DALJINSKI NADZOR I PRETRAGA RAČUNALA KAO POSEBNA DOKAZNA RADNJA

Dražen Škrtić

Namen prispevka

Prikaz prikrivene dokazne mjere daljinskog nadzora i pretrage računala namijenjen je tijelima kaznenog progona.

Metode

Deskriptivnom metodom i komparativnom analizom obuhvaćene su odredbe njemačkog zakona o kaznenom postupku kojima je propisan daljinski nadzor i pretraga računala radi prikupljanja digitalnih dokaza.

Ugotovitve

Prikrivene dokazne radnje za otkrivanje počinitelja kaznenih djela privremenim ograničavanjem temeljnih ljudskih prava i sloboda, postalesu više pravilo nego iznimka, a zbog razvoja tehnologije pokazuju se nedostatnima i nedovoljno učinkovitima.Tijela kaznenog progona za učinkovito otkrivanja i dokazivanje kaznenih djela i počinitelja primjenjuju ili razmatraju primjenu posebnih računalnih programa za prikriveni pristup računalima. Primjena upravljivih forenzičkih računalnih programa za daljinske pretrage i nadzor računala omogućuje pribavljanje dokaza koje uporabom postojećih prikrivenih dokaznih radnji nije moguće pribaviti. U radu se razmatraju pravne osnove i nužni zakonodavni koraci za uvođenje navedenih posebnih prikrivenih dokaznih radnji i opravdanost dodatnih ograničenja temeljnih ustavnih odnosno Konvencijskih prava i sloboda s ciljem učinkovitijeg otkrivanja i procesuiranja kaznenih djela i počinitelja.

Praktična uporabnost

U preglednom članku daje se poredbeni prikaz odredbi nekih zakona kojima je propisana dokazna mjera daljinskog nadzora računalnog sustava i njihova kompatibilnost s Konvencijom o temeljnim ljudskim pravima i slobodama.

Izvirnost/pomembnost prispevka

Predstavljene su odredbe o daljinskom nadzoru i pretrazi računala kao posebnoj dokaznoj radnji poduzetoj radi otkrivanja kaznenih djela i počinitelja i prikupljanju digitalnih dokaza za potrebe kaznenog postupka.

Ključne besede: daljinski forenzički programi, posebne dokazne radnje, nadzor računala, daljinska pretraga računala

1 UVOD

Brze tehnološke promjene, svakodnevna masovna uporaba suvremene informacijske i komunikacijske tehnologije promjenile su način pristupa velikom broju usluga i informacija. Prilagodba pojedinaca i cijelih skupina novim okolnostima i korištenja tehnologije, korištenje tehnologije u legalnim ali i kriminalnim aktivnostima dovela je do potrebe da tijela kaznenog progon, radi sprječavanja i otkrivanja kaznenih djela koriste istu tehnologiju i iste postupke, u okviru legislativnih rješenja kao i počinitelji kaznenih djela. Ekspanzija mobilnih uređaja, korištenje više od jednog prijenosnika, pametnog telefona, tableta, fableta ili stolnog računala po stanovniku postaje realnost. Mobilni uređaji brzo preuzimaju dominaciju nad klasičnim stolnim računalima. U tekstu ćemo koristiti jednostavan naziv računalo za sve uređaje koji se mogu podvesti pod definiciju računala na način na koji je računalo odnosno računalni sustav definiran Konvencijom o kibernetičkom kriminalu VE (Convention on Cybercrime, 2001).

Digitalna forenzika, prije dvadesetak godina prihvaćena kao nužnost u u pribavljanju digitalnih dokaza za kaznena djela počinjena uporabom računala, postala je opće prihvaćeno sredstvo za pribavljanje digitalnih dokaza i za kaznena djela čije se počinjenje nužno ne veže za korištenje digitalne tehnologije. U uvjetima intenzivne digitalizacije društva jača digitalno podzemlje (digital udergrounde) i uvjetuje nužne aktivnosti države i tijela kaznenog progona u prilagođavanju novim okolnostima.

Primjerna posebnih i prikrivenih dokaznih radnji radnji radi pribavljanja digitalnih dokaza prati trendove rasta uporabe digitalne tehnologije. Prikrivene dokazne radnje, pribavljanje podataka o komunikacijskim kontaktima i komunikacijskom prometu određenog korisnika i nadzor sadržaja komunikacija, u postupcima tijela kaznenog progona poduzetim radi otkrivanja kaznenih djela i počinitelja, postaje gotovo više pravilo nego izuzetak.
Legislativna rješenja koja su pravila za pribavljanje tradicionalnih dokaza samo djelomično i nužno prilagodila prikupljanju digitalnih dokaza postaju nedostatna za učinkovito prikupljanje digitalnih dokaza. Pitanje prilagođavanja propisa novim okolnostima i novim tehnologijama tijelima kaznenog progona nameće potrebu korištenja istih alata koji se koriste u svakodnevnom korištenju digitalne tehnologije i koje digitalno podzemlje koristi za počinjenje kaznenih djela. Tako se postupno nameće potreba zakonskog uređenja daljinske pretrage računala, pretraga računalnih podataka u oblaku (cloud) odnosno online pretrage i daljinski nadzor računala.

U radu deskriptivnom metodom i komparativnom analizom obuhvaćene su odredbe njemačkog zakona o kaznenom postupku kojima je propisan daljinski nadzor i pretraga računala radi prikupljanja digitalnih dokaza i pravne osnove i nužni zakonodavni koraci za uvođenje navedenih posebnih prikrivenih dokaznih radnji i opravdanost dodatnih ograničenja temeljnih ustavnih odnosno Konvencijskih prava i sloboda s ciljem učinkovitijeg otkrivanja i procesuiranja kaznenih djela i počinitelja.

2 DALJINSKA PRETRAGA RAČUNALA

Postojeći zakoni koji uređuju pretragu računala, a posljedično i oduzimanje računalnih podataka odnosno informacija pohranjenih na računalu ili mediju za pohranu podataka uređuju to pitanja na način kako je to pitanje uređeno kad je riječ o konvencionalnim predmetima odnosno pretragama prostora i predmeta i oduzimanje predmeta koji imaju poslužiti kao dokaz u kaznenom postupku. Međutim, ta pravila nisu u potpunosti primjenjiva na sva područja pretraga računala i na računalne podatke. Naime, pravna pravila se odnose na uglavnom na računala i nositelje računalnih podataka koja su i posjedu i pod kontrolom tijela koje provodi dokaznu radnju pretrage i oduzimanja računalnih podataka. Pitanja pretraga računala i nositelja podataka koji nisu pod kontrolom i unutar jurisdikcije tijela koje provodi pretragu nisu riješena (Škrtić, Kralj i Švegar, 2013).Termin oduzimanje predmeta kad se odnosi na računalne podatke samo je djelomično primjenjiv. Naime, termin će odgovarati stvarnom stanju samo u slučajevima kad su računalni podaci pohranjeni na samo jednom mediju za pohranu podataka koje je sastavni i neodvojivi dio računala, a da se ne naruši njegova funkcionalnost ili mediju za pohranu podataka kojima se može pristupiti pohranjenim podacima njihovim spajanjem ili umetanjem u računalo. Oduzimanje računalnih podataka ili drugih predmeta podrazumijeva činjenicu da je posjed i nadzor nad oduzetim predmetima preuzelo tijelo koje provodi pretragu i da oduzeti računalni podaci više nisu dostupni osobi od koje su predmeti oduzeti. U slučaju da su računalni podaci koji su predmet oduzimanja pohranjeni na više medija za pohranu koji nisu u posjedu i pod kontrolom tijela koje provodi pretragu, može se govoriti samo o podacima koji su dostupni tijelu koje provodi pretragu i oduzimanje, što će biti samo jedna od kopija tih računalnih podataka.

Daljinska pretraga podataka na računalu je relativno tehnički jednostavna i provediva bez posebnih forenzičkih računalnih programa. Neovlašteni daljinski pristup računalnim podacima uporabom malicioznih računalnih programa je jedan od načina pribavljanja podataka pohranjenih na mediju za pohranu podataka u računalu. Isto tako, suvremeni operacijski sustavi omogućuju pristup računalu online osobama koje su ovlaštene za pristup računalu.

Korištenje daljinski upravljanih forenzičnih računalnih programa za pribavljanje dokaza u kaznenom postupku je aktivnost tijela koje provodi pretragu prodorom u računala osoba prema kojima se ta mjera primjenjuje Daljinska ili online pretraga (njem. "Online-Durchsuchung") označava skup različitih tehničkih sredstava i postupaka kojim kroz elektroničku komunikacijsku mrežu iz jednog računala daljinski pribavljaju računalni podaci i pohranjuju na mediju za pohranu podataka u računalnom sustavu s kojeg se vrši daljinska pretraga.

Daljinska pretraga, predstavlja jednokratni pristup drugom računalu kroz elektroničku komunikacijsku mrežu i prijenos podataka na medij za pohranu podataka na računalu s kojeg je poduzeta pretraga. To znači da će na mediju pretraženog računala ostati svi podaci koji su preneseni prilikom pretrage ili će biti moguće restaurirati sve podatke koji su prilikom pretrage eventualno izbrisani odnosno učinjeni privremeno nedostupnim. Način autentifikacije prenesenih podataka i jamstva da su podaci preneseni u neizmijenjenom obliku bi u tom slučaju trebalo propisati zakona (Škrtić et al., 2013).

Za provođenje daljinske pretrage podrazumijeva se uporaba forenzičnog računalnog programa koji se instalira na informacijsko-tehnički sustav (računalo) na kojem se pretraga provodi,a koji i prenosi informacije s tog računala sustava na računao s kojeg se provodi pretraga. Za daljinske pretrage koriste se forenzične inačice, fizički ili daljinski instaliranog malicioznog računalnog programa,daljinski upravljan forenzični računalni program (remote forensic software– RFS), poznatog pod nazivom trojanski konj ili trojanac. Kad navedene računalne programe koriste tijela kaznenog progona oni se kolokvijalno nazivaju državni trojanski konji ili kraće državni trojanci (govware, policeware).

3 DALJINSKI NADZOR RAČUNALA

Daljinski nadzor računala u svojoj naravi predstavlja gotovo identičnu mjeru kao i daljanska pretraga računala. Pristup računalu u pravilu traje duže od vremena koje je nužno za pretragu i prijenos računalnih podataka kroz elektroničku komunikacijsku mrežu od pretraživanog računala prema računalu s kojeg se vrši pretraga. Nadzor (Online-Überwachung, online surveillance - online nadzor) dakle traje određeno vremensko razdoblje, u kojem je tijelo koje vrši nadzor u mogućnosti pratiti sve aktivnosti koje se odvijaju na računalu. Pojam online-pretraga pravilno označuje samo trenutni pristup računalu koje se pretražuje sa svrhom kopiranja pohranjenih podataka. Nadziranje tekućih aktivnosti na ciljanom računalu koje traje neko vrijeme također naziva "online-nadziranjem", dok se kao višim pojmom koji označuje obje navedene aktivnosti koristi izravnom online-poseg -Online-Zugriff (Sieber, 2007). Terminologija prihvatljiva s aspekta kaznenog procesnog jer dokazna radnja pretraga

procesna radnja ima jednokratni, trenutačni karakter i traje dok se ne izvrši pretraga. Pored tog izraza, za označivanje navedene mjere, kao viši pojam, u uporab ije (osobito u Austriji) i izraz "online-istraživanje - Online-Fahndung (Pajačić, 2009).

No nadzor računala, rada na računalu odnosno trenutnu interakciju između korisnika računa i računala obuhvaća i mogućnost istovremenog nadzora komunikacija pa i pristup podacima koji se nalaze u privremenim memorijama računa. Dakle, nadzor računala pored sadržaja komunikacija koji se prenosi računalom omogućuje i uvid u prijenos računalnih podataka kao što su korisnička imena i zaporke za pristup određenim servisima kao što su pristup korisničkim računima elektroničke pošte na serverima koji nisu pod jurisdikcijom tijela koje provodi nadzor, pristup Internet bankarstvu, bezgotovinski prijenos novac, kupovinu vrijednosnih papira, online klađenje, pristup portalima i sadržajima na portalima.

Dakle, nadzor računala tijelu koje provodi nadzor pruža znatno veći broj informacija od jednostavne pretrage računalnih podataka pohranjenih na računalu i kopiranja tih podataka i od podataka prometu i sadržaju svih oblika komunikacija ostvarenih uporabom računala i ne može biti pokriveno niti sudskim nalogom za nadzor komunikacija niti sudskim nalogom za provjeru uspostavljanja telekomunikacijskog kontakta prema odredbama članak 339.a Zakona o kaznenom postupku.

Većina korisnika računala, instaliranu kameru i mikrofon koristi za video i audio komunikaciju. Nadzor računala omogućuje i akustični i video nadzor prostora i osoba u prostoru preko računala koje ima instaliranu video kameru i mikrofon. Ukoliko se radi o prijenosniku, tabletu ili pametnom telefonu nadzor će biti moguće proširiti na sve prostore u kojima se kreće nadzirano računalo.

4 ONLINE PRETRAGA I DALJINSKI NADZOR RAČUNALA U NJEMAČKOM PRAVU

Za online pretrage računala u njemačkom kaznenom pravu navodimo dvije sudske odluke. Na zahtjev državnog odvjetništva za prikrivenu online-pretragu računala okrivljenika početkom 2006. godine, sudac istrage najprije je pretragu osobnog računala okrivljenika, osobito podataka pohranjenih na tvrdom disku i radnoj memoriji. Pravni temelj za odobravanje takve pretrage pronašao je u propisima o pretrazi stana (Pajčić, 2009).

Drugi sudac istrage odbio je zahtjev glavnog državnog odvjetnika za provođenjem druge tajne online-pretrage (Pajčić, 2009). Odbijanje zahtjeva obrazloženo je nepostojanjem pravnog temelja za tajno

provođenje takve mjere budući da zakon za provođenje pretrage računala propisuje obveznu nazočnost svjedoka i vlasnika računala pretrage ili njegova zastupnika. Na žalbu glavnog državnog odvjetnika Savezni vrhovni sud, u postojećim propisima kaznenog procesnog prava na nalazi zakonsku ovlast za provođenje te mjere Pajčić, 2009).

Takav bi poseg bio "ozbiljno zadiranje u pravo na informacijsko samoodređenje".Sud je upozorio da nije dopušteno kombinirati pojedine elemente raznih ovlasti posezanja uprava radi stvaranja pravnog temelja za neku novu, zbog razvoja tehnike moguću, mjeru prikupljanja informacija. To bi se protivilo načelu zakonitosti ograničavanja posega u temeljna prava iz čl. 20. st. 3. Temeljnog zakona kao i načelu određenosti normi kaznenog procesnog prava o mjerama ograničenja ljudskih prava i sloboda za potrebe kaznenog postupka. Sud je istaknuo da je tajna infiltracija nekog informacijsko-tehničkog sustava, pomoću kojeg se može nadzirati uporaba tog sustava i pročitati medije za pohranu podataka, ustavno pravno dopuštena samo ako postoje činjenična uporišta konkretne opasnosti za posebno važno pravno dobro. Posebno važna dobra su tjelesna nepovredivost, život i sloboda osobe ili takva opća dobra kojih ugrožavanje dira temelje ili opstanak države ili temelje egzistencije ljudi. (Pajčić, 2009). Ta mjera, ističe Ustavni sud, može biti opravdana i tada kad se ne može još s dovoljno velikom vjerojatnošću ustanoviti da će opasnost nastupiti u bliskoj budućnosti ako određene činjenice upućuju na to da u pojedinom slučaju od određenih osoba prijeti opasnost za posebno značajno pravno dobro.

Savezni ustavni sud svoju je odluku obrazložio navodeći da se provođenjem online-pretrage na način kako je to predviđeno u Zakonu u ustavnom ustrojstvu Sjeverne Rajne-Vestfalije povređuje "temeljno pravo na jamstvo povjerljivosti i integriteta informacijsko-tehničkog sustava". Riječ je o novom temeljnom pravu koje je Savezni ustavni sud izveo iz općeg prava osobnosti. "Opće pravo osobnosti (čl. 2. st. 1. u vezi s čl. 1. st. 1. Temeljnog zakona sadržava u sebi temeljno pravo na jamstvo povjerljivosti i integritet informacijsko-tehničkih sustava". Sud je istaknuo da je tajna infiltracija nekog informacijsko-tehničkog sustava, pomoću kojeg se može nadzirati uporaba tog sustava i pročitati medije za pohranu podataka, ustavno pravno dopuštena samo ako postoje činjenična uporišta konkretne opasnosti za posebno važno pravno dobro. Posebno važna dobra su tjelesna nepovredivost, život i sloboda osobe ili takva opća dobra kojih ugrožavanje dira temelje ili opstanak države ili temelje egzistencije ljudi (Pajačić, 2009). Ta mjera, ističe Ustavni sud, može biti opravdana i tada kad se ne može još s dovoljno velikom vjerojatnošću ustanoviti da će opasnost nastupiti u bliskoj budućnosti ako određene činjenice upućuju na to da u pojedinom slučaju od određenih osoba prijeti opasnost za posebno značajno pravno dobro (Pajačić, 2009).

Sud je upozorio da tajna infiltracija nekog informacijsko-tehničkog sustava treba načelno biti odobrena sudskom odlukom. Zakon koji propisuje ovlast na takav poseg mora sadržavati odredbe kojima će se zaštititi "jezgra privatnog življenja" (Pajačić, 2009).

5 ZAKON O KAZNENOM POSTUPKU

Zakon o kaznenom postupku ne sadrži odredbe koje bi propisivale i uređivale pitanje online pretrage. Odredbama zakona propisana je pretraga računala i nadzor elektroničkih komunikacija odnosno provjera uspostavljanja telekomunikacijskog kontakta, a odredbama Zakona o policijskim poslovima i ovlastima propisana je policijska ovlast provjera uspostavljanja elektroničke komunikacije.

5.1 Provjera uspostavljanja telekomunikacijskog kontakta

Propisivanje posebne dokazne radnje provjere uspostavljanja telekomunikacijskog kontakta novina je u Zakonu o kaznenom postupku i kvalitativni pomak u zaštiti Konvencijskih, Ustavnih garancija prava na tajnost komunikacije i u skladu s interpretacijom prava na privatnost komunikacije prema presudi Europskog suda za ljudska prava u slučaju Malone v. United Kingdom (Malone v. United Kingdom, 1984).

Zakon o kaznenom postupku u članku 339.a propisuje provjeru uspostavljanja telekomunikacijskog kontakta kao posebnu dokaznu radnju. Posebna dokazna radnja može se provesti ako je registrirani vlasnik ili korisnik komunikacijskog sredstva dao pisani pristanak, na temelju naloga nadležnog državnog odvjetnika koji podliježe naknadnoj sudskoj konvalidaciji i na temelju naloga suca istrage.

Obrazloženi prijedlog za provođenje posebne dokazne radnje provjere telekomunikacijskog kontakta sucu istrage podnosi državni odvjetnik. Odluku o zahtjevu državnog odvjetnika sudac istrage dužan je donijeti u roku od četiri sata. Iznimno, ako postoji opasnost od odgode i ako državni odvjetnik ima razloga vjerovati da na vrijeme neće moći pribaviti nalog suca, nalog za provođenje posebne dokazne radnje provjere telekomunikacijskog kontakta može izdati nadležni državni odvjetnik. Nalog za provođenje posebne dokazne radnje provjere telekomunikacijskog kontakta i dopis u kojem će obrazložiti razloge za njegovo izdavanje državni odvjetnik mora odmah, a najkasnije u roku od 24 sata od izdavanja, dostaviti sucu istrage. Sudac istrage odlučuje rješenjem o zakonitosti naloga državnog odvjetnika u roku od 48 sati od primitka naloga i dopisa. Protiv rješenja suca istrage državni odvjetnik nema prava žalbe.

Za registriranog vlasnika ili korisnika telekomunikacijskog sredstva koji je povezan s osobom za koju postoji sumnja da je počinila kazneno djelo za koje se kazneni postupak pokreće po službenoj dužnosti policija može, na temelju naloga suca istrage, zatražiti od operatora javnih komunikacijskih usluga provjeru telekomunikacijskog kontakta.

Provjeru telekomunikacijskog kontakta moguće je izvršiti ako postoji sumnja da je registrirani vlasnik ili korisnik telekomunikacijskog sredstva počinio kazneno djelo za koja se kazneni postupak pokreće po službenoj dužnosti policija će, na temelju naloga suca istrage, a radi prikupljanja dokaza, od operatora javnih komunikacijskih usluga zatražiti provjeru istovjetnosti, trajanja i učestalosti komunikacije s određenim elektroničkim komunikacijskim adresama, utvrđivanje položaja komunikacijskog uređaja, kao i utvrđivanje mjesta na kojima se nalaze osobe koje uspostavljaju elektroničku komunikaciju, te identifikacijske oznake uređaja.

Podaci o telekomunikacijskim kontaktima koji su pribavljeni bez naloga suca istrage odnosno ako državni odvjetnik nije u propisanom roku dostavio sucu istrage nalog za provođenje posebne dokazne radnje ili ako je odbijen zahtjev državnog odvjetnika za ovjeru naloga za provjeru uspostavljanja telekomunikacijskih kontakata, ne mogu se upotrijebiti kao dokaz u postupku.

5.2 Provjera uspostavljanja elektroničke komunikacije

Prema odredbama članka 68. Zakona o policijskim poslovima i ovlastima, policijsku ovlast provjera uspostavljanja elektroničke komunikacije moguće je poduzeti temeljem pisanog odobrenju načelnika Uprave kriminalističke policije ili načelnika Policijskog nacionalnog ureda za suzbijanje korupcije i organiziranog kriminaliteta ili načelnika policijske uprave, a u njihovoj odsutnosti osoba koje ih zamjenjuju, a temelji se na činjenicama iz kojih je vidljivo da se drugim radnjama nije mogao ili se neće moći postići cilj policijskog posla ili bi postizanje tog cilja bilo povezano s nerazmjernim teškoćama. Iznimno, ako je to potrebno radi sprječavanja neposredne opasnosti ili nasilja odnosno radi žurnog traganja za osobama, odobrenje može biti dano i usmeno, ali mora biti pisano potvrđeno najkasnije u roku od 24 sata od danog usmenog odobrenja.

Policijsku ovlast provjera uspostavljanja elektroničke komunikacije moguće je poduzeti radi sprječavanja i otkrivanja kaznenih djela za koja se progoni po službenoj dužnosti i njihovih počinitelja, sprječavanja opasnosti i nasilja, traganja za osobama i predmetima. Policija može od davatelja komunikacijskih usluga zatražiti provjeru istovjetnosti, trajanja i učestalosti komunikacije s određenim elektroničkim komunikacijskim adresama i utvrđivanje položaja komunikacijskog uređaja, kao i utvrđivanje mjesta na kojima se nalaze osobe koje uspostavljaju elektroničku komunikaciju te identifikacijske oznake uređaja.

Odredba Zakona o policijskim poslovima i ovlastima, unesena u navedeni zakon u noveli iz 2014. godine, propisuje ovlast provjere uspostavljanja elektroničke komunikacije na usporediv način kao i posebna dokazna radnja provjere uspostavljanja telekomunikacijskog kontakta Zakona o kaznenom postupku. Iako je izmijenjen sam naziv članka, i policijska ovlast pravno definirana neutralnim tehnološkim terminima, Zakon s aspekta zaštite Konvencijskih i Ustavnih garancija prava na tajnost komunikacije i interpretacijom prava na privatnost komunikacije prema presudi Europskog suda za ljudska prava u slučaju Malone v. United Kingdom (Malone v. United Kingdom, 1984) ne zadovoljava navedene pravne standarde. To se posebno odnosi na odredbe kojim je propisna mogućnost primjene policijske ovlasti radi sprječavanja i otkrivanja kaznenih djela za koja se progoni po službenoj dužnosti i njihovih počinitelja. Iako je ovlast za odobrenje primjene policijske ovlasti, u odnosu na izmijenjene odredbe prema kojima je odobrenje za primjenu mjere donosi čelnik kriminalističke policije bez navođenja ranga i položaja, definirana određenije i preciznije, kao i postupanje u žurnim situacijama, nije zadovoljen uvjet prethodne sudske kontrole primjene ovlasti odnosno naknadne sudske provjere i konvalidacije naloga. Smatram da navedena policijska ovlast nije u skladu s pravnim standardima zaštite prava na privatnost komunikaciju.

Pitanje uporabe digitalnih dokaza pribavljenih primjenom navedene policijske ovlasti u kaznenom postupku nije dvojbeno. Zakon o kaznenom postupku izričito propisuje da se podaci o telekomunikacijskim kontaktima koji su pribavljeni bez naloga suca istrage odnosno ako državni odvjetnik nije u propisanom roku dostavio sucu istrage nalog za provođenje posebne dokazne radnje ili ako je odbijen zahtjev državnog odvjetnika za ovjeru naloga za provjeru uspostavljanja telekomunikacijskih kontakata, ne mogu se upotrijebiti kao dokaz u postupku. Dakle, digitalni dokazi pribavljeni prema odredbama Zakona o policijskim poslovima i ovlastima, ne mogu biti zakonit dokaz u kaznenom postupku. Isto tako, korištenje podataka pribavljenih primjenom policijske ovlasti provjere uspostavljanja elektroničke komunikacije radi pribavljanja sudskog naloga i ponovnog pribavljanja istih dokaza temeljem sudskog naloga u skladu s odredbama članka 339.a predstavljalo bi nezakonit dokaz prema doktrini „plodova otrovne voćke“.

U svakom slučaju, u tijeku su sudski postupci pokrenuti temeljem dokaza pribavljenih primjenom policijskih ovlasti prije stupanja na snagu odredbi članka 339. Zakona o kaznenom postupku i moguće je da će Vrhovni sud Republike Hrvatske biti u prilici zauzeti stajalište o zakonitosti digitalnih dokaza pribavljenih bez sudskog naloga, primjenom policijske ovlasti provjere uspostavljanja elektroničke komunikacije.

5.3 Pretraga pokretne stvari i bankovnog sefa

Prema odredbama članka 256. Zakona o kaznenom postupku pretraga pokretnih stvari obuhvaća i pretragu računala i s njim povezanih uređaja, drugih uređaja koji služe prikupljanju, pohranjivanju i prijenosu podataka, telefonskim, računalnim i drugim komunikacijama i nositelja podataka. Na zahtjev tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu ili drugom uređaju ili nositelju podataka, te davatelj telekomunikacijskih usluga, dužni su omogućiti pristup računalu, uređaju ili nositelju podataka, te dati potrebne obavijesti za nesmetanu uporabu i ostvarenje ciljeva pretrage.

Po nalogu tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu i drugim uređajima koji su predmet pretrage, te davatelj telekomunikacijskih usluga, dužni su odmah poduzeti mjere kojima se sprječava uništenje ili mijenjanje podataka. Tijelo koje poduzima pretragu, može provedbu tih mjera naložiti stručnom pomoćniku.

Osobu koja koristi računalo ili ima pristup računalu ili drugom uređaju ili nositelju podataka, te davatelj telekomunikacijskih usluga, a koji ne postupe po nalogu tijela koje poduzima pretragu, premda za to ne postoje opravdani razlozi, sudac istrage može na prijedlog državnog odvjetnika novčano kazniti. Odredba o kažnjavanju ne odnosi se na okrivljenika.

Odredba Zakona o kaznenom postupku o pretrazi računala, definira pretragu računala odnosno medija za pohranu računalnih podataka koji je dostupan, u posjedu i pod kontrolom tijela koje provodi pretragu. Ne propisuju se posebni uvjeti pod kojima se pretraga provodi, tko može, a tko je obvezan prisustvovati pretrazi kao niti način postupanja i jamstvo autentičnosti i nepromjenjivosti računalnih oduzetih nakon proveden pretrage.

5.4 Nadzor i tehničko snimanje telefonskih razgovora i drugih komunikacija na daljinu

Člankom 332. Zakona o kaznenom postupku propisani su uvjeti o provođenju posebnih dokaznih radnji. Ako se istraga ne može provesti na drugi način ili bi to bilo moguće samo uz nerazmjerne teškoće, na pisani obrazloženi zahtjev državnog odvjetnika, sudac istrage može protiv osobe za koju postoje osnove sumnje da je sama počinila ili zajedno s drugim osobama sudjelovala u kaznenom djelu iz kataloga kaznenih djela za koja je moguće izdavanje naloga za provođenje posebnih dokaznih radnji, pisanim, obrazloženim nalogom odrediti posebne dokazne radnje kojima se privremeno

ograničavaju određena ustavna prava građana, i to: nadzor i tehničko snimanje telefonskih razgovora i drugih komunikacija na daljinu, presretanje, prikupljanje i snimanje računalnih podataka, ulazak u prostorije radi provođenja nadzora i tehničko snimanje prostorija, tajno praćenje i tehničko snimanje osoba i predmeta, uporabu prikrivenih istražitelja i pouzdanika, simuliranu prodaju i otkup predmeta te simulirano davanje potkupnine i simulirano primanje potkupnine, pružanje simuliranih poslovnih usluga ili sklapanje simuliranih pravnih poslova, nadzirani prijevoz i isporuku predmeta kaznenog djela.

Iznimno, kad okolnosti nalažu da se s izvršenjem radnji započne odmah, nalog prije početka istrage na vrijeme od dvadeset četiri sata može izdati državni odvjetnik. Nalog s oznakom vremena izdavanja i obrazloženjem državni odvjetnik mora u roku od osam sati od izdavanja dostaviti sucu istrage. Sudac istrage odmah odlučuje rješenjem o zakonitosti naloga. Ako odobri nalog državnog odvjetnika pisanim, obrazloženim nalogom odrediti će posebne dokazne radnje kojima se privremeno ograničavaju određena ustavna prava građana. Ako sudac istrage odbije nalog, državni odvjetnik, može u roku od osam sati podnijeti žalbu. O žalbi odlučuje vijeće u roku od dvanaest sati.

Zakon o kaznenom postupku propisuje uvjete pod kojim sudac istrage ili nadležni državni odvjetnik može izdati nalog za nadzor i tehničko snimanje telefonskih razgovora i drugih komunikacija na daljinu, presretanje i prikupljanje i snimanje računalnih podataka. Odredbama nije propisana mogućnost daljinske pretrage računala radi prikupljanja i snimanja računalnih podataka niti nadzor računala radi nadzor i tehničko snimanje telefonskih razgovora i drugih komunikacija na daljinu. Način provođenja propisan je podzakonskim propisom i ne uključuje nadzor računala, već samo podatke o komunikaciji i sadržaju komunikacije.

6 ZAKLJUČAK

Intenzivna legislativna aktivnost, odluka Ustavnog suda o ustavnosti pojedinih odredbi Zakona o kaznenom postupku iz 2008. godine, izmjene i dopuna Zakona o kaznenom postupku kao i izmjene i dopune Zakona o policijskim poslovima i ovlastima, nisu bitne promijene odredbi kojima je definirano privremeno ograničenje temeljnih ljudskih prava radi pribavljanja digitalnih dokaza.

Pozitivno hrvatsko kazneno procesno zakonodavstvo ne propisuje mogućnost provođenja dokaznih radnji daljinske pretrage računala i daljinski nadzor računala. Navedene odredbe, kao analizirana stajalište njemačkih sudova, daljinsku pretragu i daljinski nadzor računala ne daju mogućnost da se navedene prikrivene radnje podvedu pod postojeće odredbe zakona.

Tijela kaznenog progona za pribavljanje digitalnih dokaza o počinjenim kaznenim djelima i počiniteljima kaznenih djela naglašavaju potrebu zakonskih mogućnosti obavljanja daljinskih pretraga i daljinskog nadzora rada računala. Zahtjevi za zaštitom temeljnih ljudskih prava i interesa društva za učinkovitom borbom protiv kriminalnih aktivnosti i zaštite nacionalne sigurnosti neminovno vode prema otvaranju rasprava i postizanja konsenzusa o uvođenju daljinske pretrage i daljinskog nadzora računala kao posebnih prikrivenih dokaznih radnji kojim se temeljna ljudska prava dodatno ograničavaju.

Nove dokazne radnje i podrazumijevaju i nova ograničenja temeljnih ljudskih prava stoga zahtijevaju temeljito razmatranje uvjeta za uvođenje novih dokaznih radnji i propisivanje materijalno pravnih pretpostavki za njihovu primjenu.

LITERATURA

Case Of Malone V. The United Kingdom.(1984). Application no. 8691/79. Judgment , Strasbourg. Pribavljeno na http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57533

Convention on Cybercrime. (2001). Pribavljeno na http://www.conventions.coe.int/treaty/EN/treaties/html/185.htm

Krapac, D. (2006). *Zakon o kaznenom postupku i drugi izvori hrvatskog kaznenog postupovnog prava*. Zagreb: Narodne novine.

Pajčić, M.(2009). Korištenje forenzičnim računalnim programima za prikupljanje dokaza u kaznenom postupku. *Hrvatski ljetopis za kazneno pravo i praksu, 16*(1), 281-317.

Sieber, U. (2007). *Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen, zur Anhörung in der mündlichen Verhandlung am 10. Oktober 2007*. Pribavljeno na http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf,

Škrtić, D., Kralj, D. i Švegar, M. (2013). Search and seizure data in cyberspace: mechanism to preserve and reproduce data in non-volatile format. V G. Meško, A. Sotlar in J. R. Greene (ur.), *Contemporary Criminal Justice Practice and Research: conference proceedings* (str. 509–523). Ljubljana: Faculty of Criminal Justice and Security.

Zakon o kaznenom postupku. (2008). *Narodne novine RH*, 152/08, 76/09, 80/11, 91/12 - Odluka i Rješenje USRH, 143/12, 56/13 i 145/13,

Zakon o policijskim poslovima i ovlastima. (2009). Narodne novine RH, 76/09 i 96/14.