. Imajući u vidu značaj i količinu informacija koja se nalazi u savremenim kompjuterskim i drugim komunikacionim mrežama, neophodno je, pored ovih specijalizovanih jedinica i njihovog konstantnog unapređenja i edukacije, razvijati softverske alate i pratiti razvoj tehnologije kako bi se uspostavila efikasnija zaštita, uz uspešnije otkrivanje i suzbijanje kompjuterskog kriminala. Unapređena zaštita u ovoj sferi doprinosi stvaranju ambijenta pogodnog za investicije i razvoj poslovanja privrednih subjekata.²¹

Uvođenje novih mera u krivično zakonodavstvo iz oblasti visokotehnološkog kriminala, ali i unifikacija i efikasna međunarodna saradnja, predstavljaju osnovu za realizaciju nacionalnih napora u pravcu suzbijanja ovih krivičnih dela.²²

Bez obzira na značajnu posvećenost suzbijanju računarskog kriminaliteta, ne očekuje se da će se zastupljenost ovog oblika kriminaliteta u skorijoj budućnosti smanjiti.²³ Ovakav zaključak proizilazi iz permanentnog razvoja računarske tehnologije, a samim tim i proširivanja mogućnosti zloupotreba, ali i iz činjenice da nadležni organi za otkrivanje, gonjenje i suđenje u predmetima vezanim za ovu oblast nisu u dovoljnoj meri specijalizovani i obučeni, niti raspolažu najsavremenijom tehničkom infrastrukturom, odnosno opremom koja predstavlja preduslov za efikasno suzbijanje ovog oblika kriminaliteta.

Pored specijalizacije u pogledu otkrivanja i dokazivanja krivičnih dela računarskog kriminaliteta, neophodno je značajnu pažnju posvetiti samoj ličnosti izvršilaca ovih krivičnih dela.

U tom smislu, motiv za izvršenje ovih krivičnih dela predstavlja značajnu indicijalnu činjenicu, a posebno dolazi do izražaja pri postavljanju verzije o osumnjičenom licu, bez obzira na to da li je reč o jednom učiniocu, ili o grupi, pa je tada metodom eliminacije potrebno odstraniti sumnju sa nevinih lica.²⁴

20 Prema procenama FBI manje od 1% ukupno izvršenog kompjuterskog kriminaliteta biva otkriveno, a samo 12% prijavljeno (pre svega zbog straha od negativnog publiciteta i gubitka poverenja kod poslovnih partnera). Obradović, S, Mijalković, M., Perić, D., Puača, D. (2007). *Istraživanje kriminala na računarima*, Međunarodni simpozijum Infoteh-Jahorina, vol. 6, str. 455.

21 Milošević, M. (2007). Aktuelni problemi suzbijanja kompjuterskog kriminala, *Nauka, bezbednost, policija - Žurnal za kriminalistiku i pravo*, vol. 12, broj 1, str. 71.

22 Prlja, D., Reljanović, M. (2009). Visokotehnološki kriminal – uporedna iskustva, *Strani pravni život*, br. 3, str. 161.

23 Rogers, M., Seigfried, K., Tidke, K. (2006). *Self-reported computer criminal behavior: A psychological analysis*, From the proceedings of The Digital Forensic Research Conference DFRWS 2006 USA Lafayette, IN (Aug 14th - 16th), p. 120.

24 Banović, B. (2002). *Obezbeđenje dokaza u kriminalističkoj obradi krivičnih dela privrednog kriminaliteta*, Viša škola unutrašnjih poslova, Beograd-Zemun, str. 85.

Najčešći načini dolaženja do saznanja o izvršenom krivičnom delu iz oblasti računarskog kriminaliteta jesu prijave radnika, anonimne i pseudonimne prijave, ili kroz vršenje nadzora i kontrole.²⁵ Nekada je otkrivanje računarskih krivičnih dela bilo znatno lakše upravo zbog toga što je manji broj ljudi posedovao odgovarajuća znanja i veštine koje bi im omogućile da kompjuter koriste u kriminalne svrhe, a danas je problematika otkrivanja ovih krivičnih dela složenija imajući u vidu izuzetno širok krug korisnika kompjutera. U praksi se pokazalo da se mnogi oblici kompjuterskog kriminaliteta otkriju tek kada neko od učinilaca napravi grešku ili se kroz istraživanje uočene greške otkrije kriminalna delatnost pojedinca ili grupe. U tom smislu, sve češće se primenom specijalnih programa postavljaju odgovarajuće „zamke” koje za cilj imaju otkrivanje učinioca ovih krivičnih dela.²⁶

ZAKLJUČAK

Računarski kriminalitet karakteriše izuzetna fenomenološka raznovrsnost koja otežava njegovo jedinstveno i precizno pojmovno određenje, a permanentan intenzivni razvoj računarskih tehnologija doprinosi konstantnom proširivanju pojava oblika i postavlja sve veće izazove pred organe nadležne za njegovo suzbijanje.

Pristupačnost i softverska nezaštićenost računarske tehnologije, izražena anonimnost kao jedna od ključnih karakteristika računarskog kriminaliteta, neprilagodljiva pravna regulativa i neefikasna prevencija samo su neki od faktora koji doprinose konstantnom rastu broja krivičnih dela iz oblasti računarskog kriminaliteta.

Izražena „tamna brojka” računarskog kriminaliteta i opasnosti koje iz njega proizilaze nametnule su potrebu za posvećenijim pristupom u pogledu analize kriminološkog i kriminalističkog aspekta ovog oblika kriminaliteta. U tom smislu, posebnu pažnju neophodno je posvetiti uzrocima koji dovode do pojave računarskog kriminaliteta, samoj ličnosti izvršilaca ovih krivičnih dela, mogućnostima za njegovo efikasnije otkrivanje i dokazivanje, ali i različitim merama prevencije.

Adekvatna legislativa u Republici Srbiji koja je pretežno usklađena sa međunarodnim standardima nije dovoljna za efikasno suzbijanje računarskog kriminaliteta. Specifičnosti računarskog kriminaliteta ukazuju na neophodnost kontinuirane edukacije nadležnih organa za otkrivanje, gonjenje i suđenje u predmetima vezanim za ovu oblast kako bi se odgovorilo izazovima koje računarski kriminalitet sa sobom nosi. Međutim, sama edukacija nije dovoljna ukoliko na raspolaganju nemaju najsavremeniju tehničku infrastrukturu, odnosno opremu. Posebnu ulogu ima preventivno delovanje koje se odnosi na edukaciju stanovništva

25 Aleksić, Ž., Milovanović, Z. (1994). *Kriminalistika*, Partenon, Beograd, str. 297.

26 Vasić, G., Šarić, B., Jovanić, V. (2012). Kompjuterski kriminalitet, *Zbornik radova Međunarodne naučnostručne konferencije „Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal”*, Laktaši, str. 186.

o karakteristikama i opasnostima koje proizilaze iz računarske tehnologije, odnosno iz računarskog kriminaliteta.



Maja Subotin, PhD, Assistant Professor
University Business Academy in Novi Sad,
Faculty of Law in Novi Sad

Jelena Matijašević Obradović, PhD, Associate Professor
University Business Academy in Novi Sad,
Faculty of Law in Novi Sad

CRIMINOLOGICAL AND CRIMINAL ASPECTS OF COMPUTER CRIME

Abstract:

Accelerated development of information and computer technology has improved almost all areas of life, but has also opened up opportunities for increasingly complex and dangerous forms of abuse. The specific characteristics of computer crime have influenced the theoretical considerations of the numerous aspects of this social phenomenon, as well as the changing of legislation in the direction of quantitatively and qualitatively better regulation of this area. The exceptional phenomenological complexity, diversity and dynamics of manifestation contributed to its difficult definition and understanding as a special form of crime. The development, possibilities and the pronounced "dark figure" of computer crime followed by insufficient training of responsible persons for its suppression imposed a need for a more devoted approach in terms of analyzing the criminological and criminalistic aspect of this form of crime.

Keywords: *computer crime, criminological aspect, criminalistic aspect*

L I T E R A T U R A:

1. Aleksić, Ž., Milovanović, Z. (1994). *Kriminalistika*, Partenon, Beograd
2. Aleksić, Ž., Škulić, M. (2007). *Kriminalistika*, Pravni fakultet Univerziteta u Beogradu i Javno preduzeće „Službeni glasnik“, Beograd
3. Banović, B. (2002). *Obezbeđenje dokaza u kriminalističkoj obradi krivičnih dela privrednog kriminaliteta*, Viša škola unutrašnjih poslova, Beograd-Zemun

4. Bošković, M. (2012). *Socijalna patologija*, Unija fakulteta Jugoistočne Evrope, Novi Sad
5. Bošković, M., Marković, M. (2015). *Kriminologija sa elementima viktimologije*, Pravni fakultet za privredu i pravosuđe, Novi Sad
6. Dimovski, D. (2010). Kompjuterski kriminalitet, *Zbornik radova Pravnog fakulteta u Nišu*, br. 55, str. 193-210
7. Jovašević, D., Hašimbegović, T. (2004). Krivičnopravna zaštita bezbednosti računarskih podataka, *Naučno stručno savetovanje Ziteh*. Preuzeto sa: <https://singipedia.singidunum.ac.rs/izdanje/40081-krivicnopravna-zastita-bezbednosti-racunarskih-podataka> (28.06.2019.)
8. Krivični zakonik ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019)
9. Matijašević, J. (2013). *Krivičnopravna regulativa računarskog kriminaliteta*, Pravni fakultet za privredu i pravosuđe, Novi Sad
10. McEwen, T. J. (1988). *Dedicated Computer Crime Units*, Davis-Associates. Preuzeto sa: <https://books.google.rs/books?id=qZBXcX0ZgZwC&lp-g=PA1&ots=JEhlU1FzGS&dq=computer%20criminal&pg=PR1#v=onepage&q=computer%20criminal&f=false> (27.06.2019.)
11. Milošević, M. (2007). Aktuelni problemi suzbijanja kompjuterskog kriminala, *Nauka, bezbednost, policija - Žurnal za kriminalistiku i pravo*, vol. 12, broj 1, str. 57-74.
12. Obradović, S., Mijalković, M., Perić, D., Puača, D. (2007). *Istraživanje kriminala na računarima*, Međunarodni simpozijum Infoteh-Jahorina, vol. 6, str. 455-459.
13. Petrović, S. (2002). *Kompjuterski kriminal*, MUP Srbije, Beograd
14. Pisarić, M. (2013). Potrebni normativni odgovor na probleme otkrivanja i dokazivanja dela visokotehnološkog kriminala, *Zbornik radova Pravnog fakulteta*, Novi Sad, vol. 47, br. 1, str. 291-307.
15. Prlja, D., Reljanović, M. (2009). Visokotehnološki kriminal – uporedna iskustva, *Strani pravni život*, br. 3, str. 161-184.
16. Randelović, D. M., Nikač, Ž., Stefanović, M. (2012). Softverski alati i pranje novca kao oblik visokotehnološkog kriminala, *Poslovna ekonomija*, vol. 6, br. 2, str. 97-118.
17. Rogers, M., Seigfried, K., Tidke, K. (2006). *Self-reported computer criminal behavior: A psychological analysis*, From the proceedings of The Digital Forensic Research Conference DFRWS 2006 USA Lafayette, IN (Aug 14th - 16th), pp. 116-120.
18. Strategija za borbu protiv visokotehnološkog kriminala za period 2019-2023. godine („Sl. glasnik RS”, br. 71 od 25. septembra 2018. godine)
19. Vasić, G., Šarić, B., Jovanić, V. (2012). Kompjuterski kriminalitet, *Zbornik radova Međunarodne naučnostručne konferencije „Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal”*, Laktaši, str. 181-192.
20. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Sl. glasnik RS”, br. 61/2005 i 104/2009)

CIP - Каталогизација у публикацији
Библиотеке Матице српске, Нови Сад

007.5:34(082)

**НАУЧНИ скуп Правнички дани проф. др Славко Царић (16 ;
2019 ; Нови Сад)**

Pravo i digitalne tehnologije : [zbornik referata sa XVI
Međunarodnog naučnog skupa "Pravnički dani prof. dr Slavko
Carić", 26-28. septembra 2019. godine u Novom Sadu] = Law and
digital technology : [proceedings of the 16th International Scientific
Conference "Legal Days Prof. Slavko Carić Ph.D.", September 26-28,
2019 in Novi Sad] / priredio, edited by Marko Carić. - Novi Sad :
Univerzitet Privredna akademija : Pravni fakultet, 2019 (Novi Sad :
Feljton). - 386 str. ; 24 cm

Tiraž 80. - Napomene i bibliografske reference uz tekst. - Bibliografija
uz svaki rad. - Rezime na engl. jeziku uz većinu radova.

ISBN 978-86-6019-103-0

a) Информације - Правна заштита - Зборници

COBISS.SR-ID 330571527