Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

PRETRESANJE UREĐAJA ZA AUTOMATSKU OBRADU PODATAKA I AUTOMATSKO RAČUNARSKO PRETRAŽIVANJE PODATAKA

SEARCH AND SEIZURE OF THE AUTOMATIC DATA PROCESSING DEVICE AND AUTOMATIC COMPUTER DATA SEARCH

Pregledni naučni rad

Ivanović Zvonko[405]
Žarković Milan[406]

Abstrakt

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): U primeni novih metoda za otkrivanje izvršilaca krivičnih dela, sve više se, kao osnovni metodi, javljaju računarski metodi otkrivanja, pronalaženja i obezbeđenja digitalnih relikata krivičnih dela i njihovih izvršilaca ili veza sa njima.

Ciljevi rada (naučni i/ili društveni): U Republici Srbiji je nekoliko metoda prepoznato kao veoma ekstenzivnih i značajno zadirućih u slobode i prava građana, te su, iz tih razloga, oni i njihova primena definisani u okvirima dokaznih, odnosno, posebnih dokaznih radnji.

Metodologija/Dizajn: Konkretno u pitanju su pretresanje uređaja za automatsku obradu podataka, kao i automatsko pretraživanje podataka. Osnovni *ratio* ovakvog restriktivnog odnosa prema svemu što je tehnički naprednije nije nov u istoriji krivičnog zakonodavstva. Svaka nova metoda i mera je prema stavu zakonodavaca uvek prihvatana uz zadršku i sa značajnom rezervom. Ovakvo shvatanje i stav su razumljivi ali treba ukazati na neke aspekte takvog tretmana, koji nisu neophodni za pojedine aktivnosti u vezi sa digitalnim podacima. Ograničenja istraživanja/rada:

Opravdanost istraživanja/rada: Naime, ovakvim radnjama se teško mogu izmeniti sadržaji digitalnih podataka, a da se isto ne primeti od strane stručnog lica. Šta više, moguće je putem postojećih načina i metoda evidentiranje aktivnosti utvrditi svaku radnju koja je preduzeta na uređaju sa velikom preciznošću. Drugi razlozi tiču se obima podataka.

Rezultati/Nalazi: Kada se malo više udubi u značenje, domašaje, svrhu i logiku shvatanje restriktivnog odnosa prema ovim radnjama gubi smisao.

Generalni zaključak: U ovom radu pokušavamo da prikažemo značaj i domašaj ovih radnji i njihove limite – ograničenja i krajnje obuhvate, kako bi prikazali nepotrebnost limita kojima ih daruje zakonodavac.

[405] Vanredni profesor na KPU, e-mail:zvonko31@gmail.com
[406] Redovni professor na KPU, e-mail:milan.zarkovic@kpu.edu.rs

Ključne riječi:
automatsko računarsko pretraživanje podataka, pretresanje računara, digitalni dokazi, elektronsko okruženje, dokazne radnje

Abstract
In the implementation of new methods for the detection of perpetrators of criminal acts, the methods of detection, finding and providing digital relics of criminal offenses and their perpetrators or connections with them are becoming more and more the basic methods. In the Republic of Serbia, several methods have been recognized as very extensive and significantly embittered in the freedoms and rights of citizens, and for these reasons, they and their application have been defined within the frames of evidence or special evidentiary actions. Specifically, they include automatic data processing utensils (devices) search (or Scanning the automatic data processing device) as well as automatically searching already processed data. The basic ratio of such a restrictive relationship to everything that is technically more advanced is not new in the history of criminal legislation. Every new method and measure, according to the attitude of the legislators, is always accepted with delay and significant reserve. This understanding and attitude are understandable, but one should point out some aspects of such treatment, which are not necessary for certain activities related to digital data. When it comes to a little more meaning, scope, purpose, and logic, understanding the restrictive attitude toward these actions loses its meaning. Namely, such actions can hardly change the contents of digital data, without being noticed by an expert. What's more, it is possible through the existing ways and methods to record activities to determine any action taken on a device with high precision. Other reasons concern data volume. In this paper, we try to show the importance and scope of these actions and their limitations and ultimate coverage, in order to show the unnecessary limits imposed by the legislator.

Keywords
automatic computer search of data, computer search, digital evidence, electronic environment, evidence actions

Uvod

Potreba za inkriminisanjem radnji izvršenih protiv, odnosno, upotrebom računara – nastala je još u vreme kada su računari postali dostupni široj javnosti. U svetu, već 1973. godine, otpočinje se sa pravnim regulisanjem kompjuterskog kriminaliteta, kada je u Švedskoj donet propis koji poznaje krivično pravnu zaštitu od kompjuterskog kriminaliteta, gde je u čl. 21. predviđeno krivično delo „neovlašćeni programski pristup". Tako su, ostale države, implementirale i razvile sopstvene propise koji bliže uređuju ovu materiju. Tek kasnije dolaze u fokus i radnje kojima se pribavljaju dokazi u elektronskom vidu sa ovakvih uređaja.

Narodna skupština Republike Srbije je početkom 2009. godine, posebnim zakonima ratifikovala Konvenciju Saveta Evrope o visokotehnološkom kriminalu i Dodatni protokol uz

tu Konvenciju, koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko kompjuterskih sistema, nakon čega su doneti i drugi važni propisi iz ove oblasti.

Poznato je da je Konvencija Saveta Evrope o visokotehnološkom kriminalu potpisana u Budimpešti 23. novembra 2001. godine[407], dok je Dodatni protkol koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko kompjuterskih sistema[408] sačinjen u Strazburu 28. januara 2005. godine. Takođe, Republika Srbija je 16. aprila 2005. godine u Helsinkiju potpisala ovu Konvenciju o visokotehnološkom kriminalu i Dodatni protokol uz tu Konvenciju, ali ih sve do 2009. godine nije ratifikovala. Važan deo Konvencije o visokotehnološkom kriminalu posvećen je obavezama država da stvore normativne pretpostavke za uvođenje dodatnih procedura i ovlašćenja, kako bi se omogućilo efikasno otkrivanje i procesuiranje slučajeva kompjuterskog kriminala.

Konvencija o visokotehnološkom kriminalu, usvojena u Budimpešti, 23. novembra 2001, jer su države svesne rizika da se kompjuterske mreže i elektronske informacije mogu, takođe, koristiti za izvršenje krivičnih dela i da dokazni materijali koji se odnose na takve prestupe mogu biti uskladišteni u tim mrežana ili prenošeni preko njih. Konvencijom se, po prvi put, uvode pravne norme koje se tiču kršenja prava intelektualne svojine, prevara izvršenih korišćenjem računara, zloupotrebe maloletnika u pornografske svrhe, protivpravnog pristupa zaštićenom računaru i računarskoj mreži, presretanju podataka, takođe se propisuju i radnje i mere, kako materijalno, tako i procesnopravne prirode, koje su usmerene ka negativnom sankcionisanju društveno štetnog ponašanja u ovoj oblasti. Ovom Konvencijom omogućava se primena savremenih istražnih metoda prilikom otkrivanja i gonjenja izvršilaca krivičnih dela, kao što su pretraga računarskih mreža i presretanje računarskih podataka i ona, trenutno, predstavlja jedini međunarodno pravno priznati pravni instrument u oblasti visokotehnološkog kriminala. Konvencija Saveta Evrope o visokotehnološkom kriminalu pre svega se zalaže za usklađivanje domaćih materijalnih krivičnopravnih odredbi u oblasti računarskog kriminala i omogućavanje domaćem pravnom okviru da nadležnim državnim organima pruži ovlašćenja koja su neophodna za otkrivanje i gonjenje izvršilaca ovih krivičnih dela, kao i uspostavljanje brzog i efektivnog okvira međunarodne saradnje u ovoj oblasti. Sastoji se iz tri dela, pri čemu prvi sadrži materijalno pravne odredbe, drugi procesno – pravne, treći odredbe kojima se reguliše međunarodna saradnja. Cilj propisivanja materijalnopravnog okvira Konvencijom jeste poboljšanje zakonskih odredbi radi sprečavanja i gonjenja specifične vrste kriminaliteta koji se izvršava pomoću računara i u računarskom okruženju uz korišćenje računarskih mreža. Krivična dela koja su određena konvencijom su: neovlašćeni (protivpravni) pristup, neovlašćeno (protivpravno) presretanje, ometanje toka podataka, ometanje rada

[407] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 poslednji put pristupljeno 15.08.209. god.
[408] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 poslednji put pristupljeno 15.08.209. god.

računarskog sistema, zloupotreba uređaja, falsifikovanje izvršeno pomoću računara, prevara izvršena pomoću računara, krivična dela dečje pornografije (iskorišćavanja dece i maloletnika u pornografske svrhe), i krivična dela autorskih i srodnih prava.

Zemlje koje su ratifikovale Konvenciju obavezne su da donesu procesnopravne norme radi uspostavljanja i primene ovlašćenja, a čije će propisivanje biti u skladu sa domaćim pravnim okvirom. Ove odredbe mogu uključivati i takvu vrstu zaštitnih odredbi koje su na domaćem - nacionalnom nivou predviđene u okviru Ustava, pravnog poretka, sudskog i javnotužilačkog sistema, i slično.

Kada govorimo o procesnim odredbama, predviđeno je: 1. hitno čuvanje pohranjenih podataka, 2. hitno čuvanje i delimično otkrivanje podataka o saobraćaju, 3. naredbu za dostavljanje, 4. pretragu i zaplenu računarskih podataka, 5. prikupljanje podataka o saobraćaju u realnom vremenu, 6. presretanje podataka o saobraćaju.

U trećem odeljku, Konvencija sadrži odredbe koje se odnose na tradicionalne i računarski povezanepravne instrumente međusobne saradnje, tj. međunarodne saradnje u krivičnom pravu, kao i pravila zauspostavljanje takozvane „7/24“ mreže za hitno reagovanje radi omogućavanja brze i efektivne saradnje izmeđunadležnih organa strana potpisnica (Stamenković i dr. 2017:17).

Zakonodavni okvir

Narodna skupšina Republike Srbije usvojila je Zakon o potvrđivanju Dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu ("Sl. glasnik RS", br. 19/2009) koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sitema, koji je objavljen 18. marta 2009. godine u Službenom glasniku Republike Srbije. U skladu sa Dodatnim protokolom pod pojmom "rasistički i ksenofobični materijal" označavaće se svaki pisani materijal, slika ili drugo predstavljanje ideja ili teorija koje zagovaraju, promovišu ili podstiču mržnju, diskriminaciju ili nasilje, protiv bilo kojeg pojedinca ili grupe pojedinaca, zasnovano na rasi, boji kože, naslednom, nacionalnom ili etničkom poreklu, kao i veri, ako se koriste kao izgovor za bilo koji od tih faktora. U poglavlju II pod nazivom „Mere koje treba da se preduzmu na nacionalnom nivou“ u članu 3. pod nazivom „Širenje rasističkog i ksenofobičnog materijala preko računarskih sistema“ u stavu 1. stoji da države potpisnice treba da usvoje zakonodavne i druge mere, neophodne da bi se kao krivično delo u domaćem pravu propisalo kao kažnjivo ako je izvršenosa namerom i protivpravno: širenjem ili na drugi način činjenjem dostupnim javnosti, preko računarskog sistema, rasističkog i ksenofobičnog materijala. U stavu 2. stoji da strana ugovornica može da zadrži pravo da krivična odgovornost ne postoji za ponašanje propisano u stavu 1. ovog člana, kada materijal, kako je propisano u članu 2. stav 1. zagovara, promoviše ili podstiče diskriminaciju, koja nije povezana sa mržnjom ili nasiljem, pod uslovom da su dostupni drugi delotvorni pravni lekovi. Takođe, stoji i da potpisnice mogu da zadrže pravo da ne primenjuju stav 1. ovog člana na one slučajeve diskriminacije za koje,

usled uspostavljenih načela u domaćem pravnom sistemu u vezi sa slobodom izražavanja, ne mogu da obezbede efikasne pravne lekove kako je pomenuto u stavu 2.

Napred navedenim se, između ostalog, propisuju i one radnje koje su osobene za govor mržnje na internetu, kao što je javno izlađanje poruzi lica ili grupe zbog pripadnosti određeno rasi, boji kože, veroispovesti, etičkog porekla ili drugog ličnog svojstva. Inkriminišu se radnje kojima se izaziva ili pospešuje nacionalna, veska ili rasna netrpeljivost među narodima ili etičkim zajednicama koje žive u Republici Srbiji.

Zakonodavac Republike Srbije je u periodu od aprila 2005. do marta 2009. godine usvojio više propisa u kojima je implementirao Konvenciju Saveta Evrope o suprotstavljanju sajberkriminalu, (kod nas odomaćenu kao visokotehnološki kriminal) CETS 185 i Dodatni protokol CETS 189 u naš pravni sistem. Najvažniji među njima su: Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala ("Sl. glasnik RS", br. 61/2005 i 104/2009), 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), Zakon o odgovornosti pravnih lica za krivična dela ("Sl. glasnik RS", br. 97/2008), Zakonik o krivičnom postupku – ZKP ("Sl. glasnik RS", br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014 i 35/2019), Zakon o policiji ("Sl. glasnik RS", br. 6/2016, 24/2018 i 87/2018), Zakon o autorskim i srodnim pravima ("Sl. glasnik RS", br. 104/2009, 99/2011, 119/2012 i 29/2016 - odluka US), Zakon o elektronskim telekomunikacijama ("Sl. glasnik RS", br. 44/2010, 60/2013 - odluka US, 62/2014 i 95/2018 - dr. zakon), Zakon o elektronskom potpisu ("Sl. glasnik RS", br. 94/2017), Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine ("Sl. glasnik RS", br. 46/2006 i 104/2009 - dr. zakoni).

Krivični zakonik Republike Srbije sadrži određen broj krivičnih dela koji bi mogla biti obuhvaćena pojmom visokotehnološkog kriminala. Ova krivična dela možemo podeliti u dve grupe. Prvu grupu čine krivična dela kojima se povređuje sam sistem kompjuterske tehnologije oštećenjem ili uništenjem računarskog podatka ili programa, ili ometa njihovo korišćenje, ili se vrši neovlašćen pristup računarskoj mreži i obradi elektronskih podataka. U drugu grupu se ubrajaju dela kod kojih se koristi računarska tehnologija, kako bi se pomoću nje vršila krivična dela. Sva krivična dela iz ovih grupa čine se sa umišljajem.

Radi suzbijanja nedozvoljenih ponašanja u vezi sa upotrebom informacionih tehnologija kao *ultima ratio* u Krivičnom zakoniku u glavi 27. je propisano osam krivičnih dela protiv bezbednosti računarskih podataka

Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, po prvi put, se uspostavljaju zakonski okviri za uspostavljanje institucija za borbu protiv visokotehnološkog kriminala. Takođe, ovim zakonom uređuje se obrazovanje, organizacija, nadležnost i ovlašćenja posebnih organizacionih jedinica državnih organa radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela određena ovim zakonom.

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala primenjuje se radi otkrivanja, krivičnog gonjenja i suđenja za: 1) krivična dela protiv bezbednosti računarskih podataka određena Krivičnim zakonikom;

2) krivična dela protiv intelektualne svojine, imovine, privrede i pravnog saobraćaja, kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj primeraka autorskih dela prelazi 2000 ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara;

3) krivična dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, koja se zbog načina izvršenja ili upotrebljenih sredstava mogu smatrati krivičnim delima visokotehnološkog kriminala, u skladu sa članom 2. stav 1. ovog zakona.

U navedenim pravnim i instituciopnalnim okvirima u toku 2007. godine, u Ministarstvu unutrašnjih poslova Republike Srbije u Službi za borbu protiv organizovanog kriminala obrazovano je Odeljenje za borbu protiv visokotehnološkog kriminala. Ovo odeljenje sastoji se od dva odseka: Odsek za suzbijanje kriminaliteta u oblasti intelektualne svojine i Odsek za suzbijanje elektronskog kriminala.

Za postupanje u predmetima krivičnih dela na osnovu Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala nadležno je Više javno tužilaštvo u Beogradu za teritoriju Republike Srbije. U Višem javnom tužilaštvu u Beogradu obrazovano je posebno odeljenje za borbu protiv visokotehnološkog kriminala tj. Posebno tužilaštvo. Radom Posebnog tužilaštva rukovodi Posebni tužilac za visokotehnološki kriminal. Posebnog tužioca postavlja Republički javni tužilac iz reda zamenika javnih tužilaca koji ispunjavaju uslove za izbor za zamenika višeg javnog tužioca, uz pismenu saglasnost lica koje se postavlja. Prednost imaju zamenici javnih tužilaca koji poseduju posebna znanja iz oblasti informatičkih tehnologija. U Posebnom tužilaštvu pored rukovodioca angažovana su još dva zamenika Višeg javnog tužioca specijalizovana za ovu oblast kao i dva tužilačka savetnika uz prateće administrativno osoblje. Od osnivanja početkom 2006. godine zaključno sa 1. oktobrom 2011. godine, Posebno tužilaštvo za visokotehnološki kriminal je postupalo ili postupa u preko 1700 predmeta u okviru svoje nadležnosti[409].

U našem zakonodavstvu, primena specijalnih istražnih tehnika u dužem periodu bila ograničena samo na dostavljanje podataka o stanju poslovnih i ličnih računa osumnjičenih, ali samo za krivična dela za koja je propisana kazna zatvora od najmanje četiri godine. Zbog toga se pribavljanje elektronske pošte osumnjičenog, odnosno, okrivljenog od

[409] http://www.beograd.vtk.jt.rs/ poslednji put pristupljeno 20.08.2019.god.

internet provajdera, uz naredbu suda (po pravilu sudije za prethodni postupak), sprovodi na taj način što se vrši predaja pisama, telegrama i drugih pošiljki od strane subjekata registrovanih za prenos informacija, upućenih okrivljenom ili koje on odašilje, ako postoje okolnosti zbog kojih se može osnovano očekivati da će date pošiljke poslužiti kao dokaz u krivičnom postupku. Poštanska, telegrafska i druga preduzeća, društva i lica registrovana za prenošenje informacija su dužna da ovlašćenim službenicima policije omoguće izvršenje navedenih mera. Iako su se na ovaj način prikupljali dokazi postojali su problemi u praksi zbog specifičnosti načina pribavljanja dokaza za tako specifična krivična dela, budući da se do njih često često dolazi monitoringom na mreži u realnom vremenu (''*on line*'').

Za suzbijanje visokotehnološkog kriminala značajno je i to što u ZKP –u (član 147. stav 3.) u predmete koji se mogu privremeno oduzeti spadaju i uređaji za automatsku obradu podataka i oprema na kojoj se čuvaju ili se mogu čuvati elektronski zapisi. Lice koje se koristi ovim uređajima i opremom dužno je da organu koji vodi postupak, na zahtev suda, omogući pristup i da pruži obaveštenja potrebna za njihovu upotrebu. Ono što možemo odrediti kao nedostatak ovde je to da za propuštanje ove obaveze nije predviđena sankcija. Pre oduzimanja ovih predmeta organ koji vodi postupak će u prisustvu stručnog lica izvršiti pregled uređaja i opreme i popisati njihovu sadržinu. Najzad, ako korisnik prisustvuje ovoj radnji može staviti primedbe.

U teoriji je izražen i stav da je od posebnog značaja za borbu protiv visokotehnološkog kriminala mogućnost da sudija za prethodni postupak, na pisani i obrazloženi predlog javnog tužioca, naredi nadzor i snimanje telefonskih i drugih razgovora ili komunikacija drugim tehničkim sredstvima (npr. telefaksom, teleprinterom, pejdžerom, elekronskom poštom - Internetom i dr.) onih lica za koja postoji osnovana sumnja da su sama ili sa drugim licima izvršila određena krivična dela. S tim u vezi treba naglasiti da se za otkrivanje nekih od tipičnih dela visokotehnološkog kriminala može koristiti i mera računarskog pretraživanja podataka, koja je značajna zbog sve izraženije kompjuterizacije ličnih i drugih podataka, te velikih mogućnosti koji ti podaci pružaju u vezi pribavljanja dokaza. Ovu radnju, po naređenju sudije za prethodni postupak, sprovode: kriminalistiška policija, Bezbednosno-informativna agencija, Vojno-bezbednosna agencija, organi carinske službe ili drugi državni organi, odnosno druga pravna lica koja na osnovu zakona vrše određena javna ovlašćenja. Mera može trajati najviše tri meseca, a zbog neophodnosti daljeg prikupljanja dokaza može se izuzetno produžiti još najviše dva puta u trajanju od po tri meseca. Računarsko pretraživanje podataka sastoji se u automatskom pretraživanju već pohranjenih, ličnih i sa njima neposredno povezanih, podataka i njihovom automatskom poređenju sa podacima. Po svojoj suštini ovo je „ negativna raster“ potraga koja doprinosi eliminaciji određenih lica iz kruga osumnjičenih automatizovanim pretragama kroz policijske, administrativne i druge evidencije. Drugim rečima, ovaj metod eliminiše određena lica iz kruga onih koja se služe lažnim identitetom, tuđim kreditnim karticama i tome slično.

Računarsko pretraživanje podataka

Računarsko pretraživanje podataka i njihova elektronska obrada može se preduzeti ako postoje osnovi sumnje da je učinjeno krivično delo za koja je posebnim zakonom određeno da postupa javno tužilaštvo posebne nadležnost, ako se na drugi način ne mogu prikupiti dokazi za krivično gonjenje ili bi njihovo prikupljanje bilo znatno otežano. Izuzetno se može odrediti i ako postoje osnovi sumnje da se priprema neko od krivičnih dela za koja je posebnim zakonom određeno da postupa javno tužilaštvo posebne nadležnost, a okolnosti slučaja ukazuju da se na drugi način delo ne bi moglo otkriti, sprečiti ili dokazati, ili bi to izazvalo nesrazmerne teškoće ili veliku opasnost. Suština ovog metoda je slobodan pristup policije svim evidencijama koje se vode automatizovano, što odudara od načela zaštite prava na privatnost građana i informatičko samoodređenje.

Opšti uslovi za određivanje posebnih dokaznih radnji propisani su u čl. 161. ZKP-a. U literaturi se susreću shvatanja po kojima uslovi za primenu posebnih dokaznih radnji predstavljaju činjenični i pravni osnov za određivanje ovih radnji. Činjenični osnov predstavlja stepen verovatnoće (osnovi sumnje) da je određeno lice učinilo krivično delo za koje se ove dokazne radnje mogu odrediti. Standard na kome insistira Evropski sud za ljudska prava u svojim odlukama jeste usmerenost posebnih dokaznih radnji prema određenom licu za koje postoji sumnja da priprema ili je izvršilo krivično delo. Taj sud, prema objavljenim presudama, smatra da nacionalno zakonodavstvo koje se bavi specijalnim istražnim metodama mora da osigura adekvatne i efikasne garancije da neće doći do zloupotreba prilikom primene tih metoda. U tom smislu, nije dozvoljen opšti nadzor primenom ovih mera, već nadzoru mogu da budu izložene isključivo osumnjičene i „pretpostavljenje" kontakt osobe (European Court of Human Right, 2019). Pravni osnov za određivanje ovih dokaznih radnji, kao što je već navedeno, sadrži element restriktivnosti, dakle, ove radnje se mogu odrediti samo ako se na drugi način ne mogu prikupiti dokazi za krivično gonjenje ili bi njihovo prikupljanje bilo znatno otežano (Subotić, D, 2013). Neki autori, ipak, uslove za primenu posebnih dokaznih radnji identifikuju kao materijalne i formalne. Materijalni uslov odnosi se na vrste krivičnih dela za koje je dozvoljeno da se primeni radnja, kao i postojanje dokaznih poteškoća koje uskovljavaju primenu posebnih dokaznih radnji. Formalni uslov za primenu radnji sastoji se, takođe, od dva kumulativna elementa. Prvi element čini procesna inicijativa nadležnog javnog tužioca u vidu obrazloženog predloga, a prihvatanje predloga sudije za prethodni postupak, i to u formi naredbe za sprovođenje konkretne posebne dokazne radnje, drugi element formalnog uslova (Ignjatović, Škulić, 2010).

Mera se sastoji u računarskom pretraživanju već pohranjenih ličnih i drugih, sa njima neposredno povezanih podataka i u njihovom automatskom poređenju sa podacima koji se odnose na krivično delo iz čl. 162. st.1 tač. 1. i 2. ZKP i na osumnjičenog, da bi se kao mogući osumnjičeni isključila lica u pogledu kojih ne postoji verovatnoća da su povezana sa krivičnim delom. Naredba sadrži podatke o osumnjičenom, zakonski naziv krivičnog dela, opis podataka koje je potrebno računarski pretražiti i obraditi, označenje državnog organa koji je dužan da sprovede pretragu traženih podataka, obim i vreme trajanja posebne dokazne radnje.

Računarsko pretraživanje podataka može trajati najviše tri meseca, a zbog neophodnosti daljeg prikupljanja dokaza može se izuzetno produžiti još najviše dva puta u trajanju od po tri meseca. Sprovođenje računarskog pretraživanja podataka se prekida čim prestanu razlozi za njegovu primenu. Po završetku računarskog pretraživanja podataka državni organ, odnosno pravno lice dostavlja sudiji za prethodni postupak izveštaj koji sadrži: podatke o vremenu početka i završetka računarskog pretraživanja podataka, podatke koji su pretraženi i obrađeni, podatke o službenom licu koje je sprovelo posebnu dokaznu radnju, opis primenjenih tehničkih sredstava, podatke o obuhvaćenim licima i rezultatima primenjenog računarskog pretraživanja podataka. Sudija za prethodni postupak će izveštaj dostaviti javnom tužiocu. Ako javni tužilac ne pokrene krivični postupak u roku od šest meseci od dana kada se upoznao sa materijalom prikupljenim korišćenjem posebnih dokaznih radnji ili ako izjavi da ga neće koristiti u postupku, odnosno da protiv osumnjičenog neće zahtevati vođenje postupka, sudija za prethodni postupak će doneti rešenje o uništenju prikupljenog materijala. (Čl. 163).

O donošenju rešenja sudija za prethodni postupak može obavestiti lice prema kome je sprovedena posebna dokazna radnja iz člana 166. ZKP ako je u toku sprovođenja radnje utvrđena njegova istovetnost i ako to ne bi ugrozilo mogućnost vođenja krivičnog postupka. Materijal se uništava pod nadzorom sudije za prethodni postupak koji o tome sastavlja zapisnik.

Ako je pri preduzimanju posebnih dokaznih radnji postupljeno suprotno odredbama ovog zakonika ili naredbi organa postupka, na prikupljenim podacima se ne može zasnivati sudska odluka, a sa prikupljenim materijalom se postupa u skladu sa članom 84. stav 3. ZKP.

Digitalni dokazi

Sa razvojem tehnike i tehnologije pojavile su se novi načini njihove zloupotrebe, kao što je kompjuterski kriminalitet. Razvoj informacione tehnologije obeležava ogroman protok digitalnih podatakau vidu elektronskih (računarskih) zapisa, a koji se nalaze u računaru ili se prenose putem njega, a kao takvi mogu biti ključni dokaz u otkrivanju i dokazivanju zloupotrebe računara i računarskih mreža. Glavni cilj istrage u oblasti kompjuterskog kriminaliteta je, kao i slučaju klasičnog kriminala, izgraditi za pravosudne organe neoboriv ili čvrst dokaz krivice ili dokaz za oslobađanje osumnjičenog, i/ili pravedno sankcionisanje učinjenog dela. Direktan (neposredan) dokaz u slučaju kompjuterskog kriminala gotovo je nemoguće obezbediti, ali moguće je izgraditi čvrst digitalni dokaz, bez tzv. pukotina,od niza posrednih dokaza. Savremeni pojavni oblici kriminaliteta traže i inovacije u vezi sa metodikom otkrivanja krivičnih dela, odnosno pribavljanje dokaza u elektronskoj formi, odnosno elektronskih, softverskih ili kompjuterskih dokaza. Osnovna funkcija kompjuterskog sistema je obrada i distribucija podataka u elektronsku sredinu. Elektronski podaci predstavljaju niz magnetskih tačkica na stalnoj ili privremenoj memoriji računara i oni mogu predstavljati primarni dokaz. U takvom obliku ne mogu se čulno opaziti, ali mogu

se koristiti kao dokaz. Moguće ih je presnimiti na drugi oblik elektronske memorije: tvrdi ili meki disk (flopi disketu), optički kompakt disk, eksternu memoriju i tako sačuvati u neizmenjenom obliku, a da bi se čulno opazili, možemo ih preformulisati u čoveku čitljive oblike u tekst, fotografiju, video zapis, zvuk ili drugi oblik koji je pogodan za ljudsko opažanje i razumevanje (Komlen Nikolić i dr. 2010:217).

Može se uočiti da zapravo postoje dve kategorije elektronskih zapisa: one koje je računar generisao i one koji su u računaru samo arhivirani. U prvoj kategoriji elektronskih zapisa su oni zapisi koje je sam računar stvorio nezavisno od korisnika (npr. zapisi provajdera internet usluga koji se tiču identifikacije korisnika prilikom uključuvanja na mrežu). Drugu kategoriju čine zapisi koje je kreirao korisnik a koji se u računaru samo čuvaju (npr. e-mail poruke) (Banović, 2006).

U postupku prikupljanja i analize digitalnih dokaza potrebno je da svi generalni forenzički i proceduralni principi budu primenjivani; da pre, u toku i posle uzimanja digitalnih dokaza ni jedna preduzeta akcija ne dovede do izmene digitalnog dokaza; samo stručno lice može pristupi originalnom digitalnom dokazu, kada se za to ukaže potreba; sve aktivnosti koje se odnose na sakupljanje, skladištenje, pristup ili transfer digitalnih dokaza moraju biti potpuno dokumentovane, sačuvane i raspoložive zastavljanje na uvid, bilo kojoj zainteresovanoj strani u sporu; lice koje rukuje digitalnim dokaznim materijalom je odgovorno za sve aktivnosti u odnosu na digitalni dokaz, kada je isti u njegovom posedu; izuzeti dokazi se moraju dobro skladištiti.

Policijski službenik koji prikuplja dokaze sa računara ili računarske mreže, mora pravilno postupiti i prikupiti te podatake, u suprotnom ti podaci ne mogu biti iskorišćeni u sudskom postupku. Digitalni dokaz je kompjuterski podatak koji može potvrditi da je izvršeno krivično delo, ili ukazuje na uzročno – posledičnu vezu između krivičnog dela i žrtve, krivičnog dela i njegovog izvršioca. U većini slučajeva, kod ovakvih krivičnih dela, informacija koja je pohranjena na kompjuteru može biti jedini trag, koji će istragu odvesti na pravi put. Veoma mali broj ovakvih dokaza moguće je otkriti ''klasičnim alatima'', većina se otkriva samo posebnim alatima. U odnosu na materijalne dokaze, digitalni dokazi imaju nekoliko prednosti:

- od digitalnih dokaza je moguće napraviti tačnu kopiju koja se naknadno može istraživati kao da se radi o originalu, dok je kod materijalnih dokaza to gotovo nemoguće. Na taj način se izbegavaju oštećenja koja bi mogla nastati na originalu prilikom istraživanja;
- pomoću pravilnih alata moguće je vrlo lako odrediti da li je digitalni dokaz menjan ili uništen, jednostavno upoređujući ga sa originalom;
- digitalni dokaz je vrlo teško uništiti (čak i onda kada su ''obrisani'', digitalni dokazi se mogu povratiti na kompjuterski disk ili neki drugi medij za pohranu podataka);

- digitalni dokaz je jednostavno pohraniti, a zbog lakoće izrada kopija, gotovo ih je nemoguće uništiti ili izgubiti;
- digitalnim dokazima se može lako manipulisati.

Obezbeđivanje digitalnih dokaza

Da bi se došlo do čvrstih dokaza potrebno je na mestu događaja utvrditi šta se stvarno desilo, da li je nastala šteta i koliki je njen iznos, kao i da li je akt koji se desio, u stvari, krivično delo iz oblasti visokotehnološkog kriminala. Dokaze treba prikupljati na mestu događaja uz objektivan pristup. Policijski službenik koji prvi stigne na mesto događaja potrebno je da zna da se podaci ili informacije mogu izgubiti u toku procesa isključivanja računara i da mora obezbediti mesto događaja do dolaska stručnog lica koje će pre isključivanja računara pronaći i presnimiti potrebne podatke, jer se može desiti da se posle isključivanja ne može doći do njih (npr. vlasnik šifre za pristup odbija saradnju ili ga je nemoguće locirati). Takođe, podaci uskladišteni na hard disku se lako mogu izmeniti, a pojedinim podacima se može pristupiti samo u određeno vreme (npr. šifrovani podaci). Podaci se mogu koristiti kao dokazi u postupku samo ako su adekvatno izuzeti i ako zadovoljavaju kriterijume u sudskom veštačenju. U ovom slučaju posredni dokaz je onaj dokaz, koji se sakupi analizom samog softvera, računara i/ili računarske mreže, a da bi bio prihvatljiv za sud, mora biti takav da potvrđuje hipotezu o čvrstom dokazu, ili da je pobija.

Digitalni dokazi moraju zadovoljiti i sve ostale zahteve pravosudnih organa, koji se odnose na sudske dokaze i to:

- ako je potrebno koristiti kopiju, ona mora biti najbolja,
- ako je original na raspolaganju onda kopija ne važi,
- kopija može zadovoljiti sve zahteve za izvođenje dokaza ako postoji orginalna datoteka u računaru za upoređenje,
- sudski veštak za IT mora posvedočiti kako je kopija napravljena, kao i druge detalje rukovanja sa datotekom i kopijom.

Što se tiče procesnog aspekta, uviđaj je najznačajnija dokazna radnja koju preduzima organ krivičnog postupka po službenoj dužnosti, kada je za utvrđivanje ili razjašnjenje kakve važne činjenice potrebno neposredno opažanje organa postupka. Neposredno opažanje se vrši čulnim opažanjem, ali se mogu koristiti određena sredstva (kao što su hemijska sredstva, fotoaparat i sl.), koja omogućavaju da se tragovi učine vidljivim i da se fiksiraju. U tom cilju moguće je izvršiti određena merenja, opisivanjem, upoređivanjem i fiksiranjem, kako bi se mogao pribaviti relevantan dokaz. Ove aktivnosti organ postupka može raditi sam ili uz pomoć stručnih lica, čijom pomoći će on potpunije razumeti stanje i situacije na licu mesta.

Pored dokaznih radnji za otkrivanje i dokazivanje krivičnih dela koriste se i operativno taktičke ili potražne radnje a koje omogućavaju sprovođenje radnji koje imaju dokazni značaj.

Za prikupljanje dokaza najčešće se koristi uviđaj računara, a kako je zakonodavac uveo posebnu radnju pretresanja uređaja za automatsku obradu podataka, kao i opreme na kojoj se čuvaju ili se mogu čuvati elektronski zapisi (preduzima se na osnovu naredbe suda i, po potrebi, uz pomoć stručnog lica) postavlja se pitanje razlike između ove dve radnje. Pretresanje računara i uređaja nosilaca digitalnih tragova može se odrediti kao najširi oblik zahvatanja (zadiranja) u prava i slobode. Prema Zakoniku o krivičnom postupku ovo nije ni potražna radnja, ni posebna dokazna radnja, već dokazna radnja, i sprovodi se na osnovu naredbe suda (sudije za prethodni postupak) a na obrazloženi predlog javnog tužioca. Kao blaži oblik radnje koja zadire u slobode i prava čoveka sprovodio bi se uviđaj i to kao dokazna radnja. Prva radnja koja bi predstavljala vid najblažeg zadiranja u privatnost a sprovodila bi se nakon saznanja za delo i učinioca je radnja obezbeđenja mesta kriminalnog (krivičnog) događaja, kao preduslov vršenja uviđaja, kao potražna ili operativno – taktička mera i radnja. Najviši stepen uslova zadiranja u slobode i prava vezuje se za posebne dokazne radnje[410].

U cilju obezbeđenja dokaza moguće je pribaviti evidencije i podatke provajdera komunikacionih usluga. Sve korporacije koje obavljaju delatnost pružanjem internet usluga u cilju omogućavanja bilo kakvog oblika komunikacije trebalo bi smatrati „telekomunikacionim operaterima“. Zahtev za dobijanje podataka mora biti u skladu sa Zakonikom o krivičnom postupku i Zakonom o elektronskim komunikacijama.

Podaci o komunikaciji su:

- podaci kojim se utvrđuje identitet lica, sprave ili lokacije sa koje se komunikacija obavlja, obavljena je ili će biti;
- informacije u vezi lica koja koriste neku telekomunikacionu ili poštansku uslugu;
- informacije o licu kojem se pruža ili je već pružena telekomunikaciona ili poštanska usluga.

Zahtevi za dobijenje podataka o komunikacije upućuju se poštanskom ili telekomunikacionom operateru, preko Službe za specijalne istražne metode. Sadržaj komunikacije na osnovu Zakonika o krivičnom postupku se dobija upućivanjem zahteva nadležnom tužilaštvu, radi iniciranja posebne dokazne radnje i dobijanja Naredbe nadležnog suda. Policijski službenici mogu po osnovu Zakonika o krivičnom postupku (čl.161, 162) i Zakona o elektronskim komunikacijama (čl. 128) zahtevati podatke od veb satova koji obavljaju

[410] Reč je o radnjama koje su za nas u ovom radu značajne: automatskom računarskom pretraživanju ličnih i sa njima vezanih podataka i tajnom nadzoru komunikacija

delatnost „onlajn usluga". Veliki broj ovakvih usluga pružaju organizacije, koje se nalaze van naše države i u tom slučaju za dobijanje podataka potrebna je pomoć inostranih policijskih organa[411]. Da bi se sprečio gubitak podataka dok traje postupak međunaronih upita, preporučuje se da se vlasniku podataka (internet provajderu) izda Zahtev za očuvanje podataka kojim će se obavestiti koji su podaci potrebni. Na taj način se podaci čuvaju dok se ne dobije odgovarajući pravni dokument (međunarodna zamolnica za pružanje pravne pomoći). Zahtev za očuvanje podataka se upućuje preko kontakt tačke 24/7 pri Odeljenju za borbu protiv visokotehnološkog kriminala, ili preko Uprave za međunarodnu operativnu policijsku saradnju a u cilju ubrzanja postupka i obezbeđivanja podataka neophodnih za zamolnicu.

Sa razvojem tehnologije ljudi su počeli da svoje elektronske podatke skladište onlajn, jer im je taj način najjednostavniji za pristup sa bilo kog računara koji ima pristup internetu, mobilnog telefona, laptopa. Ovaj sistem skladištenja podataka naziva se „računarstvo u oblacima" (eng. *computer cloud*). U većini slučajeva kopije fajlova se ne čuvaju na personalnom računaru, već su čuvani u šifrovanom obliku na serverima (dok su na korisničkim računarima isti skladišteni samo restriktivno). Na ovaj način se najčešće skladište elektronske poruke i multimedijalni fajlovi. Prilikom obavljanja razgovora sa osumnjičenim licem, policijski službenik će ga pitati da i ima pristup bilo kom onlajn nalogu gde se mogu pohraniti elektronski podaci. Ukoliko da potvrdan odgovor, trebalo bi od njega tražiti saglasnost za pristup i kopiranje podataka. Ukoliko taj nalog sadrži pohranjene privatne poruke, policijski službenik, pored pristanka vlasnika tog naloga mora da postupi po odredbama iz čl. 152 st.3 i čl. 157 st.4 i st.5 Zakonika o krivičnom postupku, a koje se odnose na pretresanje uređaja za automatsku obradu podataka i sam postupak pretresanja.

Prilikom obavljanja razgovora sa oštećenim licem ili svedokom, potrebno je utvrditi da li poseduju ili kontrolišu neki uređaj, koji može sadržati elektronske dokaze. Kako su isti podložni oštećenju ili uništenju, potrebno je preduzeti mere kako bi se dokazala njihova dokazna verodostojnost. Policijski službenik bi trebao da od oštećenog lica ili svedoka zatraži da sarađuju i pristanu da se uređaj obezbedi kako bi se njegovim veštačenjem moglo doći do dokaza. U slučaju da polcijski službenik od navedenih lica ne dobije saglasnost, onda može da uređaj privremeno oduzme na osnovu čl. 147 st. 3 Zakonika o krivičnom postupku. Kada se policijski službenik zakonito nađe u prostorijama, može da oduzme svaki predmet za koji postoji osnovana sumnja da je dokaz krivičnog dela i da je njegovo oduzimanje neophodno kako bi se sprečilo da uređaj bude oštećen, sakriven, izmenjen ili uništen. Policijski službenik može zahtevati da materijal koji privremeno

[411] U ovakvim slučajeivma koriste se takozvani MLAT-i (*Mutal legal assistance act* – ili zamolnica za međunarodnu pravnu pomoć) koji se koriste u skladu sa zakonom o međunarodnoj pravnoj pomoći u krivičnim stvarima ("Sl. glasnik RS", br. 20/2009).

oduzima bude sačinjen u obliku koji omogućava lak prenos, jasnoću i čitljivost, odnosno da se napravi adekvatna kopija.

Pretresanje uređaja za automatsku obradu podataka i opreme na kojoj se čuvaju ili se mogu čuvati elektronski zapisi preduzima se na osnovu naredbe suda i, po potrebi, uz pomoć stručnog lica.

Kako bi bolje razumeli suštinu obezbeđivanja digitalnih dokaza potrebno je napraviti razliku između uviđaja kao dokazne radnje na računaru od pretresanja računara. Uviđaj računara jeste uviđaj pokretnih stvari koji sprovodi stručno lice u cilju sprečavanja nastanka nepovratnih izmena i oštećenja podataka u računaru, odnosno u mrežnom okruženju. Zakonikom o krivičnom postupku je prvi put regulisano pretresanje uređaja za automatsku obradu podataka i nosilaca digitalnih dokaza i vršenje uviđaja na stvarima. Pre nego što se pristupi uviđaju nad računarima, neophodno je prikupiti što više podataka o vrsti računarskog sistema, hardveru, softveru i operativnom sistemu, konfiguraciji računara uopšte, u cilju da se utvrdi gde su tražene informacije pohranjene i na koji način su obezbeđene.

Pretresanje predstavlja detaljniju radnju u odnosu na uviđaj, iako neminovno radnju uviđaja u većinislučajeva prati i pretresanje. Pretresanjem se direktno zadiranje u srž predmeta pretresanja. Tako se kod pretresanja računara, tableta, telefona ili drugih uređaja za obradu podataka, zadire u privatnost lica na taj način što se primeljuju mnoge alatke kojima se vrše detaljne pretrage uređaja tako što se pretražuju uređaji i sadržina svih memorijskih jedinica se kopira i čuva na nakom od uređaja za skladištenje podataka. To je moguće jer svaki uređaj ostavlja određeni digitalni trag na uređaju sa kojeg nešto izuzima, iako se mogu koristiti *write-blocker* uređaji, koji omogućavaju prikupljanje informacija na hard disku bez stvaranja mogućnosti slučajnog oštećenja sadržaja hard diska. Oni to rade tako što dozvoljavaju da pročitaju naredbe, ali blokiraju naredbe za pisanje, otuda i njihovo ime.

Pre nego što se otpočne sa pretresanjem policijski službenici će prikupiti što više informacija o vrsti, mestu i konekciji svakog računara. Od izuzetnog je značaja da svi policijski službenici koji prisustvuju pretresanju budu dobro informisani, kako ne bi neobučeni policijski službenici uništili ili oštetili dokaze. Pre početka pretresanja potrebno je proveriti da li torba za pretresanje mesta događaja tzv. „torba za upad“ sadrži odgovarajući materijal koji će se koristiti prilikom oduzimanja računara i drugih uređaja za pohranjivanje elektronskih podataka.

Prilikom uviđaja treba ispitati hardverske komponente, pretražiti kompjuterske datoteke i direktorijume, izraditi kopije podataka, zaštititi elektronske zapise koji mogu poslužiti kao dokaz. Uviđaj se sprovodi da se ne bi uticalo na uništenje, oštećenje izmenu tragova i predmeta nastalih izvršenjem krivičnog dela, pa ga je potrebno sprovesti što hitnije i objektivnije. Najveći problem koji se javlja u praksi jeste taj da se prilikom pretresanja

stana i ostalih prostorija zatiču uređaji za automatsku obradu podataka, a policijski službenici ne poseduju adekvatna znanja u vezi toga, pa može doći do uništenja dokaza. Kako bi se u praksi izbegao ovaj problem i definisala odgovornost lica za postupanje sa ovakvim dokaznim materijalom, kao i obezbeđenje lanca dokazivanja, doneta je obavezna instrukcija o prikupljanju elektronskih dokaza. Čuvanje podataka koji se nalaze u radnoj memoriji ovih uređaja RAM ili ROM memoriji je specifična jer oni sadrže informacije o poslednjim pregledanim materijalima sa interneta, odnosno skorijim izmenama pojedinih dokumenata, a njihova postojanost je kratka, pa namernim ili slučajnim gašenjem uređaja ili „čupanjem" iz naponskih instalacija radi prekidanja nekih procesa dolazi do nepovratnog gubitka ovih podataka. U ovakvoj situaciji samo stručno lice može preduzeti mere i, na taj način, bezbedno izuzeti dokaze i ono samo pomaže organu postupka da kvalitetno obavi uviđaj, dok je organ postupka taj koji neposredno opaža činjenice i konstatuje ih. Tragovi i predmeti do kojih se dođe prilikom uviđaja postaju predmet veštačenja, ali ukoliko organ postupka pre sprovođenja uviđaja proceni da bi prisustvo veštaka bilo od koristi za davanje nalaza i mišljenja, može na uviđaj pozvati i veštaka.

Prilikom uviđaja računara, za razliku od pretresanja, adekvatno i potpuno se evidentiraju sve mere i radnje na mestu i virtuelnom okruženju vršenja ove radnje. Na taj način se smanjuje verovatnoća prigovora na postupanje i omogućava se sprovođenje neophodnih analiza nakon vršenja uviđaja. Tako se na mestu događaja može izvršiti audio vizuelno snimanje aktivnosti stručnog lica dok vrši pregled, uviđaj računara ili pretresanje. Ovu radnju prati zapisnik i službena beleška radi potpunijeg objašnjenja postupanja. Organ postupka će angažovati lica koja imaju stručnost i specijalizovana znanja u postupanju sa uređajima za automatsku obradu podataka tj. digitalnim tragovima. Ovako obezbeđeni predmeti i tragovi, zabeleženo stanje računara, kasnije mogu poslužiti u veštačenju ali i pretresanju računara. Prilikom vršenja uviđaja stručno lice može da napravi idealnu kopiju računara, bez menjanja sadržaja ili drugog oblika uticaja na računar, koja može služiti za upoređivanje sa stanjem računara koji se pretresa u nekom kasnijem momentu. Prilikom vršenja uviđaja postoji verovatnoća da je propušten neki važan dokaz, pa se računar može privremeno oduzeti dok traje istraga. Sve prikupljene posredne dokaze treba obraditi kao da su deo celine uz jednaku važnost za dalji postupak, jer se samo na takav način može doći do neoborivog dokaza[412].

Pretresanje uređaja za automatsku obradu podataka i privremeno oduzimanje predmeta

[412] Postoje četiri opšta principa kojih se policijski službenici moraju pridržavati kako bi se sačuvali dokazi:
1. ne treba menjati datum na računaru ili uređaju za skladištenje podataka;
2. ukoliko stručno lice smatra a treba pristupiti prvobitnom datumu na računaru ili uređaju za skladištenje podataka, mora da pruži dokaz uz objašnjenje zašto je to relevantno i na šta ukazuje taj postupak;
3. trebalo bi napraviti i sačuvati trag svih postupaka primenjenih na elektronske dokaze sa računara. Bilo bi poželjno da nezavisna treća strana pregleda ove postupke i dobije isti rezultat;
4. policijski službenik koji zaduži predmet odgovoran je za postupanje ostalih po zakonu i ovim principima.

Privremeno oduzimanje predmeta predstavlja dokaznu radnju čijim se preduzimanjem obezbeđuju predmeti kao izvor materijalnih dokaza. Ova radnja je, često, usko povezana sa pretresanjem stana i lica, ali se može preduzeti i kao samostalna radnja. Cilj ove radnje jeste privremeno oduzimanje predmeta koji se po krivičnom zakoniku mogu oduzeti, kao i predmeti koji mogu poslužiti kao dokaz u krivičnom postupku.

Predmeti koji se po krivičnom zakonu imaju oduzeti jesu predmeti koji su upotrebljeni ili namenjeni za izvršenje krivičnog dela ili predmeti koji su nastali izvršenjem krivičnog dela. S druge strane, predmeti koji mogu poslužiti kao dokaz u krivičnom postupku jesu svi oni koji su nosioci tragova u vezi krivičnog dela ili učinioca. U ove predmete Zakonik izričito ubraja i uređaje za automatsku obradu podataka, kao i uređaje i opremu na kojoj se čuvaju ili se mogu čuvati elektronski zapisi. Da bi se moglo izvršiti pretresanje računara (Odnosno uređaja za automatsku obradu podataka - UAOP) potrebno je da postoji posebna naredba suda.

Lice koje drži predmete mora da omogući organu postupka pristup predmetima, kao i da pruži obaveštenja neohnodna za njihovu upotrebu i da ih preda na zahtev organa. Organ postupka može pregledati predmete, pre nego što se predmeti oduzmu, po potrebi, uz prisustvo stručnog lica. Lice može da odbije da omogući pristup predmetima, pruži obaveštenja koja su neohodna za njihovu upotrebu ili da ih preda, i u tom slučaju, javni tužilac ili sud, takvo lice, može kazniti novčano do 150.000 dinara, u slučaju da nakon toga odbije da ispuni svoju dužnost, može biti kažnjeno istom kaznom još jednom, na šta može uložiti žalbu, koja neće zadržati izvršenje rešenja, i o njoj odlučuje sudija za prethodni postupak ili veće. Ova odredba (čl. 148. ZKP) je od neverovatnog značaja za kasnije situacije. Naime, za pretresanje UAOP neophodno je da postoji naredba za pretresanje, lice treba da obezbedi uputstvo za upotrebu i pristup predmetima, a ako to ne uradi i odbije može biti kažnjeno.

Određene kategorije lica su oslobođene dužnosti da predaju predmete, pruže obaveštenja o njima i omoguće pristup. Tu se pre svega misli na okrivljenog, ali i na lice koje bi svojim iskazom povredilo dužnost čuvanja tajnog podatka ili profesionalne tajne.

Potvrda o oduzetim predmetima izdaće se licu od koga su predmeti oduzeti, koji će se vratiti držaocu kada se otklone razlozi zbog kojih su oduzeti, a nepostoje razlozi za njihovo trajno oduzimanje, ako je predmet neophodno potreban držaocu, uz obavezu da ga na zahtev organa postupka donese. Ako je predmet neophodno potreban držaocu, on mu se može vratiti i pre prestanka razloga zbog kojeg je oduzet, uz obavezu da ga na zahtev organa postupka donese (čl. 151 st. 1 i 2 ZKP). Pojedini predmeti će se vratiti i licu koje je učinilo krivično delo (npr. poklon, odnosno druga korist, koji budu oduzeti od lica koje je primilo mito mogu se vratiti davaocu mita, u slučaju da je učinilac krivičnog dela davanja mita dao mito na zahtev službenog lica i prijavio delo pre njegovog otkrivanja ili saznanja da je delo otkriveno – čl. 368 st. 6 KZ).

Detaljnim opisom predmeta koji se privremeno oduzimaju se predupređuju slučajne ili zlonamerne zamene predmeta veće vrednosti predmetom manje vrednosti, u cilju sticanja koristi, a stvaraju se i pretpostavke za eventualnu procenu i naknadu štete licu od koga je predmet oduzet, a za koji je doneta odluka da se mora vratiti vlasniku (u slučaju oštećenja ili gubitka predmeta).

U slučaju privremenog oduzimanja nosioca digitalnih podataka, odnosno uređaja za automatsku obradu podataka, fizički će se oduzeti nosilac podataka. Ukoliko je reč o digitalnim podacima koji se nalaze u računaru, pametnom telefonu, mrežnoj opremi korisnika, serverima koji nisu u posedu lica od kojeg se oduzimaju, javljaju se drugi načini postupanja. U ovom slučaju način pribavljanja digitalnih podataka, koji se privremeno oduzimaju je drugačiji, pa se tako pribavljanje digitalnih podataka realizuje kroz dokaznu radnju pretresanja uređaja za automatsku obradu podataka (odnosno računara), a može se primeniti dokazna radnja vršenja uviđaja na stvarima, ali do one granice u kojoj bi zatečen računar (telefon, mrežna oprema) mogao oduzeti i naknadno bi se pribavila naredba za pretresanje uređaja za automatsku obradu podataka, jer je samo radnja pretresanja uređaja za automatsku obradu podataka predviđena ZKP –om a ne i uviđaj, i to samo na osnovu naredbe suda. Pregledanje uređaja bi u tom slučaju predstavljalo potražnu aktivnost a koja mora prethoditi svakom oduzimanju predmeta. Zakonikom o krivičnom postupku predviđena je radnja privremenog oduzimanja uređaja za automatsku obradu podataka, pa se na taj način omogućava privremeno oduzimanje kojim se onemogućava menjanje i uticaj na podatke u uređaju a potom može uslediti pretresanje u prostorijama organa postupka, na osnovu naredbe.

Iako nije izričito propisano prisustvo dva punoletna svedoka (opštim pravilima pretresanja jeste ali ne kod pretresanja UAOP), prilikom pretresanja, a radi onemogućavanja zloupotrebe i izmene dokaza, poželjno bi bilo upotrebljavati adekvatne uređaje (komercijalizovana kombinovana softversko – hardverka rešenja, npr. EnCase[413]) koji bi predstavljali i sredstvo pretresanja i fiksiranja radnje – pošto ovakvi metodi sadrže digitalne zapisnike a, ujedno, predstavljaju i oblik nadzora nad vršenjem radnje pretresanja i na taj način bi se uvrstilo obavezno evidentiranje aktivnosti stručnih lica u postupku.

Pretresanje ovih uređaja, u širem smislu, predstavlja fizičko pregledanje spoljašnosti i (digitalne) sadržine uređaja za automatsku obradu podataka (i nosilaca digitalnih podataka) u cilju pribavljanja njihovih karakteristika i vršenja uvida, od strane stručnih lica, u oblike veza koje ti uređaji imaju sa drugim uređajima, i tada je, moguće vršiti privremeno oduzimanje uređaja za automatsku obradu podataka. Rok za započinjanje sprovođenja ove naredbe je isti kao i u slučaju svakog pretresanja 8 dana od izdavanja (čl.155 ZKP), ukoliko se ne počne sprovoditi organ postupka je dužan da je vrati sudu i pretresanje se ne može preduzeti. U svim opisanim slučajevima privremeno oduzimanje uređaja za automatsku

[413] https://www.guidancesoftware.com/ poslednji put pristupljeno 27. 08. 2019. god.

obradu podataka, kao i nosilaca digitalnih podataka, javlja se kao radnja fizičkog oduzimanja ovakvog uređaja.

Takođe, uređaje za automatsku obradu podataka nije neophodno po svaku cenu oduzimati, već je moguće, primenom forenzičkih mera, napraviti verne kopije, jer se ista svrha postiže i pravljenjem verne kopije ovakvog uređaja u datom trenutku u vremenu. Na ovaj način se celokupan sadržaj uređaja klonira i nakon toga moguće je pretraživanje uređaja različitim softverskim alatkama a za šta je potrebna naredba suda (tada se pravi više kopija, na kojima će se kasnije vršiti realno pretresanje). Ovakvo kopiranje stanja uređaja sa sobom nosi i konotaciju pretresanja računara - uređaja za automatsku obradu podataka. Tako da se u tom slučaju neće oduzimanjem računara ili mobilnog telefona lice lišiti mogućnosti njegovog korišćenja, pristupa Internetu, komunikacije sa bliskim licima.

U svakom slučaju pretresanje uređaja za automatsku obradu podataka se može sprovesti samo na osnovu naredbe suda a koja se izdaje na obrazložen predlog Javnog tužioca. Sadržaj takvog predloga ili zahteva za izdavanje naredbe mora odražavati smisao i potrebe izdavanja iste, te je u njemu značajno odrediti uređaje koji se imaju pretresati sa svim individualnim i grupnim karakteristrikama, iz kojih razloga se očekuje da se ovakvom radnjom mogu pribaviti dokazi i činjenice vezane za izvršenje krivičnog dela (osnovni uslov za pretresanje u čl.152. ZKP jeste verovatnoća da se pretresanjem mogu pronaći predmeti i tragovi odnosno određena lica), organe koji će u pretresanju učestvovati i u kom svojstvu. Iako se u većini slučajeva ne mogu precizno definisati predmeti i tragovi koji se mogu pronaći prilikom ovakvog pretresanja (na primer promena tipa datoteke), ovakvo precizno definisanje radnje omogućava da se pretresanjem ne zadire previše u privatnost lica.

Kod primene ove radnje uočava se da se Zakonikom nisu definisali uslovi pod kojima je moguće izvršiti radnju pretresanja uređaja za automatsku obradu podataka bez naredbe nadležnog sudskog organa. U cilju operativnijeg postupanja ovaj nedostatak bi se mogao otkloniti na taj način što bi se ova radnja predvidela Zakonikom o krivičnom postupku, čak i bez prisustva svedoka uz obavezno evidentiranje svih aktivnosti i njihovo fiksiranje kroz neki oblik zapisnika, audio vizuelnog snimanja i sl. Dakle, moguće je predvideti da se u sklopu uviđaja na uređajima za automatsku obradu podataka obavezno mora napraviti verna kopija svih raspoloživih memorija, a da se kasnije ista može, uz dodatne oblike sigurnosnog pristupa takvoj kopiji i analizirati. Naredbom za pretresanje uređaja za automatsku obradu podataka definišu se zadaci i subjekti koji u istom učestvuju uz predmete ka kojima je radnja pretresanja usmerena. U ovim slučajevima će odbrana angažovati stručnog savetnika, radi kontrole zakonitosti i poštovanja pravila postupanja organa gonjenja u slučajevima ovakvog pretresanja.

Pretresanje uređaja za automatsku obradu podataka, u užem smislu, podrazumeva pretraživanje računara uz pomoć različitih softverskih paketa, koji koriste pretrage datoteka u virtuelnom okruženju operativnog sistema računara, kao i drugim raspoloživim memorijama uređaja, na način kojim se konstatuju i pronalaze određene datoteke svi digitalni

elementi virtuelnog okruženja kao i pristupi uređaju, konekcije, oblici šifrovanih delova računara i njihova veličina i sl. Pregled računara predstavlja spoljašnji pregled uređaja i fiksiranje stanja na radnoj površini uređaja, konstatovanje postojećih veza na uređaju i aktivnih bežičnih veza u okruženju i samog uređaja kao i okruženje radnog prostora oko uređaja.

Da bi se obezbedio i očuvao dokazni kredibilitet oduzetih predmeta potrebno je poštovati sistem njihovog čuvanja i kontrolu manipulisanja. Sistem čuvanja podrazumeva označavanje, kategorizaciju, fotografsko i video snimanje, prikupljanje i pakovanje materijalnih dokaza, ali i postojanje pisanih podatka o službenim licima koja su postupala sa njima. Čuvanje takvih predmeta obezbeđuje organ postupka. Na ovaj način pruža se garancija da su dokazi koji se predstavljaju na sudu upravo oni koji su, kao takvi, prikupljeni na mestu događaja, odnosno pronađeni pretresanjem ili oduzeti od lica. Zbog toga se smatra da je u slučaju adekvatnog obezbeđivanja dokaznog materijala, gde se zahteva neraskidivi lanac dokazivanja (en. *chain of custody*) najbolje da se isti nalaze kod malog broja ljudi. Posebnu pažnju treba usmeriti ka oduzimanju i pakovanju onih predmeta koji su po svojoj prirodi izvor opasnosti. Za pojedine predmete, uz obavezu oduzimanja, zakonodavac predviđa i obavezu njihovog uništavanja: predmeti kojima je neovlašćeno iskorišćavano autorsko delo ili srodno pravo (čl. 199 st. 5 KZ), predmeti kojima je izvršeno neovlašćeno uklanjanje ili menjanje elektronske informacije o autorskom i srodnim pravima (čl. 200 st. 2 KZ), predmeti kojima je izvršena povreda pronalazačkog prava (čl. 201 st. 5 KZ).

Pretresanje uređaja za automatsku obradu podataka i opreme na kojoj se čuvaju ili se mogu čuvati elektronski zapisi

Pod automatskom obradom podataka podrazumeva se postupak obrade podataka automatskim sredstvima, pre svega računarima. Podaci koji se na ovaj način unose, kao i oni koji su dobijeni obradom, čuvaju se na memorijskim jedinicama. Uređajima za automatsku obradu podataka i opremi na kojoj se čuvaju ili se mogu čuvati elektronski zapisi, podrazumevamo svaki proizvod koji se koristi za obradu i/ili skladištenje elektronskih (digitalnih) podataka: računari (desktop, laptop, ili serveri), mobilni uređaji (pametni telefoni, Personal Digital Assistant - PDA, tableti, uređaji za satelitsku navigaciju...), memorijski medijumi (HD, CD/DVD, USB diskovi, SD kartice, ...), određena mrežna oprema (npr. modemi, ruteri, svičevi...), digitalne kamere, *Cloud Data* serveri i dr. Ovi uređaji se pretresaju kako bi se pronašle informacije u elektronskom (digitalnom) obliku koje imaju dokaznu vrednost, a koje su ili uskladištene ili prenesene u takvom obliku.

Postoje dve osnovne kategorije elektronskih podataka mogu činiti elektronski dokaz:

1. Nestalni (nepostojani, *Volatile*) podaci: - oni koji se nalaze u radnoj memoriji (RAM), ili se nalaze u prenosu, a gube se nakon isključivanja računara (npr. mrežni status i veze, aktivni procesi...);

2. Stalni (ali osetljivi) podaci uskladišteni na memorijskom medijumu (npr. na čvrstom disku - HD) i koji su sačuvani i nakon isključivanja računara. Neki od tih podataka se mogu lako izmeniti (npr. poslednje vreme pristupa), a nekima je moguće samo uslovno pristupiti (npr. podaci na šifrovanom disku koji su privremeno dostupni samo dok je računar uključen, a gde nakon isključenja i ponovnog startovanja računara njihova dostupnost zavisi od posedovanja odgovarajuće šifre).

Elektronski dokazi su podložni promeni, oštećenju, čak i uništenju usled nepravilnog rukovanja ili ispitivanja. Zato je neophodno preduzeti posebene mere postupanja kako bi ovakav, dokazni materijal, bio prihvatljiv za izvođenje u sudskom postupku u okviru dokaznih radnji.

Pretresanje uređaja za automatsku obradu podataka i opreme na kojoj se čuvaju ili se mogu čuvati elektronski zapisi, preduzeće se od strane stručnog lica i to:

1. u forenzičkoj laboratoriji ukoliko je izvršeno privremeno oduzimanje navedenih predmeta;
2. na licu mesta na uređaju koji je uključen (tzv. *live* forenzika), ukoliko u svom posedu ima za to specijalizovane alate.

Važno je napomenuti da, kada je god to moguće, stručno lice će napraviti forenzičku kopiju uređaja, tako da će se radi očuvanja originalnog dokaza, sve metode i alati za analizu elektronskih dokaza primenjivati na forenzičkoj kopiji, a ne na originalnom uređaju. Kako bi bila obezbeđena proverljivost dobijenih rezultata, po pravilu se prave dve forenzičke kopije - jedna radna i jedna rezervna. Istovetnost forenzičke kopije i originala potvrđuje se određivanjem njihovih heš (hash[414]) vrednosti koje moraju biti identične. Upravo ovakav forenzički postupak ukazuje na pravce o kojima je već obrazlagano ranije u radu.

Isključivanjem i oduzimanja uređaja radi njegove forenzičke analize, dolazi do gubitka velike količine nestalnih podataka. Zato se danas, pre isključenja računara, neophodnim smatra postupak čuvanja trenutnog sadržaja radne memorije (RAM-u), kao vrednog izvora kratkotrajnih i nestalnih informacija koje između ostalih mogu uključivati i: lozinke za šifrovane particije (TrueCrypt, BitLocker, PGP Disk), identifikacione podatke za prijavljivanje na različite naloge i servise (Gmail, Yahoo Mail, Hotmail; Facebook, Twitter, Google Plus; Dropbox, Flickr, SkyDrive, i dr.), spisak aktivnih procesa i sl. Za tu svrhu se mogu iskoristiti alati (koji se kao forenzički testirani i potvrđeni mogu pokrenuti sa DVD/CD-ROM ili USB uređaja) koji omogućavaju dampovanje sadržaja memorije bez unošenja bilo

[414] Više na https://en.wikipedia.org/wiki/Hash_function poslednji put pristupljeno 21.08.2019. god.

kakvih promena u elektronske podatke posmatranog uređaja (npr. Helix, Belkasoft Live RAM Caputer, AccessData FTK Imager, PMDump i dr.).

Ukoliko je iz bilo kojeg razloga nemoguće izvršiti privremeno oduzimanje uređaja za automatsku obradu podataka, pretresanje će se od strane stručnog lica obaviti na mestu događaja, primenom odgovarajućih forenzičkih alata, u postupku koji se naziva live forensics. U ovom slučaju, potraga za elektronskim dokazima sprovodi se u realnom vremenu, na uređaju koji radi. Ovakav postupak bi trebao biti pravilo, a ne izuzetak.

Zaključak

Prikazane radnje predstavljaju osnovne metode i sredstva u aktualnom suprotstavljanju organizovanom kriminalitetu, šta više, oni predstavljaju nezaobilazne dokazne odnosno posebne dokazne radnje u cilju pribavljanja dokaza. Njihov obim zadiranja u slobode i prava čoveka i građanina nije isti u svakom slučaju, ali ih zakonodavac u Srbiji veoma plastično etiketira. Kao što je prikazano, uslovi koji se vezuju za posebne dokazne radnje su značajnije oštro postavljeni u odnosu na "obične" dokazne radnje. U našem slučaju pretresanje UAOP ima i još značajnije garancije u odnosu na "obično" pretresanje stana i ostalih prostorija iako oba imaju karakter dokazne radnje, a još blaži su uslovi za sprovođenje radnje uviđaja koji je takođe dokazna radnja. Obrazloženja u vezi sa pooštravanjem uslova za pretresanje UAOP u odnosu na pretresanje stana i ostalih prostorija nikako nisu na mestu – naročito ako se ima u vidu ustavna garancija nepovredivosti stana, dok sama radnja pretresanja predviđa izuzetke od neophodnosti postojanja odluke suda za pretresanje stana i ostalih prostorija. Dakle, postoji protivrečnost u odnosima teorije i realnog stanja u Ustavu i zakoniku u pogledu odnosa prema ove dve procesne radnje. Isto bi trebalo promeniti kako i sugerišemo u ovom radu u pravcu propisivanja uslova za sprovođenje ove radnje i bez naredbe. Takođe, u pogledu radnje računarskog pretraživanja podataka opravdano su sniženi kriterijumi za primenu i pružena je mogućnost da širi set organa primenjuje ovu radnju, što je opravdano, sa stanovišta kako materije koju dotiče radnja, tako i sa aspekta delokruga organa kojima je povereno moguće vršenje.

Literatura:

1. Banović, B.: Elektronski dokazi, Revija za kriminologiju i krivično pravo, 2006. god, 3/ 06, str. 226
2. European Court of Human Right, CASE OF KLASS AND OTHERS v. GERMANY, Application no. 5029/71), JUDGMENT, STRASBOURG, 6, September 1978, <http://hudoc.echr.coe.int/eng?i=001-57510> 27. 8. 2019.
3. Ignjatović, Đ.; Škulić, M.; Organizovani kriminalitet, Beograd, 2010, str. 275
4. Komlen Nikolić, L. Gvozdenović, R. Radulović, S. Milosavljević, A. Jerković R. Živković, V. Živanović, S. Reljanović M. Aleksić, I.: Suzbijanje visokotehnološkog kriminala, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, 2010, str. 217.
5. Stamenković, B. Živanović, S. Paunović, B. Stevanović, I: Vodič za sudije i tužioce na temu visokotehnološkogkriminala i zaštite maloletnih lica u Republici Srbiji, Pravosudna akademija, 2017, str. 17
6. Subotić, D.; Posebne dokazne radnje, Beograd, 2013, str. 126–127

Internet izvori:

1. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 poslednji put pristupljeno 15.08.209.god.
2. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 poslednji put pristupljeno 15.08.209.god.
3. http://www.beograd.vtk.jt.rs/ poslednji put pristupljeno 20.08.2019.god.
4. https://www.guidancesoftware.com/ poslednji put pristupljeno 27.08.2019.god.
5. Više na https://en.wikipedia.org/wiki/Hash_function poslednji put pristupljeno 21.08.2019.god.