UDK 004.4
343.98
343.132
342.738
Primljeno 1. svibnja 2009.
Izvorni znanstveni rad

Mr. sc. Matko Pajčić*

KORIŠTENJE FORENZIČNIM RAČUNALNIM PROGRAMIMA ZA PRIKUPLJANJE DOKAZA U KAZNENOM POSTUPKU

Slijedeći tehnološki napredak, državna tijela koja sudjeluju u otkrivanju kaznenih djela i počinitelja i prikupljanju dokaza za potrebe kaznenog postupka rabe, ili razmatraju njihovu uporabu, posebne računalne programe kojima prikriveno posežu u računalni sustav osobe osumnjičene za počinjenje teškog kaznenog djela. Primjena daljinski upravljanih forenzičnih računalnih programa s jedne strane omogućuje učinkovitu otkrivačku djelatnost te otkrivanje i prikupljanje dokaza protiv počinitelja koji na neki drugi način vjerojatno ne bi bili otkriveni. S druge strane, riječ je o mjeri koja možda čak i više od drugih posebnih istražnih mjera zadire u ustavna prava i slobode. S njezinom primjenom zbog cijelog niza razloga valja biti iznimno oprezan.

1. UVOD

Brzi razvoj računalnih tehnologija izaziva promjene u svim područjima života.[1] Budući da je prihvaćanje promjena i prilagođivanje nužno za uspjeh u svakom pothvatu, pa tako i onom kriminalnom, jasno je i da su počinitelji kaznenih djela u velikoj mjeri usvojili nove tehnološke promjene.[2]

S druge strane, i policija i državno odvjetništvo koriste se računalnom tehnologijom pri otkrivanju i dokazivanju kaznenih djela i počinitelja. Jedan od najnovijih i najsofisticiranijih načina na koji policija i državno odvjetništvo,

* Mr. sc. Matko Pajčić, asistent na Katedri za kazneno procesno pravo Pravnog fakulteta Sveučilišta u Splitu

[1] Vremena kad su se osobna računala koristila samo kao nešto moderniji pisaći strojevi odavno su prošla. Preko nekog međurazdoblja, kad su računala počela služiti i za igranje računalnih igrica, slušanje glazbe, rad na nekim proračunima i nacrtima, došli smo, pojavom interneta, do vremena kad se preko računala obavlja, ili se barem može obavljati, mnogo toga. Od čitanja i pisanja sadržaja (*world wide web*), pisane komunikacije (elektronička pošta), razgovora (VoIP – Voice over Internet Protocol) pa sve do online-trgovine, online-bankarstva, obavljanja raznih administrativnih poslova, korištenja društvenim mrežama...

[2] V. članak u Večernjem listu od 15. 2. 2009.: Talijanski kriminalci koriste Skype.

ali i neka druga državna tijela, mogu primjenjivati računalnu tehnologiju u tu svrhu jest korištenje daljinski upravljanih forenzičnih računalnih programa.

Riječ je o pitanju koje je posljednjih nekoliko godina predmetom vrlo žustre rasprave u nizu europskih zemalja. Razlog zašto ono izaziva tako oštru raspravu jest taj što se na njemu u velikoj mjeri prelamaju osjetljiva pitanja granica ovlasti države na ograničavanje određenih temeljnih prava i sloboda građana radi obrane državne sigurnosti, ustavnog poretka te otkrivanja kaznenih djela i počinitelja. Nakon određenja pojmova forenzičnih računalnih programa i "online-pretrage" u radu se opisuju tehnički uvjeti i način provođenja ove mjere. Potom se iznosi kratak poredbeni prikaz. Osobita pozornost posvećena je pravnom uređenju te mjere u Saveznoj Republici Njemačkoj budući da je u toj državi to pitanje izazvalo najburniju raspravu u području kaznenog prava u širem smislu u posljednjih nekoliko godina te budući da su se o tome izjasnili i najviši sudovi u toj državi. U poredbenom dijelu prikazuju se moguće pravne osnove za provođenje te mjere i u nekim drugim državama u kojima se ona primjenjuje ili u kojima se razmatra njezina primjena te se poduzimaju zakonodavni koraci u tom smjeru. Potom se pokušava utvrditi postoji li pravna osnova za provođenje te mjere u hrvatskom pravu, prema Zakonu o kaznenom postupku iz 1997. godine te novom Zakonu o kaznenom postupku iz 2008. godine. U zaključku se iznose razmišljanja o mogućnostima primjene ove mjere *de lege lata* i *de lege ferenda*, njezinoj korisnosti, ali i opasnosti od prevelikog posezanja u temeljna ljudska prava i slobode.

2. FORENZIČNI RAČUNALNI PROGRAMI I "ONLINE-PRETRAGA"

Korištenje daljinski upravljanih forenzičnih računalnih programa jest državni poseg u informacijsko-tehničke sustave (računala) osoba prema kojima se ta mjera primjenjuje radi dobivanja podataka preko komunikacijske mreže. Tim se izrazom dakle označuje skup različitih tehničkih sredstava i postupaka koji služe kako bi se iz jednog računalnog sustava prikriveno prikupili podaci putem zahvata provedenog iz daljine preko elektroničke mreže. Riječ je o elektroničkom otvaranju računalnog sustava od državnih istražnih tijela i elektroničkom prenošenju podataka s računala na kojem se mjera primjenjuje korištenjem posebnim forenzičnim računalnim programima.

Moguće je teoretski zamisliti i javnu primjenu forenzičnih računalnih programa u kojoj bi se ta mjera provodila uz znanje osobe prema kojoj se primjenjuje, no u ovom radu bit će riječi isključivo o prikrivenom posegu u računalni sustav.

Može se raditi o trenutačnom zahvatu prikupljanja informacija, ali i o nadziranju koje traje određeno vrijeme. Kao metoda prikupljanja informacija od

državnih tijela, njezina primjena moguća je sa svrhom prikupljanja dokaza za potrebe kaznenog postupka, kao policijska preventivna djelatnost te kao djelatnost sigurnosnih službi sa svrhom zaštite ustavnog ustrojstva države.

Za navedenu mjeru često se, osobito u zemljama njemačkog govornog područja, koristi i izraz "online-pretraga" (njem. "Online-Durchsuchung"). U njemačkoj stručnoj, ali i općoj javnosti, izraz "online-pretraga" obično je viši pojam koji obuhvaća i jednokratni zahvat, tzv. "online-pregled" (njem. "Online-Durchsicht") i nadziranje koje traje određeno razdoblje, tzv. "online--nadziranje" (njem. "Online-Überwachung").

Sieber, naprotiv, u svom stručnom mišljenju dostavljenom njemačkom Saveznom ustavnom sudu, pojmom "online-pretraga" pravilno označuje samo trenutni poseg 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" (njem. "Online-Zugriff"). Takva je terminologija prihvatljivija budući da je u terminologiji kaznenog procesnog prava pretraga procesna radnja koja ima jednokratni, trenutačni karakter, tj. ne traje određeno vrijeme.

Pored tog izraza, za označivanje navedene mjere, kao viši pojam, u uporabi je (osobito u Austriji) i izraz "online-istraživanje" (njem. "Online-Fahndung").

3. TEHNIČKI UVJETI I NAČINI PROVOĐENJA MJERE

Iako se o toj mjeri vodi burna rasprava, malo se zna o samom načinu odnosno mogućim načinima njezina provođenja.

Element koji je zajednički svim oblicima provođenja ove mjere i koji predstavlja glavno obilježje koje tu mjeru razlikuje od drugih oblika prikupljanja informacija jest uporaba posebnog forenzičnog računalnog programa koji se instalira na informacijsko-tehnički sustav (računalo) na kojem se mjera provodi, a koji prikuplja i prenosi informacije s "inficiranog" sustava osobi koja upravlja tim računalnim programom. Po svojoj prirodi riječ je o malicioznom računalnom programu, u pravilu je riječ o jednoj vrsti "trojanskog konja".[3]

[3] Jednostavnije računalne programe koji mogu prodrijeti u slabije zaštićena računala može se pronaći preko interneta i kupiti na crnom tržištu po cijeni od stotinu do više desetaka tisuća dolara, dok cijena za još nepoznate i stoga vrlo učinkovite (jer postoji velika vjerojatnost da ih ni ažurirani antispyware programi neće otkriti) trojance (tzv. "less-than-zerodays-exploits") prelazi stotinu tisuća dolara. *Sieber, Ulrich,* Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen, verzija 1.0 od 9. listopada 2007., str. 6. dostupno na: http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf. (zadnji posjet. 25. svibnja 2009.).

Budući da su autori tog "trojanskog konja" državna tijela, navedeni računalni programi kolokvijalno se nazivaju i "državni trojanski konji" ili kraće "državni trojanci".[4] Ponekad se koristi i izraz "govware", što je kombinacija pojmova "government" i "spyware", odnosno "policeware". U engleskom jeziku službeni tehnički naziv takve vrste računalnih programa jest "*remote forensic software"* (RFS).[5] Budući da navedeni pojam postaje sve više uobičajen i u državama izvan engleskog govornog područja, u nastavku ovog rada za navedeni računalni program koristit će se kratica RFS, puni hrvatski naziv "daljinski upravljan forenzični računalni program".

Takvi forenzični računalni alati imaju nekoliko posebnih obilježja. Mobilnost, kao obilježje koje je važno istaknuti znači da takvi programi mogu prelaziti s računala na računalo koristeći se internetom kao prijevoznim sredstvom, što može uzrokovati niz problema, od toga da ti programi dođu u posjed trećih osoba pa do problema teritorijalnosti i dr. Autonomnost, kao daljnje važno obilježje nekih RFS-a, znači da takvi programi koji su u određenoj mjeri autonomni mogu u nekim situacijama prikupljati određene informacije i izvan zahtjeva osobe koja "upravlja" programom, što može dovesti do izlaženja iz sadržajnih ili vremenskih okvira određenih nalogom o primjeni te mjere.

Postupak uporabe daljinski upravljanog forenzičnog računalnog programa za prikupljanje podataka obično se dijeli u tri stadija: infiltracija u sustav osumnjičenika, dobivanje podataka i njihovo prenošenje te okončanje mjere.[6]

3.1. Infiltracija

Infiltracija jest stadij postupanja u kojem se na ciljani računalni sustav instalira poseban forenzični računalni program, RFS. Postoji više načina provođenja infiltracije, pri čemu se mogu razlikovati dvije glavne grupe metoda. Infiltracija se može odvijati isključivo preko interneta ili se RFS može naći na računalu fizičkim putem, tj. spajanjem s računalom nekog medija za prenošenje (pohranu) podataka na kojem je snimljen RFS i njegovim prebacivanjem na to računalo.

[4] U Njemačkoj i Austriji, kao saveznim državama, umjesto izraza "državni trojanac" u prvilu se koristi izraz "savezni trojanac" ("Bundestrojaner"). Tu je riječ u Austriji stručni žiri kojim je predsjedao Rudolf Muhr s Instituta za germanistiku Sveučilišta u Grazu 2007. izabrao za riječ godine.

[5] Taj se naziv koristi i u njemačkom Ministarstvu unutarnjih poslova. V. Spiegel-Online: Netzticker – Bundes-Trojaner sind spähbereit: http://www.spiegel.de/netzwelt/web/0,1518,502542,00.html (zadnji posjet. 15. svibnja 2009.).

[6] *Hansen, Markus; Pfitzmann, Andreas; Roßnagel, Alexander,* Online-Durchsuchung, Deutsche Richterzeitung, 2007., str. 226.

3.1.1. Infiltracija RFS-a putem interneta

O toj metodi infiltracije ciljanog računala RFS-om riječ je kad RFS na računalo stiže putem interneta. Internetska metoda infiltracije može se dalje podijeliti na one koje se provode uz (nesvjesnu) aktivnu pomoć samog korisnika ciljanog računalnog sustava te metode za provođenje koje nije potrebna aktivna pomoć korisnika računala.[7]

Jedna od najčešćih metoda infiltracije računala putem interneta koja računa na pomoć korisnika ciljanog računalnog sustava jest slanje određenih dokumenata ili programa u prilogu (attachmentu) elektroničke pošte. U ovom slučaju korisnik mora elektroničku poštu, odnosno njezin prilog, otvoriti kako bi započeo proces prenošenja, tj. instalacije navedenog računalnog programa sadržanog u prilogu elektroničke pošte na tvrdi disk ciljanog računala. Navođenju korisnika da otvori određeni dokument (koji se nalazi u attachmentu, tj. prilogu poruke) služi naslov ili popratni tekst koji treba biti zanimljiv korisniku kako bi ga naveo pokušati doći do njega.[8] Daljnja mogućnost infiltracije računala jest navođenje na pregledavanje određenih web-stranica koje korisniku mogu nuditi određene dokumente ili ga navode na download i pokretanje nekog računalnog programa. Nadalje, može se raditi o tzv. phishingu, tj. imitiranju izgleda nekih službenih stranica nekih tvrtki ili državnih tijela koje zahtijevaju od korisnika poduzimanje određene radnje koja će neprimjetno prouzročiti aktivaciju RFS-a na računalo.

Drugu podgrupu isključivo računalne infiltracije ciljanog računala predstavljaju načini koji ne zahtijevaju aktivno djelovanje korisnika kojim bi on sam pridonio instalaciji RFS-a. Riječ je uglavnom o korištenju propustima u sigurnosnom sustavu računala.[9] Najčešće je riječ o korištenju propustima u programima za pregledavanje web-stranica (web-preglednici, npr. Internet Explorer, Mozilla Firefox i dr.), u programima za rad s elektroničkom poštom ili u samom operacijskom sustavu. Kod te metode potrebno je iskoristiti prikladan trenutak, budući da proizvođači tih programa, u pravilu, čim uoče krupnije propuste, žurno reagiraju te nude novije verzije tih programa koje nemaju više takvih propusta ili nadopune (tzv. *patch*) za postojeće verzije.[10] No, valja istaknuti da velik broj korisnika (iz neznanja ili drugih razloga) i ne instalira novije verzije ili nadopune odmah nakon što se pojave, što njihov računalni sustav ostavlja izrazito podložnim napadu.

---

[7] Ibid.

[8] Najčešće je riječ o nuđenju raznih mogućnosti brze i lake zarade te linkovima na razne atraktivne sadržaje. Ibid. Pritom se mora voditi računa o tome da navođenje na otvaranje nekog dokumenta ne smije biti poticanje na počinjenje kaznenog djela.

[9] Ibid.

[10] Ibid.

3.1.2. Fizička infiltracija RFS-a

Fizičkom infiltracijom RFS-a na ciljano računalo smatra se svaka metoda infiltracije koja se ne odvija preko interneta, već se RFS unosi u ciljano računalo fizičkim putem, tj. spajanjem s računalom nekog medija za prenošenje (pohranu) podataka (prijenosna memorija, CD, DVD, vanjski tvrdi disk i dr.) na kojem je snimljen RFS i njegovim prebacivanjem na to računalo.

Uobičajeni način fizičke infiltracije ciljanog računala jest ulazak djelatnika državnih tijela koja provode tu mjeru u prostoriju u kojoj se nalazi ciljano računalo, pristup tom računalu te instalacija RFS-a na tvrdi disk računala.[11]

Pored ulaska u prostoriju u kojoj se nalazi računalo, postoje i drugi načini moguće fizičke infiltracije RFS-a na ciljano računalo. Moguće je na razne medije za prijenos i pohranu podataka (CD, DVD, prijenosne memorije i dr.) snimiti RFS koji će na takav način doprijeti do ciljanog računala. Takve medije treba na neupadljiv način dostaviti osobi čiji informacijsko-tehnički sustav treba pretražiti.[12] Nužno je spomenuti i da trojanci moraju biti posebno prilagođeni određenom operacijskom sustavu.[13]

3.1.3. Mogući problemi prilikom infiltracije RFS-a u ciljano računalo

Zanimljivo je da je pitanje korištenja daljinski upravljanim forenzičnim računalnim programom izazvalo ogromnu pažnju i raspravu u stručnoj, ali i općoj javnosti niza europskih zemalja, dok je istovremeno u velikoj mjeri vrlo upitno koliko se uspjeha može očekivati u provođenju te mjere. Glavni problem koji se javlja prilikom pokušaja infiltracije tih računalnih programa jesu mjere zaštite računalnih sustava. U računalo na koje su instalirani najnoviji programi koji ne sadržavaju (poznate) sigurnosne propuste mnogo je teže prodrijeti trojancem, osobito ako to računalo ima još neke metode zaštite, poput antivirusnih i antispyware programa te vatrozida (*firewall*).

Većina velikih proizvođača antispyware programa u početku je načelno otklonila mogućnost suradnje s državnim tijelima prilikom infiltracije RFS-a

[11] U ovoj varijanti primjene mjere korištenja RFS-om za prikupljanje podataka infiltracija tog računalnog programa sadržava u sebi i ulaz u prostorije radi pristupa računalu, jednako kao u slučaju instaliranja uređaja za tehničko snimanje prostorija kod provedbe posebne izvidne mjere ulaska u prostorije radi provođenja nadzora i tehničko snimanje prostorija iz čl. 180. st. 1. t. 2. ZKP/97.

[12] Poželi li korisnik, primjerice, poslušati određeni glazbeni CD, koji je prerađen tako da sadržava špijunski program, infiltracija RFS-a u računalni sustav može uslijediti i samim umetanjem CD-a u računalo te automatskim pokretanjem. Ibid.

[13] Na većini današnjih osobnih računala instalirana je neka od verzija operacijskog sustava Windows, tvrtke Microsoft.

tako da bi sami ti proizvođači tih programa namjerno propustili RFS, tj. državne trojance, tj. da antivirusni odnosno antispyware programi tih proizvođača propuste detektirati korisniku prisutnost državnog trojanca na njegovu računalu.[14]

Problem takvog pristupa je u tome što postoji relativno velika mogućnost da s korisnika ciljanog računala inficiranog RFS-om taj računalni program (u pravilu bez namjere i znanja korisnika) prijeđe na druga računala. Moguća je i situacija da nad tim programom koji se nađe na nekom računalu kontrolu nemaju državna tijela, izvorni autori tog programa, već treća osoba.[15]

Naravno, u slučaju da ni proizvođačima antispyware programa određeni državni trojanac nije poznat, ne postoji jamstvo da će ga antispyware program odmah detektirati i upozoriti korisnika.[16] No valja istaknuti da najnoviji antispyware programi imaju vrlo dobro razvijen heuristički sustav prepoznavanja malicioznih računalnih programa, što znatno povisuje razinu zaštite i smanjuje mogućnost iniciranja računala nekim novim malicioznim računalnim programom koji još nije prepoznat kao takav i koji još nije stavljen na listu takvih programa.

Ima i prijedloga da se proizvođače antispyware računalnih programa obveže na suradnju, tj. da su dužni propustiti državnog trojanca.[17] No, prema dostupnim informacijama, ni u jednoj državi to još nije učinjeno, između ostalog i zbog navedenih problema kontrole nad tim računalnim programom.[18]

Iako su mjere antivirusne i antispyware zaštite računala doista problem prilikom instalacije RFS-a na ciljano računalo, informatički stručnjaci navode da u većini slučajeva postoji metoda kako računalnim putem zaobići sve navedene prepreke i sigurno instalirati RFS na ciljano računalo.[19]

---

[14] Marc Maiffret, glavni tehnološki ekspert i suosnivač tvrtke eEye Digital Security bio je izričit: "Naši klijenti plaćaju nam za uslugu da ih štitimo od svih oblika malicioznih računalnih programa. Nije na nama da radimo policijski posao umjesto njih i mi ne činimo, i nećemo činiti, nikakve iznimke za policijske malware računalne programe i druge slične alate." McCullagh, Declan; Broache, Anne, Will security firms detect police spyware?, dostupno na: http://news.cnet.com/2100-7348-6197020.html?tag=tb (zadnji posjet 22. svibnja 2009.).

[15] Graham Cluley iz renomirane tvrtke Sophos koja se bavi sigurnosnom zaštitom računalnih sustava je kazao: "Ne možemo znati je li neki program napisao FBI, a čak i kad bismo to znali, ne bismo mogli znati da li se njime trenutno koristi FBI ili njime upravlja treća osoba." Jackson, William, Antivirus vendors are wary of FBI's Magic Lantern – Government Computer News, Gcn.com.

[16] *Hansen, Pfitzmann,* op. cit., bilj. 6., str. 226.

[17] I telekomunikacijske tvrtke obvezne su surađivati s policijom i pravosudnim tijelima pri provođenja posebnih izvidnih mjera nadzora telekomunikacija.

[18] Valja očekivati da bi se u toj situaciji informatički vještiji kriminalci okrenuli korištenju *open source* antivirus i antispyware programima.

[19] *Hansen* i *Pfitzmann* ističu da u Njemačkoj, primjerice, već postojeći međusklopovi za nadziranje, koji radi provedbe mjera nadzora telekomunikacija moraju biti instalirani kod svakog internetskog providera u toj zemlji, mogu bez većih problema biti reprogramirani se svr-

3.2. Pristup podacima i prenošenje podataka

Nakon uspješne infiltracije slijedi stadij pristupa podacima i njihovo prenošenje. Taj stadij često se naziva "online-pretragom" u užem smislu. Koristeći se instaliranim RFS-om, istražitelji imaju putem interneta pristup računalu i mogu pristupiti podacima sadržanim na računalu te provesti njihovo pretraživanje, snimanje i prenošenje.[20]

3.2.1. Mogućnosti pristupa podacima, njihova snimanja i prenošenja

Radi preciznog razgraničenja pojedinih načina provođenja ovog stadija, što ima vrlo značajne procesnopravne posljedice, potrebno je navesti različite mogućnosti bilježenja, snimanja, pretraživanja te prijenosa podataka s računala na kojem se mjera primjenjuje, tj. koje su sve mogućnosti koje pruža uporaba RFS-a.

a) Nadzor komunikacije

Prije svega, uporaba RFS-a može predstavljati tehnički način provedbe mjere nadzora telekomunikacija. Pojavom interneta, računalo je postalo vrlo važno sredstvo komunikacije. Uporaba elektroničke pošte postala je svakodnevni dio života i u velikoj mjeri potisnula tradicionalnu pisanu komunikaciju koja se koristila poštanskim uslugama. Povećanjem brzine pristupa internetu (download i upload) započelo se s glasovnim komuniciranjem preko interneta (VoIP, Voice over Internet Protocol). Internetska telefonija posljednjih je nekoliko godina doživjela ogromnu ekspanziju, prije svega zahvaljujući vrlo niskim troškovima korištenja odnosno za komunikaciju s računala na računalo potpuno besplatnom korištenju.[21] Postoji niz VoIP programa od kojih je svakako najpopularniji program Skype istoimene tvrtke. Nadzor i snimanje telefonskih razgovora vođenih preko interneta korištenjem RFS-a instaliranog na računalo jednog od sugovornika predstavlja moguću primjenu tog

hom infiltracije trojanaca tijekom bilo kakvog neosiguranog skidanja (download) računalnih programa (software). Takav način infiltracije trojanca izravni je poseg protiv kojeg su i najbolji načini zaštite nemoćni. Ibid.

[20] Osoba koja upravlja trojancem može i zamijeniti podatke na "inficiranom" računalu. Ibid., str. 227.

[21] Internetska telefonija gotovo je potpuno potisnula telefonske razgovore kad je riječ o međunarodnim razgovorima, a korisnici se sve više njome koriste i za razgovore unutar određene države. Korisnicima su razgovori s računala na računalo potpuno besplatni ako imaju *flat rate* pristup internetu, što danas postaje pravilo.

računalnog programa. To osobito vrijedi kad je riječ o VoIP komunikaciji koja je enkriptirana (zaštićena šifriranjem), kao što je to slučaj kod već spomenutog najpopularnijeg programa te vrste Skype.[22] Pored elektroničke pošte te VoIP komunikacije, RFS može služiti i za nadzor ostalih oblika komunikacije putem računala, npr. *chat,* raznih društvenih mreža (od koji je najrasprostranjeniji *Facebook*) i dr.

b) Pretraga i prijenos pohranjenih podataka

Pored nadzora komunikacija putem računala, drugo glavno područje primjene RFS-a jest pretraživanje, snimanje te prenošenje podataka spremljenih na računalu (tvrdom disku računala, radnoj memoriji i dr.). Ovo područje primjene RFS-a izaziva mnogo više prijepora, reakcija, ali i pravnih problema. Riječ je praktično o pretrazi računala, a problem predstavlja tajnost primjene RFS-a. Naime, u gotovo svim pravnim sustavima pretraga računala je procesna radnja s provođenjem koje je korisnik ciljanog računala upoznat. Za ispravnost njezine primjene odnosno za autentičnost dobivenih rezultata predviđeno je poštovanje određenih jamstava njezina pravilnog provođenja, što kod tajne pretrage tvrdog diska računala putem RFS-a nije slučaj.

Pri bilježenju, snimanju i prenošenju pohranjenih podataka potrebno je razlikovati dvije situacije. U prvoj situaciji RFS bilježi unos određenih podataka u računalo putem vanjskih jedinica (u pravilu tipkovnice računala) te na osnovi tih podataka rekonstruira sadržaj dokumenta. Računalni program koji bilježi unos podataka u računalni sustav naziva se *keylogger*.[23] Takav program osobito je prikladan za bilježenje raznih lozinki (lozinke za elektroničku poštu, VoIP i brojne druge sadržaje), što kasnije omogućuje, primjerice, nesmetano čitanje elektroničke pošte s nekog drugog računala. Primjenom takvog programa moguće je međutim zabilježiti samo one unose podataka koji su načinjeni nakon instalacije *keyloggera* na računalo. Ako se želi ustanoviti što je sve snimljeno na tvrdi diska računala prije infiltracije *keyloggera*, nužno je da RFS, pored *keylogginga*, ima i mogućnost pretrage, snimanja i prenošenja podataka i dokumenata koji su već prije učinjeni i pohranjeni na računalu.

[22] Tvrtka Skype navodi da su razgovori vođeni preko njihova istoimenog programa enkriptirani "jer se koriste javnim internetom kako bi prenijeli razgovore i poruke koji se ponekad prenose preko drugih korsnika. Enkripcija Skypea osigurava da nepozvane treće osobe ne mogu slušati razgovore ni čitati poruke poslane tim programom." http://support.skype.com/en/faq/FA144/Why-are-Skype-calls-encrypted?frompage=search&q=encrypted (zadnji posjet 22. svibnja 2009.). EUROJUST je izrazio želju za stvaranjem pravne regulative koja će omogućiti slušanje razgovora osumnjičenika preko Skypea. http://www.mvpei.hr/ei/default.asp?ru=588&gl=200902240000029&sid=&jezik=1 (zadnji posjet 22. svibnja 2009.).

[23] Kovanica riječi *keystroke* i *logging*.

Ako u vrijeme unošenja određenih podataka u računalo (npr. pisanja nekog teksta te snimanja tog teksta na tvrdi disk računala) računalo nije spojeno na internet, prikupljene podatke moguće je spremiti u međuspremnik te ih prenijeti kad računalo bude spojeno internetskom vezom.[24]

c) Akustični i videonadzor

Naposljetku, uz nadzor komunikacija i pretragu sadržaja pohranjenih na računalu, postoje i neka druga, vrlo zanimljiva područja primjene daljinski upravljanih forenzičnih računalnih programa. Na računalu na kojem je takav program instaliran moguće je uključiti uređaj za snimanje zvuka (bilo da je riječ o mikrofonu koji čini sastavni dio računala, bilo da je riječ o uređaju koji je naknadno kupljen pa spojen s računalom) i tako izvesti tehničko audiosnimanje prostorije u kojoj se računalo nalazi. Isto vrijedi i za vizualni nadzor i snimanje, ako računalo ima instaliranu kameru. Naime, na mnogobrojna računala instalirana je web-kamera, dok mnoga prijenosna računala novije proizvodnje imaju ugrađenu kameru. Za većinu korisnika osnovna svrha kamere na računalu jest omogućiti videotelefonsku vezu, tj. korisnicima usluga internetske telefonije pored audioveze omogućiti i video, vizualnu vezu. No, jasno je da se kamera na računalu može iskoristiti kao sredstvo tehničkog snimanja prostorije u kojoj se računalo nalazi. Potrebno je samo pronaći način kako uključiti kameru, što nije problem ako je na to računalo instaliran RFS.[25] Situacija postaje još složenija ako je riječ o prijenosnom računalu koje korisnik nosi sa sobom.

d) Nadziranje korištenja računalom u određenom razdoblju

Naravno, moguća je i kombinacija navedenih pristupa, što pruža gotovo potpuni nadzor nad radom korisnika na računalu u određenom razdoblju. Taj oblik korištenja RFS-a svakako je najveći poseg u ustavna prava, budući da pored nadzora komunikacije, jednokratne pretrage pohranjenih sadržaja te eventualnog audio i videonadzora uključuje i saznanje o takvim podacima koji se ne mogu smatrati internetskim komuniciranjem, a nisu ni pohranjeni na računalu, već se samo privremeno zadržavaju u radnoj memoriji računala radi obavljanja određene radnje, npr. razni unosi kod internetskog bankarstva. Nužno je upozoriti da svaki trojanac *keylogger* bilježi takve podatke,

[24] Ibid., str. 227.

[25] Pri uključivanju kamera i mikrofona računala, problem s uključenom kamerom je taj što je tada u pravilu uključeno i signalno svjetlo koje pokazuje da je kamera uključena.

što stvara velike probleme pri ograničavanju na prikupljanje samo određenih podataka, npr. samo internetske komunikacije.

3.2.2. Problemi prilikom pristupa podacima, njihova snimanja i prenošenja

U poredbenoj se literaturi upozorava na to da računalo s instaliranim RFS--om (koji je po svojoj prirodi, kako je već istaknuto, maliciozni računalni program, u pravilu trojanac) nije pod potpunom kontrolom ni samog korisnika ni osoba koje upravljaju tim računalnim programom, već obiju strana. U takvoj situaciji nije moguće zajamčiti autentičnost prenesenih podataka.[26] Takvu potvrdu autentičnosti može načelno pouzdano pružiti samo onaj tko ima isključivu kontrolu nad sustavom (u ovom slučaju računalom). Taj prigovor jedan je od najvažnijih, potpuno utemeljenih, prigovora, provođenju ove mjere. Nadalje, kod računala infiltriranog trojancem ne može se isključiti ni mogućnost da netko treći (npr. putem nekog drugog instaliranog trojanca) eventualno istovremeno ima djelomičnu kontrolu nad računalom s instaliranim državnim trojancem.[27]

Prilikom primjene RFS-a potrebno je utvrditi koje su mogućnosti računalnog programa kojim se želi koristiti te u kolikoj je mjeri njegovo djelovanje autonomno. Poželjno je da se infiltrira onaj forenzični računalni program koji je načinjen samo za obavljanje one zadaće koja se njegovom uporabom želi postići.[28] Primjerice, ako se želi nadzirati elektronička pošte ili VoIP komunikacije, takav program ne mora sadržavati mogućnost pretrage podataka ili dokumenata pohranjenih na tvrdom disku računala. Nadalje, prilikom koncipiranja takvog računalnog programa treba težiti da njegovo djelovanje bude što je moguće manje autonomno, tj. da podaci koje program šalje osobi koja njime upravlja budu oni podaci kojih je prijenos naložila osoba koja upravlja programom. U suprotnom, program sam šalje i više od onog što treba odnosno više od onog što je dopušteno rješenjem o određivanju primjene te mjere.[29] Ta

[26] Ibid. Tako i *Sieber*, op. cit. bilj. 3. str. 18-19, i *Abel, Wiebke*, Agents, Trojans and tags: the next generation of investigators, 23:1-2 International Review of Law, Computers & Technology, str. 103.

[27] Već je spomenuto da je, za vrijeme dok inficirano računalo nije spojeno na internet, prikupljene podatke moguće spremiti u međuspremnik te ih prenijeti kad računalo bude spojeno internetskom vezom. Ovo međuspremanje je osobito opasno za korisnika računala prema kojem se vrši mjera budući da je neovlašten pristup podacima u tom međuspremniku od strane trećih osoba u velikoj mjeri olakšan. Ibid. O integritetu prikupljenih dokaza v. i:

[28] *Abel,* op. cit. bilj. 26. str. 107.

[29] Manja autonomnost programa poželjna je i sa stajališta zaštite ljudskih prava, ali i sa stajališta radnih resursa budući da velike količine prenesenih podataka poslije zahtijevaju mnogo

se metoda može pokazati problematičnom zbog toga što se lako može dogoditi da se inficiraju, pored ciljanog, ili umjesto njega, računala drugih korisnika, čime se povređuju temeljna prava drugih osoba prema kojima se mjera ne primjenjuje.

3.3. Okončanje mjere

Po završetku primjene mjere potrebno je predvidjeti način njezina okončanja. Neki programi imaju vremenski određeno djelovanje nakon čega se pokreće postupak samouništenja. U protivnom, potrebno je provesti postupak koji će pouzdano odstraniti RFS s računala osobe prema kojoj se mjera primjenjivala. To osobito vrijedi u slučajevima u kojima više ne postoji sumnja koja je bila osnovom za određivanje primjene mjere. Pritom se mora paziti da se u računalu odstranjivanjem trojanca ne stvore nove sigurnosne rupe ili da ne dođe do daljnjeg prijenosa podataka za koji više nema pravne ovlasti.[30]

4. POREDBENI PREGLED

U poredbenom dijelu ovog rada osobita pozornost posvećena je pravnom uređenju ove mjere u Saveznoj Republici Njemačkoj. Razloga za to je više: u toj je državi ovo pitanje izazvalo najburniju raspravu u području kaznenog prava u širem smislu u posljednjih nekoliko godina, o tome su se u određenom dijelu izjasnili i najviši sudovi u toj državi, a od 1. siječnja 2009. korištenje forenzičnim računalnim programima pravno je uređeno u posebnom zakonu na pravnotehnički vrlo visokoj razini, na način koji je sigurno neusporedivo kvalitetniji, kako sa stajališta pravne određenosti, tako i sa stajališta zaštite temeljnih ljudskih prava. Potom se iznosi kratak prikaz korištenja forenzičnim računalnim programima u nekim drugim državama. Budući da je u njemačkoj stručnoj pa i općoj javnosti naziv "online-pretraga" već uvriježen, prilikom izlaganja pravnog uređenja upotrebe forenzičnih računalnih programa u toj državi rabi se u pravilu taj izraz.

vremena za odvajanje bitnih podataka od onih koji su potpuno beskorisni tijelu koje provodi mjeru.

[30] Do stvaranja sigurnosnih rupa u računalnom sustavu može doći npr. zbog ponovnog učitavanja sigurnosne kopije podataka (*backup*), koju je korisnik napravio tijekom provođenja mjere, pa je na toj kopiji snimljen i RFS koji se sad ponovo unosi u računalo.

4.1. Savezna Republika Njemačka

4.1.1. Online-pretraga za potrebe kaznenog postupka u njemačkom pravu

Odobravanje primjene online-pretrage radi prikupljanja dokaza za potrebe kaznenog postupka je u Saveznom vrhovnom sudu SR Njemačke bilo je vrlo prijeporno. Državno odvjetništvo uputilo je prvi zahtjev sudu za odobravanjem primjene tajne online-pretrage računala okrivljenika početkom 2006. godine. Sudac istrage najprije je odlukom od 21. veljače 2006. naložio "pretragu osobnog računala okrivljenika, osobito podataka pohranjenih na tvrdom disku i radnoj memoriji". Pravni temelj za odobravanje takve mjere pronašao je u propisima o pretrazi stana.[31]

No, 25. studenoga iste godine drugi sudac istrage odbio je zahtjev glavnog državnog odvjetnika za provođenjem druge tajne online-pretrage.[32] Odbijanje zahtjeva obrazložio je nepostojanjem pravnog temelja za *tajno* provođenje takve mjere budući da zakon za provođenje (obične) pretrage predviđa obveznu nazočnost svjedoka i vlasnika objekta pretrage odnosno njegova zastupnika.[33] Protiv navedene odluke o odbijanju zahtjeva glavni državni odvjetnik uložio je žalbu koju je vijeće Saveznog vrhovnog suda odbilo 31. siječnja 2007.[34]

Razlog odbijanja bio je taj što, prema mišljenju Saveznog vrhovnog suda, u postojećim propisima kaznenog procesnog prava ne postoj pravni temelj, tj. zakonska ovlast za provođenje te mjere.[35] Takav bi poseg bio "ozbiljno zadiranje u pravo na informacijsko samoodređenje".[36] Sud je upozorio da

---

[31] Beschluss vom 21. Februar 2006 – Az. 3 BGs 31/06. Odluka je dostupna na: http://www.hrr-strafrecht.de/hrr/3/06/3-bgs-31-06.php (zadnji posjet 15. travnja 2009.).

[32] Beschluss vom 25. November 2006 – Az. 1 BGs 184/2006. Odluka je dostupna na: http://www.hrr-strafrecht.de/hrr/1/06/1-bgs-184-2006.php (zadnji posjet 15. travnja 2009.).

[33] Čl. 105. st. 2 StPO (za svjedoke) i čl. 106. st. 1. za vlasnika.

[34] Odluku je donio 3. kazneni senat Saveznog vrhovnog suda. Beschluss des 3. Strafsenats des BGH vom 31. Januar 2007 – StB 18/06BGH, - Ermittlungsrichter des BGH. Odluka je dostupna na: http://www.hrr-strafrecht.de/hrr/3/06/stb-18-06.php (zadnji posjet 15. travnja 2009.).

[35] Nakon donošenja navedene presude Ministarstvo unutarnjih poslova izdalo je priopćenje za tisak u kojem je savezni ministar unutarnjih poslova Wolfgang Schäuble istaknuo da je iz "istražno-taktičkih razloga nužno da tijela kaznenog progona imaju mogućnost, na temelju sudske odluke, provesti tajnu online-pretragu" te je zatražio žurnu izmjenu Zakona o kaznenom postupku u tom smjeru. Suprotno tome, savezna ministrica pravosuđa Brigitte Zypries istaknula je u razgovoru za Berliner Zeitung da je tajna online-pretraga ekstreman zahvat u privatnost. Istaknula je da prije eventualnog uvođenja tog istražnog instrumenta "moraju biti razjašnjene tehničke mogućnosti, posljedice i ustavnopravne pretpostavke" te je upozorila na potrebu zaštite trećih osoba.

[36] Njemački Savezni ustavni sud izveo je pravo na informacijsko samoodređenje (koje bi se moglo ukratko opisati kao pravo odrediti uporabu vlastitih osobnih podataka) iz prava na pri-

nije dopušteno kombinirati pojedine elemente raznih ovlasti posezanja u prava 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.[37]

4.1.2. Online-pretraga kao mjera zaštite ustavnog poretka u njemačkom pravu koju su primjenjivale obavještajne službe

U prosincu 2006. godine parlament savezne države Sjeverne Rajne-Vestfalije donio je novelu tamošnjeg Zakona o zaštiti ustavnog poretka (*das Verfassungsschutzgesetz*).[38] Tim zakonom proširene su ovlasti Službe za zaštitu ustavnog poretka te njemačke savezne države te joj je dopušteno s ciljem borbe protiv terorizma provesti tajnu online-pretragu računala osoba za koje se sumnja da na takav način ugrožavaju ustavni poredak. Za provedbu te mjere nije bilo potrebno ni prethodno sudsko odobrenje ni naknadna konvalidacija.[39] U zakonu je bilo navedeno da Služba za zaštitu ustavnog poretka smije primijeniti "tajno promatranje i drugo razjašnjavanje interneta, ... isto tako tajni zahvat u informacijsko-tehničke sustave pomoću tehničkih sredstava."[40]

Grupa građana podnijela je zahtjev za ispitivanjem ustavnosti navedenog zakona Saveznom ustavnom sudu.[41] Dana 27. veljače 2008. taj je sud donio odluku prema kojoj je navedene odredbe Zakona o zaštiti ustavnog poretka Sjeverne Rajne-Vestfalije o online-pretragama proglasio kao protivne njemačkom Temeljnom zakonu (*das Grundgesetz*).[42]

---

vatnost. To pravo taj je sud 1983. priznao kao novo temeljno pravo vezano uz zaštitu podataka; nije izričito navedeno u Ustavu, već je proizašlo iz judikature Saveznog ustavnog suda.

[37] *Hofmann* naprotiv drži da online-pretraga ima pravnu osnovu za provedbu već u postojećim propisima njemačkog Zakona o kaznenom postupku (StPO), i to u čl. 102. i 103. koji reguliraju procesnu radnju istrage. *Hofmann*. *Manfred*, Die Online-Durchsuchung - staatliches "Hacken" oder zulässige Ermittlungsmaßnahme? Neue Zeitschrift für Strafrecht, 2005., str. 123-125.

[38] Zakon o izmjenama i dopunama Zakona o zaštiti ustavnog poretka donesen je 25. 12. 2006.

[39] Više o online-pretrazi prema Zakonu o zaštiti ustavnog ustrojstva Sjeverne Rajne-Vestfalije v. *Huber, Bertold,* Trojaner mit Schlapphut - Heimliche "Online-Durchsuchung" nach dem Nordrhein-Westfälischen Verfassungsschutzgesetz, Neue Zeitschrift für Verwaltungsrecht, 2007., str. 880-884.

[40] Ibid., str. 881.

[41] *Bundesverfassungsgericht – dalje: BVerfG*. Među podnositeljima bio je i bivši savezni ministar unutarnjih poslova Gerhart Baum.

[42] Bundesverfassungsgericht: Urteil vom 27. Februar 2008 zu 1 BvR 370/07 und 1 BvR 595/07. Odluka je dostupna na: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html (zadnji posjet 27. travnja 2009.).

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".[43] 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".[44]

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, ustavnopravno 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.[45] 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.[46] 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."[47]

---

[43] Njem: "*das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"*. To novo temeljno pravo kolokvijalno se naziva računalnim temeljnim pravom ili temeljnim pravom na digitalnu intimnu sferu. V. *Kutscha, Martin,* Mehr Schutz von Computerdaten durch ein neues Grundrecht?, Neue Juristische Wochenschrift, 2008., Heft 15, str. 1043.

[44] Ibid.

[45] Točka 247. presude BverfG-a.

[46] Ibid.

[47] Točke 270.-271. presude BverfG-a. Izraz "'jezgra privatnog življenja" prijevod je njemačkog izraza *"Kernbereich privater Lebensgestaltung"*. Taj izraz označuje u njemačkom pravu, odnosno judikaturi BVErfG, dio intimne i privatne sfere čovjeka koji je apsolutno zaštićen od posega države, tj. koji ni u kakvim okolnostima ne smije biti povrijeđen. Tinnefeld postavlja pitanje je li uopće moguće provesti online-pretragu, a da se ne povrijedi jezgra privatnog življenja kao područja koje ni pod kakvim okolnostima ne bi smjelo biti povrijeđeno. Je li prethodna i naknadna sudska kontrola doista dostatno jamstvo koje će osjetljive podatke iz tog nedodirljivog područja sačuvati od neovlaštenog uvida? *Tinnefeld, Marie-Theres,* Online-Durchsuchung - Menschenrechte vs. virtuelle Trojaner, MultiMedia und Recht, 2007., Heft 3, str. 138-139. Kudlich upozorava da nije svaki sadržaj, samo zbog toga što se nalazi na tvrdom disku i što je zaštićen šifrom, dio jezgre privatnog življenja, ali da se gotovo sve što pripada tom apsolutno zaštićenom području osobnosti može nalaziti na tvrdom disku računala. *Kudlich, Hans,* Zur Zulässigkeit strafprozessualer Online-Durchsuchungen, Humboldt Forum Recht, 2007., prilog 19, str. 10.

Ugrožavanja osobnosti vezana uz pravo na informacijsko samoodređenje nastaju iz mnogostrukih mogućnosti države na prikupljanje i obradu podataka vezanih uz osobu te na korištenje njima. Prije svega pomoću elektroničke obrade podataka mogu se iz takvih informacija stvarati nove informacije i tako izvoditi zaključci. Izvedeni zaključci povređuju načelno zaštićene interese čuvanja tajne dotične osobe, a mogu dovesti i do posega u slobodu ponašanja te osobe.[48]

Ipak, pravo na informacijsko samoodređenje ne vodi u potpunosti računa o onim ugrožavanjima osobnosti koje nastaju iz činjenice da je pojedinac radi razvoja svoje osobnosti upućen na korištenje informacijsko-tehničkim sustavima te da pritom osobne podatke povjerava sustavu ili ih već samim korištenjem tim sustavom prisilno izručuje.[49] Treća osoba koja zadire u takav sustav može si pribaviti potencijalno ogromnu bazu podataka, bez potrebe upućivanja na druge mjere prikupljanja i obrade podataka. Takav je poseg daleko teži, u pogledu povrede osobnosti pogođene osobe, od pojedinačnog prikupljanja podatka, od čega štiti pravo na informacijsko samoodređenje. Ako ne postoji dovoljna zaštita od ugrožavanja osobnosti (koja nastaju zbog toga što je pojedinac radi razvoja svoje osobnosti upućen na korištenje informacijsko-tehničkim sustavima), opće pravo osobnosti, u svojoj funkciji popunjavanja pravnih praznina, vodi stoga računa o potrebi zaštite osobnosti. Dakle, opće pravo osobnosti pritom se tumači šire nego što je to bilo dosad uobičajeno (i prihvaćeno) kako bi zajamčilo integritet i povjerljivost informacijsko-tehničkih sustava.

Pravo na integritet i povjerljivost informacijsko-tehničkih sustava upravo se kao i pravo na informacijsko samoodređenje zasniva na općem pravu osobnosti iz čl. 2. st. 1. u vezi s čl. 1. st. 1. Temeljnog zakona. Ono također čuva područje osobnog i privatnog života nositelja tog temeljnog prava od državnog zahvata u području informacijske tehnike, i to štiti od posezanja u cjelokupni informacijsko-tehnički sustav, a ne samo od zahvata u pojedine komunikacijske događaje ili pohranjene podatke.[50]

Savezni ustavni sud se osvrnuo i na pitanje povređuje li online-pretraga temeljno pravo na nepovredivost doma.[51] Sud navodi kako online-pretraga tvrdog diska računala načelno ne povređuje pravo na nepovredivost doma, budući da je taj zahvat vezan uz računalo, a ne uz prostor u kojem je računalo fizički smješteno. Stoga pravo na nepovredivost doma ne pruža dovoljnu zaštitu od online-pretrage: "Budući da se taj zahvat može izvršiti neovisno o prosto-

[48] Točka 178. presude BVerfG-a.

[49] O ulozi osobnog računala u razvoju osobnosti čovjeka te nesmetanom odvijanju privatnog života v. *Tinnefeld,* op. cit., bilj. 47, str. 137-138.

[50] Točke 166.-167. presude BVerfG-a.

[51] Čl. 13. njemačkog Temeljnog zakona te čl. 34. hrvatskog Ustava.

ru, zaštita koja se odnosi na prostor ne može ukloniti posebna ugrožavanja informacijsko-tehničkog sustava".[52] Navedena načelna konstatacija da se online-pretragom ne povređuje pravo na nepovredivost doma vrijedi ako je infiltracija RFS-a provedena *online*, bez ulaženja u prostor u kojem se nalazi računalo na koje se želi instalirati program. No, drukčije je ako je instaliranje RFS-a izvršeno ulaskom u prostor u kojem je računalo smješteno ili ako se kamera li mikrofon instalirani na računalu (kojima se može upravljati putem RFS-a) bez pravne osnove koriste za nadziranje prostora u kojem je računalo smješteno.[53]

U Njemačkoj je u tijeku burna rasprava o ovlastima sigurnosnih službi na primjenu online-pretrage.[54]

[52] Točke 191.-193. presude BVerfG-a.

[53] Točke 194.-195. presude BVerfG-a. U pogledu judikature Europskog suda za ljudska prava, *Uerpmann* ističe da čl. 8. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda štiti pored privatnog i obiteljskog života ujedno i nepovredivost doma kao i korespondenciju. Od ta četiri područja zaštite privatni život ima najširi opseg. Svako od ostala tri područja poseban je izraz privatnog života te stoga striktna podjela navedenih područja nije nužna. U slučaju online-pretrage, tvrdi, moguće je da se radi i o povredi prava na nepovredivost stana ako se računalo nalazi u stanu. Navodi da je očito iz judikature ESLJP da taj sud ostavlja otvorenom granicu između stana i privatnog života. *Uerpmann-Wittzack, Jankowska-Gilberg,* Die Europäische Menschenrechtskonvention als Ordnungsrahmen für das Internet, MultiMedia und Recht, 2008., str. 83-89. No, takav stav ne smatram prihvatljivim, čemu u prilog ide i navedena presuda njemačkog Saveznog ustavnog suda o online-pretrazi.

[54] Magazin *Der Spiegel* u ožujku 2009. objavio je da je njemačka tajna služba u proteklim godinama pretražila najmanje 2.500 računala u inozemstvu i pritom također djelomično preslikala sadržaj tvrdog diska na pretraženim računalima. Pored preslika sadržaja tvrdog diska računala snimljeni su i unosi tipkovnicom u računalo te su stoga došli i u posjed lozinke za e-mail korisničke račune. Dostupno na: http://www.spiegel.de/netzwelt/web/0,1518,611954,00.html (zadnji posjet 13. svibnja 2009.).

Nakon pojavljivanja tih brojki u javnosti, velik broj i oporbenih političara i političara vladajuće velike koalicije zalaže se za ograničenje mogućnosti obavještajnih službi da se koriste online-pretragom. "Savezna obavještajna služba (Bundesnachrichtendienst - BND) treba za online-pretragu hitno pravni temelj" kazao je dopredsjednik kluba zastupnika CDU/CSU Wolfgang Bosbach magazinu *Spiegel*. Taj magazin navodi da Ured savezne kancelarke namjerava donijeti nove upute za službu kojima bi se uspostavio restriktivniji režim primjene te mjere, čime bi se isključila ilegalna djelovanja. Online-pretraga smjela bi se, prema najavama, provoditi samo prema načelu razmjernosti, nadzirao bi je službenik koji ispunjava uvjete za sudačku dužnost, a odobrenje za njezinu primjenu mogao bi dati samo predsjednik BND-a.

Bivši savezni ministar unutarnjih poslova Gerhart Baum (FDP) optužio je saveznu Vladu da je lagala Saveznom ustavnom sudu u pogledu broja slučajeva primjene online-pretrage u praksi. Ističe da je Vlada Ustavnom sudu navela da se radi samo o nekoliko slučajeva godišnje, dok je stvarna brojka mnogo veća. Baum, koji je bio jedan od podnositelja prijedloga za ispitivanje ustavnosti Zakona o zaštiti ustavnog ustrojstva Sjeverne Rajne-Vestfalije, najavljuje podnošenje takvog prijedloga i za izmijenjeni Zakon o saveznoj kriminalističkoj službi. http://www.spiegel.de/politik/deutschland/0,1518,612047,00.html (zadnji posjet 15. svibnja 2009.).

4.1.3. Online-pretraga kao mjera koju primjenjuje njemačka Savezna kriminalistička policija u borbi protiv terorizma

Njemačka zakonodavna reforma federalizma iz 2006. godine prenijela je zadaću obrane od opasnosti međunarodnog terorizma Saveznoj kriminalističkoj policiji (das Bundeskriminalamt, dalje: BKA). Rasprostranjeno je bilo stajalište da BKA ne raspolaže dovoljnim ovlastima koje bi joj omogućile kvalitetno ispunjavanje navedene zadaće. Policije pojedinih njemačkih saveznih zemalja česte su imale znatno šire ovlasti nego BKA. Stoga je njemački parlament 25. prosinca 2008. donio Zakon o obrani od opasnosti od međunarodnog terorizma putem Savezne kriminalističke policije.[55]

Taj zakon donosi izmjene Zakona o Saveznoj kriminalističkoj policiji i suradnji saveza i zemalja u poslovima kriminalističke policije (Bundeskriminalamtgesetz, dalje: BKAG ili BKA-zakon) kojim su izrazito proširene ovlasti BKA u borbi protiv terorizma.[56] Zanimljivo je da je zakon stupio na snagu odmah, tj. dan nakon objavljivanja u službenom glasilu (1. siječnja 2009. godine).

Tim se zakonom u Zakon o Saveznoj kriminalističkoj policiji unosi pododjeljak 3. kojim se u člancima unose nove ili proširuju već postojeće ovlasti BKA Zanimljivo je upozoriti na čl. 5. tog zakona o obrani od terorizma koji nosi naziv: Ograničenje temeljnih prava, gdje se navodi: "Temeljna prava slobode osobe (čl. 2. st. 2. reč. 2. Temeljnog zakona), prava pismovne, poštanske i dojavne tajne (čl. 10. GG) te prava na nepovredivost stana (čl. 13. GG) ograničavaju se u skladu s ovim zakonom".

U prijelaznim i završnim odredbama navedeno je da st. 1. br. 5 čl. 20.k kojim se u BKAG uvodi online-pretraga prestaje važiti 31. prosinca 2020. Takvo vremensko ograničavanje primjene neke mjere nije često u zakonodavstvima, a u njemačkoj stručnoj i općoj javnosti dočekano je sa skepsom. Prevladava mišljenje da će primjena te mjere biti produljena, tj. da će se primjenjivati i nakon isteka navedenog roka, a da takvo vremensko ograničenje predstavlja samo pokušaj smirivanja javnosti zabrinute zbog kršenja svojih ustavnih prava.

---

[55] Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, objavljen u službenim novinama, Saveznom zakonskom listu, Bundesgesetzblatt, 2008., dio I., br. 66., 3083, od 31. prosinca 2008.

[56] Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten). BKA-Gesetz. Pored izmjena BKA zakona (čl. 1.), taj zakon donosi manje izmjene Zakona o telemedijima (čl. 2.), Zakona o telekomunikacijama (čl. 3.) te Uredbe o nadziranju telekomunikacija (čl. 4.). V. Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur, Neue Juristische Wochenschrift, 2009., Heft 5, str. 257-262.

Rijetkost, osobito iz hrvatske perspektive, predstavlja čl. 6. Zakona o obrani od terorizma koji propisuje obvezu evaluacije primjene st. 1. br. 2. i br. 5. čl. 20.j i 20.k tog zakona, pet godina nakon stupanja na snagu navedenih propisa. Evaluaciju treba provesti znanstveni stručnjak (ili stručno tijelo) koji će biti određen u sporazumu s Bundestagom.[57] Navedeni članci podložni evaluaciji su čl. 4.a BKA-zakona koji propisuje pretpostavke pod kojima BKA može djelovati radi obrane od međunarodnog terorizma te čl. 20.j i 20.k koji uređuju rastersku pretragu (20.j) i prikriveni poseg u informacijsko-tehničke sustave (online-pretraga – 20.k).

U BKAG-u online-pretraga pravno je uređena u čl. 20.k te nosi naziv: *Prikriveni poseg u informacijsko-tehničke sustave*. Savezna kriminalistička policija smije bez znanja osobe prema kojoj se mjera primjenjuje tehničkim sredstvima prodrijeti u informacijsko-tehnički sustav kojim se osoba koristi i utvrditi tamo sadržane podatke, ako određene činjenice opravdavaju pretpostavku da postoji opasnost za a) život, tijelo ili slobodu neke osobe ili b) takva opća dobra ugrožavanje kojih dotiče temelje ili opstanak države ili temelje egzistencije ljudi.[58] Navedena mjera dopuštena je i u slučaju kad se još ne može s dovoljnom vjerojatnošću ustanoviti da bez njezina provođenja u bliskoj budućnosti nastupa šteta, ako određene činjenice upućuju na neku neposrednu opasnost koja prijeti u pojedinom slučaju za neko navedeno pravno dobro. Zakon propisuje i načelo supsidijarnosti primjene te mjere: ona se smije provoditi samo ako je nužna za ispunjavanje zadaća BKA u obrani od međunarodnog terorizma iz čl. 4.a odnosno ako bi ispunjavanje tih zadaća inače bilo bezizgledno ili znatno otežano.[59]

BKAG sadržava i neke odredbe kojih je svrha izbjegavanje ili barem smanjenje štete na računalu na kojem se mjera primjenjuje. Propisano je da se tehnički mora osigurati da na tom informacijsko-tehničkom sustavu budu izvršene samo one promjene koje su nužne za prikupljanje podataka i da prilikom okončanja mjere izvršene promjene budu, ako je to tehnički moguće, automatski vraćene u početno stanje.[60] Isto tako, Zakon nalaže da je umetnuto sredstvo (RFS) potrebno, prema stanju tehnike, štititi protiv neovlaštenog korištenja, a umnožene podatke, prema stanju tehnike, treba zaštititi od izmjene, neovlaštenog brisanja ili općenito neovlaštenog pristupa. U Zakonu nisu specificirani mogući načini provedbe infiltracije. Važno je istaknuti da nije propisana ni ovlast ulaska u prostorije u kojima se nalazi računalo u koje je potrebno instalirati RFS radi njegova instaliranja, što je zahtijevala policija.[61]

[57] Očekuje se da će zadaće te evaluacije nakon pet godina primjene, dakle 2014. godine, biti dodijeljene Max-Planck institutu za strano i poredbeno pravo u Freiburgu.

[58] Čl. 20.k, st. 1. BKAG.

[59] Ibid.

[60] Čl. 20.k, st. 2. BKAG..

[61] Roggan, op. cit., bilj. 43, str. 260.

Prilikom svakog umetanja tehničkih sredstava mora se protokolirati: 1. oznaka tehničkih sredstava i vrijeme njihova umetanja, 2. pojedinosti za identifikaciju informacijsko-tehničkog sustava i pritom poduzete trajne promjene, 3. pojedinosti koje omogućuju utvrđivanje prikupljenih podataka i 4. naziv organizacijske jedinice koja je provela mjeru.[62]

Primjenu ove mjere smije odrediti sud samo na zahtjev predsjednika Savezne kriminalističke policije ili njegova zamjenika.[63] Mjera se smije provesti i ako su druge osobe neizbježno zahvaćene provedbom mjere.

Sud nalaže primjenu mjere pisanim nalogom u kojem treba navesti: 1. osobu protiv koje se mjera izvršava, ako je to moguće, imenom i adresom, 2. što je moguće točniju oznaku informacijsko-tehničkog sustava u koji treba prodrijeti radi prikupljanja podataka, 3. način, opseg i trajanje mjere uz oznaku točnog vremena završetka primjene mjere, kao i 4. obrazloženje.[64] Primjena mjere može se odrediti u trajanju od najdulje tri mjeseca uz mogućnost produljenja za daljnja tri mjeseca, ako pretpostavke za određivanje mjere s obzirom na prikupljene spoznaje i dalje postoje. U slučaju da pretpostavke za određivanje mjere više ne postoje, mjere koje se provode na temelju naloga moraju se odmah okončati.[65]

Ako postoje činjenična uporišta za pretpostavku da bi se samom mjerom dobila saznanja iz jezgre privatnog življenja, mjera nije dopuštena. Ako je to moguće, mora se tehnički osigurati da se podaci koji se odnose na jezgru privatnog življenja ne prikupljaju.[66] Prikupljeni podaci moraju biti pregledani da bi se utvrdilo ima li sadržaja iz jezgre privatnog življenja. Taj se nadzor provodi pod nadzorom suda koji je odredio primjenu mjere, a provode ga ovlaštenik za zaštitu podataka Savezne kriminalističke policije i dva druga službenika Savezne kriminalističke policije, od kojih jedan ispunjava uvjete za imenovanje za sudačku dužnost.[67] Informacije koje se odnose na jezgru privatnog življenja ne smiju se koristiti i moraju se odmah brisati. Činjenice ustanovljenja tih podataka i njihovo brisanje moraju se dokumentirati.[68]

[62] Čl. 20.k st. 3. BKAG. Protokolirani podaci smiju se koristiti samo kako bi osobi prema kojoj se mjera primjenjivala ili za to ovlaštenoj javnoj službi bilo moguće dokazati da je mjera provedena u skladu s propisima. Protokolirani podaci moraju se čuvati do isteka naredne kalendarske godine nakon pohrane i onda automatski izbrisati, ako nisu potrebni za dokazivanje ispravnosti provedbe mjere.

[63] Čl. 20.k st. 5. BKAG.

[64] Čl. 20.k st. 6. BKAG.

[65] Ibid.

[66] Čl. 20.k st. 7. BKAG.

[67] Ibid. Propisano je da je ovlaštenik za zaštitu podataka prilikom izvršavanja te dužnosti slobodan od uputa i utjecaja.

[68] Ibid. Ta se dokumentacija smije koristiti isključivo za kontrolu zaštite podataka. Ona mora biti izbrisana ako više nije potrebna za tu svrhu, a najkasnije na kraju kalendarske godine koja slijedi iza godine dokumentiranja.

Očekuje se da će vladajuća koalicija pokušati proširiti područje primjene online-pretrage i na prikupljanje dokaza za potrebe kaznenog postupka.[69]

4.2. Republika Austrija

U Austriji se također vode rasprave je li korištenje daljinski upravljanim forenzičnim računalnim programima radi prikupljanja dokaza za potrebe kaznenog postupka dopušteno u okviru važećih odredbi Zakona o kaznenom postupku. U nedostatku odluka visokih sudova, prevladavaju stajališta da važeće odredbe nisu valjani pravni temelj za pretraživanje sadržaja tvrdog diska računala, no o tome se i dalje vode intenzivne rasprave. Formirana je i posebna Radna grupa Ministarstva pravosuđa i unutarnjih poslova sa zadaćom temeljitog proučavanja ove materije te davanja preporuka za zakonodavnu regulaciju. Radna grupa predala je početkom travnja 2008. godine ministrici pravosuđa i ministru unutarnjih poslova završni izvještaj koji nosi naziv: Proširenje istražnih instrumenata za borbu protiv teških, organiziranih i terorističkih oblika kriminala ("online-pretraga").[70] U izvještaju se navodi da bi tajna online-pretraga računala osumnjičenika korištenjem daljinski upravljanim forenzičnim računalnim programom načelno mogla biti dopuštena, no za primjenu te mjere predlaže određivanje strogih uvjeta. Ti bi uvjeti uključivali primjenu načela razmjernosti (što znači mogućnost primjene te mjere samo kod teških kaznenih djela), nužnost prethodnog sudskog odobrenja visokog sudskog tijela i dr.[71]

Zanimljivo je navesti da su ministrica pravosuđa i ministar unutarnjih poslova zajednički istaknuli da će se online-pretragom koristiti isključivo radi prikupljanja dokaza za potrebe kaznenog postupka.[72] Dakle, tom se mjerom u Austriji ne bi trebale služiti sigurnosne službe, a ni policija obavljajući svoje zadaće prevencije kriminala, što je sasvim suprotno od trenutno važećeg prav-

[69] To je već najavio potpredsjednik kluba zastupnika koalicije Wolfgang Bosbach (CDU). http://www.stern.de/computer-technik/internet/:Online-Durchsuchung-Ermittler--Computer/658712.html (zadnji posjet 20. svibnja 2009.).

[70] Erweiterung des Ermittlungsinstrumentariums zur Bekämpfung schwerer, organisierter und terroristischer Kriminalitätsformen ("Online-Durchsuchung"), Schlussbericht der Interministerielle Arbeitsgruppe "Online-Durchsuchung". BMJ/BMI. Izvještaj je dostupan na: http://www.justiz.gv.at/_cms_upload/_docs/AG_OnlineDurchsuchung_Endbericht.pdf (zadnji posjet 20. svibnja 2009.).

[71] Ministrica pravosuđa istaknula je da će primjena te mjere biti dopuštena samo kod kaznenih djela za koja se može izreći kazna zatvora u trajanju od najmanje deset godina. http://pressetext.at/news/080409031/bundestrojaner-verfassungsexperte-aeussert-vorbehalte/?phrase=online-durchsuchung (zadnji posjet 23. svibnja 2009.).

[72] Ibid.

nog uređenja u njemačkom pravu. U austrijskom Ministarstvu unutarnjih poslova procjenjuju da bi učestalost primjene online-pretrage bila svega jedan do dva puta godišnje.[73] Izmjene kojima bi se u Zakon o kaznenom postupku unijela mogućnost provedbe online-pretrage trebale su biti predložene parlamentu i izglasane najkasnije do kraja 2008. godine, no to još nije učinjeno.

4.3. Velika Britanija

Korištenje daljinski upravljanim forenzičnim računalnim programima u Velikoj Britaniji moguće je na temelju izmjena Zakona o zlouporabi računala (Computer Misuse Act) iz 1994. godine, Zakona policiji (Police Act) iz 1997. godine i Zakona o uređenju istražnih ovlasti (Regulation of Investigatory Powers Act) iz 2000. godine.[74] Iako su zakonske odredbe nedovoljno određene, smatra se da predstavljaju pravnu osnovu za provođenje te mjere, koja se u praksi doista i koristi.[75] Zakon o policiji, primjerice, u svom trećem dijelu uređuje ovlasti za određivanje mjera u pogledu imovine osumnjičenika; propisano je da nadležni službenik može naložiti poduzimanje neke mjere u pogledu imovine osumnjičenika, koju može pobliže označiti.[76] Može naložiti primjenu takve mjere ako vjeruje: a) da je poduzimanje te radnje nužno stoga što je vjerojatno da će ona biti od temeljne važnosti u prevenciji ili detekciji teških kaznenih djela i b) da nije razumno očekivati da se cilj koji se nastoji postići primjenom ove mjere može postići drugim sredstvima.[77] Na temelju tih odredbi, iako se u navedenom zakonu nigdje ne spominje pretraga računala korištenjem posebnim računalnim programima, izvodi se ovlast policije na prikriveni poseg u računalo osumnjičenika korištenjem forenzičnim računalnim programima, što je vrlo zanimljivo tumačenje upitne osnovanosti. Te ovlasti nešto su iscrpnije uređene u Zakonu o uređenju istražnih ovlasti.

[73] Ibid.

[74] Zakonom o policiji (Police Act) izmijenjene su odredbe Zakona o zlouporabi računala (Computer Misuse Act) iz 1990. godine.

[75] Richard Clayton, istraživač pri Računalnom laboratoriju Sveučilišta u Cambridgeu, istaknuo je da su daljinski upravljane pretrage računala moguće od 1994. godine, iako su se vrlo rijetko provodile. http://news.zdnet.co.uk/security/0,1000000189,39587597,00.htm (zadnji posjet 23. svibnja 2009.).

[76] Čl. 93. st. 1.a Zakona o policiji.

[77] Čl. 93. st. 2. Zakona o policiji. U smislu ove odredbe, teškim kaznenim djelom, sukladno čl. 93. st. 4. Zakona o policiji, smatra se djelo koje uključuje uporabu nasilja, rezultira značajnom financijskom dobiti ili je poduzeto od većeg broja osoba kojih je djelovanje bilo vođeno zajedničkom svrhom ako je riječ o djelu za počinjenje kojeg se može razumno očekivati da će počinitelj (osoba koja je navršila dvadeset jednu godinu i nije prije osuđivana) biti kažnjen kaznom zatvora u trajanju od najmanje tri godine.

Preduvjet za određivanje te mjere jest odobrenje višeg policijskog službenika. Nužno je istaknuti da policiji za provođenje te mjere nije potreban sudski nalog.

Vijeće Europske unije za pravosuđe i unutarnje poslove (Justice and Home Affairs Council - JHA) objavilo je u studenom 2008. godine Zaključke o usklađenoj radnoj strategiji i praktičnim mjerama protiv cyber-kriminaliteta.[78] Vijeće je pozvalo države članice i Europsku komisiju da uvedu mjere, u kratkim i srednje dugim rokovima, koje vode računa o napretku tehnologije, sa svrhom suzbijanja cyber-kriminaliteta. Pored ostalog, predloženo je i "olakšavanje daljinski upravljanih pretraga ako su predviđene domaćim pravom, olakšavajući istražiteljskim timovima brz pristup informacijama, uz odobrenje države domaćina". Iako zaključci Vijeća nisu obvezujući (*soft law*), očekuje se da će se brojne države pozivati na njih prilikom uvođenja te mjere u svoja prava.[79] Pozivom na Zaključke Vijeća EU za pravosuđe i unutarnje poslove iz studenoga 2008., britansko Ministarstvo unutarnjih poslova planira u suradnji s drugim državama članicama Europske unije provoditi online-pretrage u cijeloj Europi i drugim zemljama omogućiti provođenje te mjere u Velikoj Britaniji.[80]

4.4. Španjolska

U Španjolskoj je online-pretraga dopuštena pod sljedećim uvjetima: 1. riječ je o teškom kaznenom djelu, 2. online-pretraga najblaže je sredstvo kojim se

[78] Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime. Dokument je nastao na 2987. sastanku Vijeća za pravosuđe i unutarnje poslove koji je održan 27.-28. studenoga 2008. u Bruxellesu. Dostupno na: http://www.ue2008.fr/webdav/site/PFUE/shared/import/1127_JAI/Conclusions/JHA_Council_conclusions_Cybercrime_EN.pdf. (zadnji posjet 20. svibnja 2009.).

[79] Zanimljivo je podsjetiti na postupak koji je prethodio donošenju navedenih Zaključaka i izmjene u tekstu. 11. srpnja 2008. Predsjedničko vijeće EU objavilo je...

[80] *The Sunday Times* od 4. siječnja 2009. http://www.timesonline.co.uk/tol/news/politics/article5439604.ece Takav plan Ministarstva unutarnjih poslova izazvao je nagativne reakcije udruga za zaštitu ljudskih prava i opozicijskih članova parlamenta koji ističu da bi ta ovlast trebala biti precizno pravno uređena novim zakonom koji bi donio parlament, a osobito se ističe potreba da uvjet za takvo djelovanje policije bude prethodno sudsko odobrenje i naknadni nadzor. Upozorava se da su procesni uvjeti za odobravanje te mjere niži, a pravna jamstva slabija nego kod provedbe "tradicionalne" mjere pretrage stana, što je nedopustivo. Udruženje viših policijskih službenika (The Association of Chief Police Officers - ACPO) navelo je da su te ovlasti podrobno pravno uređene Zakonom o istražnim ovlastima. Glasnogovornik tog udruženja otkrio je da je policija već provela određeni, doduše vrlo mali, broj online-pretraga koje ulaze u brojku od 194 tajne pretrage domova, ureda i hotelskih soba koje je policija provela 2007. godine.

pouzdano mogu razjasniti činjenice počinjenja kaznenog djela, 3. postoji sudsko odobrenje koje uvijek mora biti vremenski ograničeno, 4. rezultati primjene te mjere moraju u primjerenom roku biti podneseni istražnom sucu; 5. korišteni forenzični računalni program ne smije naštetiti računalu na kojem se mjera primjenjuje te 6. po završetku online-pretrage kriminalistička policija koja provodi mjeru mora ukloniti navedeni računalni program s računala.[81]

4.5. Rumunjska

Rumunjska je jedna od rijetkih zemalja koja je u kazneno procesno zakonodavstvo unijela izričitu odredbu kojom dopušta prikriveni poseg u računalne sustave uporabom forenzičnih računalnih programa. Zakonom br. 508. iz studenoga 2004.[82] omogućeno je državnom odvjetniku u istražnom postupku poduzeti mjere posega u računalni sustav.[83] Prema čl. 16. st. 1.c tog zakona, državni odvjetnik može za određena kaznena djela (između ostalog za organizirani kriminal ili terorizam) istraživati postojanje i učestalost veza koje su među određenim osobama uspostavljene elektroničkom poštom. No, tu samostalne ovlasti državnog odvjetnika završavaju.[84] Ako iz tako prikupljenih informacija proizlazi dovoljno osnovana sumnja na počinjenje kaznenog djela te ako državni odvjetnik želi saznati sadržaj komunikacije elektroničkom poštom, postojanje koje komunikacije je utvrdio, zatražit će od suda izdavanje naloga na temelju kojeg će se provesti online-poseg na ciljano računalo. Iz zakonskog teksta ne proizlazi smije li pritom biti izvršena pretraga podataka pohranjenih na računalu (online-pretraga u užem smislu), pa je nejasno dopušta li ta odredba samo nadzor telekomunikacija korištenjem forenzičnim računalnim programom ili i pretragu i prenošenje pohranjenih podataka i dokumenata.[85]

4.6. Sjedinjene Američke Države

U Sjedinjenim Američkim Državama daljinski upravljanim forenzičnim računalnim programima navodno se koriste već od kraja 90-ih godina prošlog stoljeća Savezni istražni ured (Federal Bureau of Investigation, dalje: FBI),

[81] Završni izvještaj austrijske Interministarske radne grupe, op. cit., bilj. 65, str. 87.

[82] Zakon je objavljen u službenom glasilu *Monitorul Oficial*, br. 1089 od 23. studenoga 2004.

[83] *Sieber*, op. cit., bilj. 2, str. 22.

[84] Ibid.

[85] Ibid.

zatim obavještajne službe te neka drugih državna tijela. Poznati programi kojima se FBI koristio jesu Carnivore, Magic Lantern i CIPAV.[86]

Posebne mjere nadzora i prisluškivanja za potrebe kaznenog postupka regulirane su posebnim zakonom. Omnibus Crime Control and Safe Streets Act donesen je 1968. godine (Title III, 18 U.S.C. §§ 2510.-2520.). Navedeni propisi uređuju općenito presretanje komunikacija, dakle federalno pravo u SAD-u ne sadržava posebne propise koji bi pravno regulirali prikrivenu uporabu forenzičnih računalnih programa radi prikupljanja dokaza za potrebe kaznenog postupka.[87]

Praksa sudova u SAD-u u pogledu pravne dopustivosti korištenja forenzičnim računalnim programima vrlo je oskudna. Prva takva presuda bila je *United States v. Scarfo*. Sud je u navedenoj presudi zauzeo stajalište da korištenjem forenzičnim računalnim programom (bila je riječ o *keyloggeru*), koji je instaliran na računalo na temelju sudskog naloga, nije povrijeđeno pravo na zaštitu od neopravdanih pretraga zajamčeno Četvrtim amandmanom na Ustav SAD-a. Pored navedene, značajna je i presuda *United States v. Council-*

[86] Prvi takav računalni program koji se koristio u forenzične svrhe bio je Carnivore. Riječ je o programu koji je pratio samo komunikciju elektroničkom poštom. Carnivore navodno nije mogao biti instaliran preko interneta, već je bio nužan fizički ulaz u stan, za što je nužan sudski nalog.

Poboljšana verzija tog računalnog programa koja se navodno koristi od kraja 90-ih godina 20. stoljeća naziva se Magic Lantern. Riječ je o *keyloggeru*, dakle računalnom programu koji prati i bilježi sve unose vanjskim jedinicama (u pravilu tipkovnicom), što omogućuje rekonstrukciju raznih lozinki kojima se služi korisnik računala, ali i tekstova koje korisnik piše. Nije poznato ima li taj program mogućnost pretraživanja sadržaja tvrdog diska računala i prenošenja podataka koji su snimljeni na tom mediju (tj. onih oblika podataka koji nisu u računalo uneseni tipkovnicom odnosno onih podataka koji su uneseni vanjskim jedinicima u računalo prije instaliranja tog računalnog programa), no može se pretpostaviti da program sadržava i tu mogućnost. *So, Amanda, Woo, Christopher,* The Case for Magic Lantern: September 11 Highlights the Need for Increased surveillance, Harvard Journal of Law and Technology, Vol. 15, str. 523-525.

Najnoviji poznati forenzični računalni program koji je FBI razvio jest CIPAV (Computer and Internet Protocol Address Verifier). Riječ je o forenzičnom računalnom programu koji pruža informacije vezane uz lokaciju (IP - Internet protocol - adresu i MAC - Media Access Control – adresu), i rad na računalu: (operacijski sustav računala, trenutno aktivni programi, informacije o web-pregledniku koji se koristi i za praćenje pregleda internetskih stranica, tj. bilježenje posjećenih URL adresa). CIPAV je postao poznat javnosti sredinom 2007. godine, kad su dokazi prikupljeni negovim korištenjem upotrijebljeni na sudu tijekom postupka protiv srednjoškolca koji je elektroničkom poštom prijetio postavljanjem bombe u svojoj školi. http://www.wired.com/threatlevel/2007/07/fbi-spyware-how/ (zadnji posjet 26. svibnja 2009.).

Središnja obavještajna agencija (CIA) razvila je program Oasis namjena kojeg je preoblikovanje snimljenih razgovora vođenih VoIP tehnologijom u tekst. Zanimljivo je da Oasis, prema nekim navodima, može razumjeti i preblikovati i hrvatski jezik. http://www.theregister.co.uk/2001/03/06/cia_patching_echelon_shortcomings/ (zadnji posjet 26. svibnja 2009.).

[87] *So, Amanda, Woo, Christopher*, op. cit., bilj. 86. str. 526-527.

man,[88] gdje je sud dopustio uporabu dokaza pribavljenih primjenom te mjere i bez naloga, opravdavajući to činjenicom da je forenzični računalni program podatke dobio iz međuspremnika podataka u računalu, što nije zaštićeno propisima o prisluškivanju sadržanim u odredbama U.S.C § 2511 (1) (a) (tzv. Wiretap Act) koje štite od neovlaštenog prisluškivanja i presretanja podataka.[89]

Iz navedenog se može zaključiti da dokazi prikupljeni uporabom RFS-a na temelju sudskog naloga mogu biti dokaz u kaznenom postupku u federalnom pravu SAD-a.

5. MOGUĆNOST KORIŠTENJA DALJINSKI UPRAVLJANIM FORENZIČNIM RAČUNALNIM PROGRAMIMA U REPUBLICI HRVATSKOJ PREMA ZAKONU O KAZNENOM POSTUPKU IZ 1997. GODINE I ZAKONU O KAZNENOM POSTUPKU IZ 2008. GODINE

5.1. Korištenje daljinski upravljanim forenzičnim računalnim programima u Republici Hrvatskoj prema Zakonu o kaznenom postupku iz 1997. godine

Zakon o kaznenom postupku iz 1997. godine ne sadržava posebne propise koji bi uređivali pitanje online-pretrage. Stoga je potrebno najprije razmotriti postoji li prema ZKP/97 pravna mogućnost provođenja takve mjere na temelju nekih odredbi koje reguliraju neke druge mjere i radnje. Pritom valja razlikovati različite varijante online-pretrage prema kriteriju objekta pretrage odnosno nadzora.

5.1.1. Nadzor komunikacija

Utvrđivanje uspostavljanja komunikacijske veze (bez utvrđivanja sadržaja komunikacije) opća je izvidna radnja koju policija može samostalno provesti,

[88] United States v. Councilman, 373 F.3d 197 (1st Cir. 2004).

[89] Što se tiče pravnog temelja koji sadržava ovlasti obavještajnih službi na prisluškivanje i druge mjere, 1978. godine Kongres je donio Foreign Intelligence Surveillance Act (dalje: FISA), kojim su postavljene određene granice ovlastima obavještajnih službi u njihovu djelovanju izvan granica države. Tim je zakonom ustanovljen poseban sud, Foreign Intelligence Surveillance Court (dalje: FISC). Načelno, Vlada treba pribaviti nalog koji izdaje FISC prije prisluškivanja i nadziranja u obavještajne svrhe izvan granica države, no od obveze pribavljanja naloga postoje brojne iznimke. FISA § 103, 50 U.S.C. § 1803. *So, Amanda, Woo*, *Christopher*, op. cit., bilj. 86, str. 526-527.

bez naloga suda. Čl. 177. st. 2. ZKP određuje da "redarstvene vlasti mogu ... od pravne osobe koja pruža telekomunikacijske usluge zatražiti provjeru istovjetnosti telekomunikacijskih adresa koje su u određenom razdoblju uspostavile vezu." To vrijedi i za komunikaciju elektroničkom poštom odnosno za telefonske razgovore preko interneta. Dakle, policija može kao opću izvidnu mjeru od pravne osobe koja pruža telekomunikacijske usluge zatražiti provjeru istovjetnosti e-mail adresa koje su u određenom razdoblju uspostavile vezu ili korisničkih računa koji su ostvarili telefonski razgovor putem interneta. No, i to se može učiniti samo ako je poznata e-mail adresa (ili korisnički račun određenog davatelja pristupa internetskoj telefoniji, npr. Skype) kojom se osumnjičenik koristi, odnosno ako je s davateljem usluga elektroničke pošte moguće uspostaviti suradnju. Budući da pravna osnova postoji, postavlja se pitanje znači li to da policija kao način provedbe opće izvidne radnje utvrđivanja istovjetnosti telekomunikacijskih adresa koje su u određenom razdoblju uspostavile vezu može (isključivo radi utvrđivanja postojanja, učestalosti i vremena komunikacije elektroničkom poštom) instalirati RFS na računalo osumnjičenika.

Smatram da bi odgovor na to pitanje o dopustivosti instalacije RFS-a na računalo osumnjičenika radi provedbe opće izvidne mjere iz čl. 177. st. 2. ZKP prema važećem hrvatskom kaznenom procesnom pravu trebao biti negativan. Prije svega, ZKP/97 dopušta od telekomunikacijske tvrtke zatražiti provjeru istovjetnosti telekomunikacijskih adresa koje su u određenom razdoblju uspostavile vezu, a ne samostalno računalnim programima dolaziti do tih podataka. Daljnji problem je što gotovo svi forenzični računalni programi imaju i mogućnost nadzora sadržaja komunikacije elektroničkom poštom.[90] Najvažnije, držim da bi svaka eventualna uporaba RFS-a trebala biti vezana za sudski nadzor, budući da, zbog prije navedenih razloga, svaka primjena takvih programa znači velik poseg u prava osobe prema kojoj se primjenjuje.

Nadzor e-mail komunikacije i VoIP komunikacije (internetske telefonije) može se podvesti pod posebnu izvidnu mjeru nadzora i tehničkog snimanja telefonskih razgovora odnosno sredstava za tehničko komuniciranje na daljinu iz čl. 180. ZKP/97.[91] Stoga se postavlja pitanje je li *de lege lata* dopušteno kao način provedbe posebne izvidne mjere iz čl. 180. st. 1. t. 1. ZKP/97 instali-

[90] Stoga bi se kod eventualnog korištenja RFS-a za tu svrhu trebalo koristiti samo onim programima kojih je jedina tehnička mogućnost utvrditi uspostavu komunikacijskih veza, ali ne i njihov sadržaj.

[91] Na ovom mjestu vrijedi istaknuti da je njemački Savezni ustavni sud u presudi *Bargatzky* zauzeo stajalište da elektronička pošta pohranjena na osobnom računalu ne predstavlja "telekomunikaciju" te stoga ne podliježe nadzoru na temelju posebne izvidne mjere nadzora telekomunikacija. Presuda je objavljena u časopisu MultiMedia und Recht, 2006., str. 117. Cit. prema: *Tinnefeld*, op. cit., bilj. 34, str. 137.

rati na računalo osumnjičenika RFS te preko njega čitati sadržaj elektroničke pošte ili nadzirati komunikaciju vođenu preko interneta. Metoda kojom se uobičajeno nadzire sadržaj e-mail komunikacije jest obraćanje davateljima usluga elektroničke pošte.

U ovoj situaciji potreba primjene ove posebne izvidne mjere je veća (načelo supsidijarnosti), a sudski nalog kao uvjet primjene mjere pridonosi jamstvu potrebe primjene mjere te pravilnosti njezine provedbe u odnosu prema općim izvidima iz čl. 177. ZKP/97. Kod tog pravnog problema, kao i kod nekih drugih instituta, dolazi do sraza između težnje za učinkovitošću postupka, izražene u namjeri primjene ove potencijalno iznimno korisne mjere prikupljanja dokaza (osobito kad se počinitelji koriste programima za vođenje šifriranih telefonskih razgovora preko interneta, što je problem za koji se smatra da je ostalim metodama nadzora internetske telefonije nerješiv) te težnje za zaštitom prava građana budući da RFS, jednom kad je instaliran na računalo, predstavlja ogroman zahvat u prava te osobe, bez dovoljnih tehničkih jamstava provedbe mjere.[92]

Držim da infiltraciju RFS-a radi nadzora internetske telefonije ne bi trebalo načelno isključiti, no pritom bi se smjelo koristiti samo onim forenzičnim računalnim programima koji imaju samo mogućnost nadzora telekomunikacija, a ne i pretrage sadržaja, ako je moguće načiniti takav program. Dakle, valjalo bi voditi računa da se nadzor komunikacija ne ostvaruje RFS-om na način (npr. *keyloggerom*) koji bi predstavljao tajnu pretragu i kojim bi se neosnovano i prekomjerno narušila ustavna prava građana. *De lege ferenda*, da bi se pristupilo korištenju RFS-om radi nadzora komunikacije preko interneta, primjenu takve mjere s tom svrhom trebalo bi dopustiti samo uz veća postupovna jamstva i precizniju zakonsku razradbu provedbe mjere (kao posebne mjere, a ne kao načina provedbe mjere iz čl. 180. st. 1. t. 1. ZKP/97), o čemu će biti riječi dalje pri razmatranju odredbe čl. 332. st. 1. t. 2. Zakona o kaznenom postupku iz 2008. godine.

[92] VoIP (Voice over Internet Protocol) komunikacija (tj. internetska telefonija) može se podijeliti u četiri temeljne grupe: a) računalo – računalo, b) računalo – telefon, c) telefon – računalo te d) IP (Internet protokol) telefon – IP telefon. IP telefoni spajaju se izravno na usmjerivač (router), ali im se može dodijeliti običan (geografski) telefonski broj ili VoIP broj. Navedene četiri vrste VoIP komunikacije su značajne jer su tehničke pretpostavke za provođenje nadzora i snimanje razgovora različite, što čini teškoće tijelima zaduženim za provedbu tih mjera. Npr. jedan od većih problema je taj što računalo, kad se spaja preko routera na ISP (Internet Service Provider) u pravilu svaki put dobije drugu IP adresu, što uvelike otežava identificiranje. Više o tome, osobito o problemima nadzora enkriptirane VoIP komunikacije (kojom se sve više služe pripadnici zločinačkih organizacija) v. *Singleton, Timothy,* Big Brother Hears You, But Can He Understand What He Hears? The Problematic Application of CALEA to VoIP Communications in the Age of Encryption, Tulsa Journal of Comparative & International Law, Vol. 15:2. (2007.-2008.), str. 283-322.

5.1.2. Pretraga i prijenos pohranjenih podataka

Što se tiče pretrage tvrdog diska računala, smatram da prema pozitivnim propisima hrvatskog kaznenog procesnog prava ne postoji pravni temelj za njezino provođenje tajnim posegom u računalni sustav korištenjem RFS-om.

U hrvatskom kaznenom procesnom pravu pretraga je procesna radnja regulirana u čl. 211.-217. ZKP/97. U čl. 211.b. ZKP određeno je da pretraga pokretnih stvari obuhvaća *i pretragu elektroničkog računala i sličnih uređaja za automatsku obradu podataka koji su s elektroničkim računalom povezani*.[93] Dakle, prema pozitivnom hrvatskom kaznenom procesnom pravu, pretragu sadržaja tvrdog diska računala (ili drugih medija za pohranu podataka, npr. USB memorija, CD, DVD, prijenosnog USB diska, disketa i dr.) osobe osumnjičene ili okrivljene za neko kazneno djelo moguće je steći isključivo istražnom radnjom pretrage, u ovom slučaju pretrage pokretne stvari, što uključuje i elektroničko računalo. Predmeti upotrijebljeni kod pretrage elektroničkog računala i sličnih uređaja za automatsku obradu podataka vratit će se nakon pretrage njihovim korisnicima, ako nisu potrebni za daljnje vođenje kaznenog postupka. Osobni podaci pribavljeni pretragom mogu se koristiti samo u svrhe kaznenog postupka i izbrisat će se bez odgode kad ta svrha prestane.[94]

ZKP predviđa prilikom pretrage stana ili drugog prostora obveznu nazočnost dvojice tzv. sudskih ili solemnitetnih svjedoka istodobno kroz cijelo vrijeme trajanja pretrage.[95] No Zakon ne predviđa nekakvo slično jamstvo kod pretrage pokretne stvari odnosno pretrage računala. Za pravilno provođenje "klasične" pretrage tvrdog diska računala potrebno je odmah napraviti kopiju tvrdog diska računala ili drugog medija koji se istražuje. Original se potom zapečaćuje; svrha izrade kopije (koja se potom pretražuje) i pečaćenja originala jest jamstvo pravilnosti provedbe radnje te jamstvo da na disk koji se pretražuje ništa nije naknadno stavljeno.[96] Zaključno se može ustvrditi da je

[93] Na zahtjev suda, osoba koja se koristi računalom dužna je omogućiti pristup računalu ili medijima na kojima su pohranjeni podaci koji se odnose na predmet pretrage (diskete, vrpce i sl.) te pružiti potrebne obavijesti za uporabu računala.

[94] Čl. 215. st. 2. ZKP/97.

[95] Članak 214. ZKP. Pretrazi stana ili drugog prostora moraju biti nazočna dva punoljetna građanina kao svjedoci istodobno kroz cijelo vrijeme trajanja pretrage. Svjedoci će se prije početka pretrage upozoriti da paze kako se pretraga obavlja te da imaju pravo prije potpisivanja zapisnika o pretrazi staviti svoje prigovore ako smatraju da pretraga nije provedena na zakonit način ili da sadržaj zapisnika nije točan. O svakoj pretrazi stana ili osobe sastavit će se zapisnik, koji potpisuju osoba kod koje se obavlja pretraga ili osoba koju se pretražuje i osobe čija je nazočnost obvezna. Pri pretrazi oduzet će se privremeno samo oni predmeti i isprave koji su u vezi sa svrhom pretrage u pojedinom slučaju osim predmeta naznačenih u članku 218. stavku 3. i 4. ZKP. U zapisnik će se unijeti i točno naznačiti predmeti i isprave koji se oduzimaju, a to će se unijeti i u potvrdu koja će se odmah izdati osobi kojoj su predmeti, odnosno isprave oduzete.

[96] *Hansen, Pfitzmann, Roßnagel,* op. cit., bilj. 6, str. 225.

prema postojećim propisima ZKP/97 utvrđivanje sadržaja pohranjenih na tvrdom disku računala osumnjičenika/okrivljenika moguće samo kao "klasična" istražna radnja: fizičkim pristupom računalu te utvrđivanjem sadržaja tvrdog diska računala. Zbog tajnosti provođenja online-pretrage korištenjem RFS-a njezina primjena *de lege lata* nije dopuštena.

5.1.3. Audio i videonadziranje

Uporaba RFS-a zbog uključivanja mikrofona ili kamere računala rezultira mogućnošću audio i videonadzora.

Posebna izvidna mjera navedena u čl. 180. st. 1. t. 2. ZKP jest ulazak u prostorije radi provođenja nadzora i tehničko snimanje prostorija. Moglo bi se postaviti pitanje može li način tehničke provedbe mjere tehničkog snimanja prostorija biti ubacivanje RFS-a u računalo osumnjičenika. Iako se može očekivati da bi iz objektivnih razloga učinkovitost promjene te mjere bila manja nego kod ulaska u prostorije i postavljanja posebnih uređaja za nadzor na prikladna mjesta te da ne bi trebalo očekivati čestu primjenu te mjere, potrebno je razjasniti i ovo pitanje. Držim da kao odgovor na nj vrijedi sve što je navedeno u vezi s provedbom mjere iz čl. 180. st. 1. t. 1. ZKP/97.

5.2. Korištenje daljinski upravljanim forenzičnim računalnim programima u Republici Hrvatskoj prema Zakonu o kaznenom postupku iz 2008. godine

Zakon o kaznenom postupku iz 2008. godine (dalje: ZKP/08) uvodi jednu novu posebnu izvidnu, odnosno sada posebnu dokaznu radnju: *presretanje, prikupljanje i snimanje računalnih podataka* (čl. 332. st. 1. t. 2 ZKP/08).[97] Je li ta odredba pravni temelj za uporabu daljinski upravljanih forenzičnih računalnih programa radi nadziranja komuniciranja preko interneta te pretrage i prijenosa podataka pohranjenih na računalu?

Navedena odredba ne sadržava informacije o načinu, ili mogućim načinima, presretanja, prikupljanja i snimanja računalnih podataka. Logičkim tumačenjem nameće se zaključak da bi jedna od metoda primjene te mjere mogla biti i infiltracija daljinski upravljanog forenzičnog računalnog programa u računalo osumnjičenika. Ako bi se prihvatilo stajalište da navedena formulacija omogućuje primjenu daljinski upravljanih forenzičnih računalnih programa radi nadziranja komuniciranja preko interneta te pretrage i prijenosa

[97] Prema čl. 89. st. 32. Kaznenog zakona, računalni podatak je svako iskazivanje činjenica, informacija ili zamisli u obliku prikladnom za obradu u računalnom sustavu.

podataka pohranjenih na računalu kao posebne dokazne radnje, takvo zakonsko rješenje nije prihvatljivo.

U dijelu rada o tehničkim mogućnostima primjene mjere objašnjeno je da je jedan od glavnih prigovora koji se upućuju ovoj mjeri prikupljanja podataka nemogućnost jamčenja vjerodostojnosti prikupljenih podataka, odnosno praktična nemogućnost postavljanja određenih jamstava sigurnosti ispravnosti provedbe ove mjere. Nadalje, pored nepostojanja jamstva vjerodostojnosti prikupljenih podataka kod pretrage i prijenosa podataka pohranjenih na računalu, veličina posega u temeljna ljudska prava, osobito prava na privatnost, čak i premašuje poseg koji predstavljaju ostale posebne dokazne mjere. Stoga prilikom eventualnog propisivanja te mjere valja biti još oprezniji nego kod ostalih posebnih izvidnih mjera, što se vidi i na primjeru SR Njemačke gdje iz navedenih razloga ni nakon burne trogodišnje rasprave još uvijek nije dopuštena primjena te mjere radi prikupljanja dokaza za potrebe kaznenog postupka.

Odredbe ZKP/08, koje o provođenju te mjere ne navode ništa osim njezina naziva, podnormirane su i stoga nedovoljno jamstvo za njezinu ispravnu primjenu. Zakonodavac koji bi se ipak odlučio za primjenu te mjere za potrebe kaznenog postupka mora biti svjestan njezinih potencijala, ali i manjkavosti, razlika u području prikupljanja podataka i mogućnostima forenzičnih računalnih programa koji se koriste. Jednako važno, potrebno je precizno pravno odrediti pojedine forenzične računalne programe kako bi se izbjegle moguće zlouporabe i neovlašteno prikupljanje osobnih podataka. Pored navedenog, nužno je precizno pravno uređenje cijelog postupka određivanja primjene mjere, njezine provedbe te korištenja informacijama prikupljenim njezinom primjenom po uzoru na opisane odredbe njemačkog BKAG-a.

U tom slučaju uporabu forenzičkih računalnih programa trebalo bi urediti kao posebnu dokaznu radnju, ali ne onako kako je to navedeno u hrvatskom ZKP/08. Manjkavost hrvatskog uređenja posebnih izvidnih (dokaznih) radnji, neovisno o uporabi RFS-a, jest u nedovoljnoj normiranosti te nedovoljnom razlikovanju pojedinih radnji u pogledu uvjeta za primjenu mjere te načina i trajanja provedbe mjere. Jasno je da sve posebne izvidne (dokazne) radnje ne znače jednak poseg u prava građana; stoga bi ta činjenica morala naći svoj odraz i u različitoj pravnoj uređenosti tih mjera. U nekim poredbenim pravima, primjerice, mjera tajnog audiovizualnog tehničkog snimanja doma smatra se većim posegom u ustavna prava te su za njezinu primjenu propisani stroži uvjeti. Prenesena na prikriveni poseg u računalne sustave uporabom RFS-a radi pretrage i prijenosa podataka pohranjenih na računalu kao potencijalne posebne dokazne radnje, navedena konstatacija znači da - ako bi se zakonodavac ipak, usprkos njezinim manjkavostima, odlučio za uvođenje te mjere u kazneno procesno zakonodavstvo - uvjeti njezine primjene također trebaju biti stroži od uvjeta za primjenu ostalih posebnih dokaznih radnji.

Prije svega, u slučaju njezina propisivanja, navedena mjera trebala bi biti dopuštena samo u iznimnim slučajevima i samo za najteža kaznena djela, nipošto ne za sva kaznena djela iz (sve šireg) kataloga kaznenih djela iz čl. 181. ZKP/97 odnosno čl. 334. ZKP/08.

Moguće trajanje svih posebnih dokaznih radnji iz čl. 335. st. 3. ZKP/08 jest 18 mjeseci (6 + 6 + 6 mjeseci, što je znatno produljenje prema ukupno 7 mjeseci iz čl. 182. st. 2. ZKP/97). U slučaju eventualne primjene online-nadziranja, dakle praćenja rada korisnika na računalu, ti rokovi u pravilu bi trebali biti znatno kraći.

Iako bi u praksi takve situacije bile vrlo rijetke, instaliranje RFS-a na računalo oštećenika uz njegov pristanak radi nadzora komunikacije u situacijama kad se očekuje internetski telefonski poziv ili elektronička pošta od osumnjičenika odnosno nepoznatog počinitelja (npr. otmičara), nosi sa sobom mnogo manje dvojbi (čl. 332. st. 5. u vezi sa st. 1. t. 2. ZKP/08).

Primjena posebnih dokaznih radnji uvjetovana je pozitivnom odlukom suda o prihvaćanju zahtjeva državnog odvjetnika (ZKP/97 i ZKP/08). ZKP/08 uvodi mogućnost da državni odvjetnik privremeno odluči o primjeni navedenih mjera, uz uvjet naknadne sudske konvalidacije, što bi kod pravnog uređenja ove mjere valjalo izostaviti.[98]

Smatram da bi u slučaju eventualnog uvođenja online-pretrage u ZKP, zbog veličine posega u ustavna prava i slobode, razina odlučivanja o primjeni naloga trebala biti što viša. Stoga bi bilo bolje rješenje da zahtjev može postaviti glavni državni odvjetnik RH, a da o zahtjevu odlučuje sudac ili vijeće Vrhovnog suda Republike Hrvatske.[99]

U pogledu kvalitete sumnje u počinjenje kaznenog djela koja mora postojati, "obične" osnove sumnje (kao u čl. 177. ZKP/97) ne bi bile dostatne. To proiz-

[98] Čl. 332. st. 2. ZKP/08: "Iznimno, kad okolnosti nalažu da se s izvršenjem radnji započne odmah, nalog o određivanju primjene posebne dokazne radnje 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 sudac istrage odbije nalog, državni odvjetnik može u roku od osam sati podnijeti žalbu. O žalbi odlučuje vijeće u roku od dvanaest sati."

[99] Slično rješenje nalazimo u čl. 36. hrvatskog Zakona o sigurnosno-obavještajnom sustavu gdje je propisano da se mjere tajnog prikupljanja podataka iz članka 33. stavka 3. točke 1. a), točke 2., točke 3. i točke 5. tog zakona mogu poduzimati samo na temelju pisanog obrazloženog naloga za njihovo provođenje koje izdaje sudac Vrhovnog suda Republike Hrvatske. Suce ovlaštene za izdavanje pisanog naloga za provođenje mjera tajnog prikupljanja podataka određuje predsjednik Vrhovnog suda Republike Hrvatske. Pisani obrazloženi prijedlog za primjenu mjere tajnog prikupljanja podataka podnose ravnatelji sigurnosno-obavještajnih agencija. *Kudlich* također zagovara što višu razinu sudskih tijela koja bi donosila odluku o primjeni ove mjere opravdavajući to većom dubinom posega u ustavna prava nego kod većine ostalih posebnih istražnih mjera. V. *Kudlich, Hans,* op. cit., bilj. 34, str. 11.

lazi iz temeljnog ustavnog pravila prema kojem za primjenu najtežih represivnih posega u temeljna ljudska prava zajamčena Ustavom i međunarodnim pravom mora postojati veći stupanj vjerojatnosti od onoga koji je potreban za početak općih izvida iz čl. 177. ZKP/97.[100] Stoga bi za određivanje primjene forenzičnih računalnih programa bio potreban veći stupanj vjerojatnosti o počinjenju kaznenog djela: takva razina sumnje koja bi u praksi mogla biti izjednačena sa stupnjem vjerojatnosti potrebnim za određivanje mjera za osiguranje okrivljenikove nazočnosti.[101]

6. ZAKLJUČAK

Korištenje daljinski upravljanim forenzičnim računalnim programima od državnih tijela radi prikupljanja informacija potencijalno je vrlo učinkovita mjera, no s druge strane riječ je o mjeri koja možda čak i više od drugih posebnih istražnih mjera zadire u ustavna prava i slobode.[102]

Područja za koja se smatra da bi u njima ova mjera mogla naći svoju primjenu jesu prikupljanje dokaza za potrebe kaznenog postupka u slučaju počinjenja najtežih kaznenih djela, policijska preventivna djelatnost te djelatnost obavještajnih službi radi zaštite ustavnog ustrojstva države.[103]

---

[100] *Krapac, Davor,* Zakon o kaznenom postupku i drugi izvori hrvatskog kaznenog postupovnog prava, Narodne novine, Zagreb, 2006., str. 180.

[101] Ibid.

[102] Problem odnosa sigurnosti i slobode u suvremenim demokratskim društvima vrlo je osjetljivo pitanje. *Di Fabio* ističe da u slučaju pojave određene (barem naizgled stvarne i ozbiljne) prijetnje mnogim ljudima sigurnost izgleda važnija od slobode. Ali dublji uvid pokazuje da se ne radi o nužnoj dominaciji jedne vrijednosti nad drugom, odnosno situaciji da jačanjem jedne od njih druga automatski slabi. Naprotiv, ističe autor, radi se o simetriji jer su obje vrijednosti jednako važne te vrijedi i da bez slobode nema sigurnosti. Sloboda i sigurnost nisu antipodi, nisu nepomirljive proturječnosti, u svojoj biti nimalo nisu proturječne. One stoje u komplementarnom odnosu, međusobno se uvjetuju i jačaju jedna drugu, ako se obje primjereno razvijaju. *Di Fabio, Udo*, Sicherheit in Freiheit, Neue Juristische Wochenschrift, 2008., str. 422. *Kutscha* ističe da bi uvođenjem tajne online-pretrage u kazneno procesno ili policijsko pravo ili pravo obavještajnih službi (navodna) potreba za sigurnošću još jednom pobijedila slobodu. Iako je nedvojbeno istina da nema slobode bez sigurnosti, autor upozorava da vrijedi i obratno. Nije slobodan onaj tko mora računati s tim da će ga u njegovim privatnim stvarima tajno nadzirati država. *Kutscha, Martin,* Verdeckte "Online-Durchsuchung" und Unverletzlichkeit der Wohnung, Neue Juristische Wochenschrift, 2007., str. 1172. Usp. i: *Tinnefeld*, op. cit., bilj. 47, str. 139.

[103] Zakon o sigurnosno-obavještajnom sustavu (Narodne novine br. 79/06 i 105/06), čl. 1. st. 1., definira posljednje navedenu djelatnost kao "prikupljanje podataka koji su od značaja za nacionalnu sigurnost, u cilju otkrivanja i sprječavanja radnji pojedinaca ili skupina koje su usmjerene: protiv opstojnosti, neovisnosti, jedinstvenosti i suvereniteta Republike Hrvatske, nasilnom rušenju ustroja državne vlasti, ugrožavanju Ustavom Republike Hrvatske i zakoni-

Pomoću te mjere ponekad je moguće prikupljanje informacija koje na neki drugi način zasigurno ne bi mogle biti prikupljene. Budući da se sve više podataka pohranjuje i prenosi elektroničkim putem, nisu rijetke tvrdnje da je možda riječ o istražnom instrumentu budućnosti.[104] U nekim slučajevima to može biti jedino sredstvo kojim se mogu otkriti počinitelji nekih teških kaznenih djela i prikupiti dokazi za njihovu osudu. Doista, otkrivačka djelatnost policije i državnog odvjetništva koja ne prati napredak tehnologije odnosno kojoj zakonodavnim putem nije omogućena uporaba novih tehnologija kojima se služe i počinitelji kaznenih djela teško može biti uspješna. S druge strane, njezina primjena, osobito ako bi se radilo o velikom broju slučajeva i uz nedostatan nadzor ispunjenosti uvjeta za njezinu primjenu i ispravnosti njezine provedbe, može predstavljati neprihvatljivo ograničenje prava i sloboda građana od strane države i prekomjerno jačanje njezinih ovlasti nadzora.[105]

Kod pravnog reguliranja korištenja navedenim forenzičnim računalnim programima nužno je voditi računa o različitim područjima primjene i mogućnostima navedenih računalnih programa radi nadzora komuniciranja preko interneta, jednokratne pretrage sadržaja pohranjenih na računalu ili nadziranja aktivnosti na računalu koje traju određeno vrijeme.

Prilikom razmatranja o eventualnom određivanju primjene te mjere za potrebe kaznenog postupka, pored njezine potencijalne velike učinkovitosti i korisnosti za društvo u borbi protiv najtežih oblika kriminala, valja imati na umu i njezine manjkavosti. Pored veličine posega u temeljna ljudska prava, glavni je problem problematično jamčenje vjerodostojnosti prikupljenih podataka. To je na određeni način i "prethodno pitanje" kad se razmatra primjena te

ma utvrđenih ljudskih prava i temeljnih sloboda te osnova gospodarskog sustava Republike Hrvatske"

[104] *Kutscha,* op. cit., bilj. 102, str. 1169.

[105] Opća je karakteristika posljednjeg (posljednjih) desetljeća, a to je slučaj i s online-pretragom, da se pojmovima kao terorizam i organizirani kriminal često koristi u namjeri uvođenja širokih ovlasti državnih tijela na prikupljanje informacija. Jednom uvedene, te ovlasti pokazuju tendenciju širenja. *Ashworth, Andrew,* Human Rights, Serious Crime and Criminal Procedure, Sweet & Maxwell, London, 2002., str. 105. *Ashworth* pritom upozorava na važnost definicija sadržanih u materijalnom pravu. Upozorava na emocionalnu obojenost takvih etiketa poput terorizma ili organiziranog kriminala te ističe da se upravo time pridobiva potpora za određene ideje. Razlog je jednostavan: ima vrlo malo ljudi koji su spremni prigovoriti nekim ovlastima koje se uvode kao sredstvo borbe protiv npr. terorizma i time se izložiti opasnosti da ih se etiketira kao protivnike "borbe protiv terorizma". Upozorava i na značajno širenje pojma terorizma u engleskom materijalnom pravu u Zakonu o terorizmu iz 2000. godine; terorizam prema tom zakonu nije više ograničen samo na uporabu nasilja i izazivanje straha među stanovništvom; proširena definicija uključuje ozbiljnu štetu imovini, ozbiljan rizik za zdravlje ili sigurnost javnosti i ozbiljne prekide elektroničkih sustava. Ibid., str. 107. *Ashworth* ističe da bi širenje definicija ključnih pravnih koncepata bilo manje zabrinjavajuće kad bi širenje postojećih ili uvođenje novih ovlasti državnih tijela kaznenog progona bilo praćeno posebnim postupovnim jamstvima osumnjičenika i okrivljenika, kao što je to u Norveškoj i Švedskoj. Ibid., str. 108.

mjere. Prema standardima digitalne forenzike, navedena mogućnost izmjene podataka je problematična. Stoga neki autori ističu da bi bilo prikladnije da se saznanjima prikupljenima prikrivenim posegom forenzičnim računalnim programima u računalne sustave koristi kao dokazima u spoznajnom smislu koji bi služili usmjerivanju daljnjeg istraživanja.[106]

Ova mjera, koju možemo smatrati jednom od najznačajnijih novina u pogledu tehnika i metoda prikupljanja informacija od državnih tijela u posljednjih nekoliko desetljeća, predstavlja značajno ograničenje ustavnog prava na poštovanje osobnog i obiteljskog života (čl. 35. Ustava Republike Hrvatske), prava na slobodu i tajnost dopisivanja i drugih oblika općenja (čl. 36. Ustava RH) te prava na sigurnost i tajnost osobnih podataka (čl. 37. Ustava RH).[107]

Europski sud za ljudska prava sažeo je načelo zakonitosti u pogledu nadzora komunikacija na sljedeći način: "Ako se ovlasti izvršne vlasti izvršavaju tajno, rizik arbitrarnosti je očigledan. U kontekstu tajnih mjera nadzora ili presretanja od strane državnih tijela, zahtjev predvidivosti implicira da domaće pravo mora ispuniti zahtjev određenosti u dovoljnoj mjeri."[108] Navedena konstatacija to više vrijedi i za ostale informacije (pored komunikacija) koje se mogu prikupiti provođenjem ove mjere, osobito za dugotrajniji nadzor aktivnosti rada na računalu.

Nakon rješavanja problema vjerodostojnosti prikupljenih podataka, eventualnu primjenu ove mjere treba iscrpno pravno urediti, vezati uz stroge i sasvim određene uvjete primjene te samo za najteža kaznena djela kod kojih već postoji određeni značajni stupanj sumnje u počinjenje tih kaznenih djela.[109] Sudski nalog kao uvjet za primjenu ove mjere je nužan, a nadležnost za izdavanje naloga može se, zbog značenja te mjere, staviti u nadležnost Vrhovnog suda.[110] Kod primjene ove mjere prisutan je i problem ograničavanja saznanja samo na one sadržaje zbog kojih je mjera određena. Sve ostale podatke koji budu eventualno zabilježeni primjenom ove mjere (npr. sadržaj tvrdog diska na računalu, ako je mjera određena samo u pogledu nadzora komunikacija) valja smatrati nezakonitim dokazima te je nužno njihovo izdvajanje i brisanje.[111] Potrebno je normirati naknadno obavještavanje osobe prema kojoj se

[106] *Sieber*, op. cit., bilj. 3, str. 17-18.

[107] Argument "Tko ništa ne krije, nema se razloga bojati" ne može se prihvatiti u državama u kojima postoji vladavina prava, ili koje barem teže tom cilju.

[108] *Valenzuela Contreras v. Spain*, presuda od 30. srpnja 1998. (58/1997/842/1048). *Trechsel, Stefan,* Human Rights in Criminal proceedings, Oxford University Press, 2005., str. 549.

[109] *Sieber,* op. cit., bilj. 3, str. 19.20.

[110] Prikladno rješenje bila bi zbornost u odlučivanju, primjerice nadležnost tročlanog izvanraspravnog vijeća. Ibid., str. 20.

[111] Uporaba daljinski upravljanih forenzičnih računalnih programa radi prikupljanja dokaza za potrebe kaznenog postupka pokazuje još jednu vrlo zanimljivu tendenciju. Iako je ot-

mjera primjenjivala o njezinoj provedbi, a ako bi bila predviđena mogućnost da se iz istražno-taktičkih razloga to ne učini, potrebno je osigurati neki drugi oblik kontrole provedbe mjere.[112]

U ovom radu prikazana su samo neka obilježja forenzičnih računalnih programa te prednosti i nedostaci njihove primjene. Opisana osnovna obilježja tih programa upućuju na to da je njihovu primjenu za prikupljanje dokaza u kaznenom postupku, zbog njegova velikog značenja, potrebno iscrpno proučiti. To vrijedi kako za pravni tako i za informatički aspekt primjene, budući da je poznavanje tehničkih osobitosti i mogućnosti tih programa preduvjet za prikladno pravno reguliranje ove materije.

LITERATURA

1. *Abel, Wiebke,* Agents, Trojans and tags: the next generation of investigators, 23:1-2 International Review of Law, Computers & Technology, str. 98-108.
2. *Ashworth, Andrew,* Human Rights, Serious Crime and Criminal Procedure, Sweet & Maxwell, London, 2002., str. 105.
3. *Di Fabio, Udo,* Sicherheit in Freiheit, Neue Juristische Wochenschrift, 2008., str. 421-425.
4. *Hansen, Markus; Pfitzmann, Andreas; Roßnagel, Alexander*, Online-Durchsuchung, Deutsche Richterzeitung, 2007., str. 225.
5. *Hofmann. Manfred,* Die Online-Durchsuchung - staatliches "Hacken" oder zulässige Ermittlungsmaßnahme? Neue Zeitschrift für Strafrecht, 2005., str. 121-125.
6. *Huber, Bertold,* Trojaner mit Schlapphut - Heimliche "Online-Durchsuchung" nach dem Nordrhein-Westfälischen Verfassungsschutzgesetz, Neue Zeitschrift für Verwaltungsrecht, 2007., str. 880-884.
7. *Krapac, Davor*, Zakon o kaznenom postupku i drugi izvori hrvatskog kaznenog postupovnog prava, Narodne novine, Zagreb, 2006.
8. *Kutscha, Martin,* Mehr Schutz von Computerdaten durch ein neues Grundrecht?, Neue Juristische Wochenschrift, 2008., Heft 15, str. 1042-1045.
9. *Kutscha, Martin,* Verdeckte "Online-Durchsuchung" und Unverletzlichkeit der Wohnung, Neue Juristische Wochenschrift 2007., str. 1169-1172.

krivačka djelatnost u prethodnom kaznenom postupku i dosad u praksi bila gotovo isključivo zadaća policije, a ne državnog odvjetništva, uvođenje takvih sofisticiranih mjera prikupljanja informacija i dokaza još više pomiče težište moći s državnog odvjetništva na policiju. Razlog tome je jednostavan: zbog nedostatnog informatičkog znanja državni odvjetnik, kao laik u informatičkom smislu, nije kadar adekvatno upravljati provođenjem te mjere te je faktično na određeni način u podređenom položaju u odnosu prema policijskom službeniku informatičke struke koji provodi tu mjeru.

[112] Npr. posebnim ombudsmanom, kao što je to u nekim poredbenim zakonodavstvima. Ibid. *Sieber* pored navedenog predlaže još restrikciju ovlasti drugih tijela na određivanje primjene te mjere, koje za većinu drugih posebnih izvidnih radnji postoje u slučaju opasnosti od odgode. Nadalje, interna obveza obrazlaganja i izvještavanja osoba odgovornih za provedbu mjere u okviru tijela u kojem rade, donošenje preciznih propisa o protokoliranju i dokumentaciji provođenja mjere. Ibid.

10. *Roggan, Fredrik,* Das neue Bka-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur, Neue Juristische Wochenschrift, 2009., Heft 5, str. 257-262.
11. Sieber, Ulrich, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen, verzija 1.0 od 9. listopada 2007., dostupno na: http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf
12. *Singleton, Timothy,* Big Brother Hears You, But Can He Understand What He Hears? The Problematic Application of CALEA to VoIP Communications in the Age of Encryption, Tulsa Journal of Comparative & International Law, Vol. 15:2 (2007.-2008.), str. 283-322.
13. *So, Amanda, Woo, Christopher,* The Case for Magic Lantern: September 11 Highlights the Need for Increased surveillance, Harvard Journal of Law and Technology, Vol. 15, str. 521-538.
14. *Tinnefeld, Marie-Theres,* Online-Durchsuchung - Menschenrechte vs. virtuelle Trojaner, MultiMedia und Recht, 2007., Heft 3, str. 137-139.
15. *Trechsel, Stefan*, Human Rights in Criminal proceedings, Oxford University Press, 2005.
16. *Uerpmann-Wittzack,Jankowska-Gilberg*: Die Europäische Menschenrechtskonvention als Ordnungsrahmen für das Internet, MultiMedia und Recht, 2008., str. 83-89.
17. Završni izvještaj austrijske interministarske radne grupe (Erweiterung des Ermittlungsinstrumentariums zur Bekämpfung schwerer, organisierter und terroristischer Kriminalitätsformen ("Online-Durchsuchung"), Interministerielle Arbeitsgruppe "Online-Durchsuchung", BMJ/BMI) dostupno na: http://www.justiz.gv.at/_cms_upload/_docs/AG_Online-Durchsuchung_Endbericht.pdf

Summary

USE OF FORENSIC COMPUTER PROGRAMS TO COLLECT EVIDENCE IN THE CRIMINAL PROCEDURE

Following the development of technology, state bodies that participate in the detection of criminal offences and of their perpetrators, and in collecting evidence for the criminal procedure, are considering the use of special computer programs through which they secretly access the computer system of the person suspected of having committed a serious criminal offence. The application of remote forensic computer programs allows, on the one hand, efficient discovery and disclosure, and the collection of evidence against perpetrators who would probably not have been detected in any other way. On the other hand, this is a measure which, perhaps more than other special investigative measures, impinges on constitutional rights and freedoms and which should, for a number of reasons, be applied with extreme caution. Therefore, the author of this paper, after an exhaustive comparative legal analysis, criticises the solutions advocated in the new Croatian Criminal Procedure Act of 18 December 2008 (OG 152/08) which should begin to be implemented on 1 November 2011. He considers that the provisions of this law are under-regulated and that they consequently provide an insufficient guarantee for the correct application of this measure. The legislator who decides to introduce this measure in the criminal procedure must be aware of its potentials, but also of its deficiencies, as well as of the differences in the area of collecting data and the opportunities offered by the forensic computer programs that are being used. It would be desirable to precisely define individual forensic computer programs in the law in order to avoid possible abuses and the unauthorised collection of personal data. Therefore, the use of forensic computer programs should be regulated as a special evidence collection procedure, taking into account that, due to its specific characteristics, it should be regulated in a different manner from other special evidence collection procedures, imposing stricter requirements concerning its application, control and duration.