Dr Tatjana Lukić

asistent Pravnog fakulteta u Novom Sadu

AUTOMATSKA KOMPJUTERSKA OBRADA PODATAKA KAO POSEBNA ISTRAŽNA RADNJA*

SAŽETAK: Primena posebnih istražnih radnji je karakteristična za proaktivne istrage u vezi sa organizovanim kriminalom. Jedna od tih posebnih istražnih radnji koja sve više dobija na značaju je i kompjuterska automatska obrada podataka koja je u Srbiji uvedena novim Zakonikom o krivičnom postupku. Predmet ovog rada su pozitivnopravna rešenja u Srbiji koja se odnose na ovu posebnu istražnu radnju. Osim toga, autor je dao i uporednopravni prikaz zakonskog regulisanja ove radnje obrađujući pravni osnov primene mere, uslove i načine njenog odobravanja, dužinu trajanja, korišćenje izvoda iz kompjutera kao dokaza u krivičnom postupku i nadzor nad zakonitim sprovođenjem radnje. Autor je posebno obradio i prikupljanje i obradu ličnih podataka na međunarodnom nivou, kao i pitanje uloge kriminalističke obaveštajne analitike u borbi protiv terorizma.

Ključne reči: posebne istražne radnje, kompjuterska obrada podataka, organizovani kriminal

Kompjuterska automatska obrada (upoređivanje) podataka građana je savremena istražna radnja kojom se vrši provera baze podataka javnih i nejavnih službi i to prema određenim kontrolnim obeležjima — karakteristikama (rasterima) u cilju pronalaženja tragova ili važnih saznanja koji bi mogli dovesti do izvršioca određenog krivičnog dela. Kod ove istražne radnje se pomoću različitih informatičkih tehnika, na brz način, mogu izdvojiti i „sravniti” različite registrovane činjenice u policijskim i ostalim bazama podataka i evidencijama: npr. visina prijavljenog poreza, *modus operandi*, prouzrokovanje ili saučesništvo u saobraćajnoj nesreći, prelazak granice, legitimisanje i dr. Rezultati ove istražne radnje mogu ubrzati

* Rad primljen: 07. VII 2006. godine.

identifikaciju izvršilaca krivičnih dela. Na taj način izdvojeno lice ulazi u krug sumnjivih lica (osumnjičenih) za izvršenje krivičnog dela, ili ga nepostojanje takvih činjenica, uz niz drugih razloga, može eliminisati kao eventualnog izvršioca krivičnog dela. Važno je napomenuti da se preduzimanje raster pretrage ne odnosi na manuelni pregled kartoteka ili datoteka.

Automatska kompjuterska obrada podataka predstavlja posebnu istražnu radnju koja se označava kao „rasterska potraga”, a njen naziv dolazi od reči raster što znači kontrolno obeležje. Pristup kompjuterskim sistemima i kompjutersko sravnjivanje podataka se odnosi na upoređivanje ličnih podataka građana koji su obrađeni u odgovarajućim bazama podataka sa podacima i registrima koji se nalaze u okviru policijskih evidencija. Saznanja o traženom licu uneta u jedan registar ličnih podataka upoređuju se sa drugim bazama podataka u kojima bi se sumnjivo lice moglo nalaziti. Tako dobijeni rezultat može dati više podataka o licu za koje se sumnja da je izvršilo krivično delo. *Pozitivna raster potraga* se koristi za utvrđivanje kruga sumnjivih lica polazeći od određenih registrovanih karakteristika. *Negativna raster potraga* isključuje iz dalje provere određeno lice koje nije sumnjivo.

U savremenim državama postoje povezani policijski, carinski, poreski, kriminalističko-obaveštajni i drugi kompjuterski informacioni sistemi i registri. U Engleskoj, na primer, postoje brojni, horizontalno i vertikalno povezani policijski, carinski, poreski i drugi kompjuterski informacioni sistemi, uključujući i centralni sistem baze kriminalističko-obaveštajnih podataka pohranjenih i obrađivanih u toku delovanja britanske Kriminalističko-obaveštajne službe (National Criminal Intelligence Service — NCIS).

Posebna istražna radnja kompjuterske obrade podataka se preduzima prema osumnjičenom licu ukoliko postoje osnovi sumnje da je izvršilo neko od krivičnih dela zakonom određenih (taksativno nabrojanih krivičnih dela — tzv. kataloški određenih krivičnih dela). Posebne radnje otkrivanja i dokazivanja krivičnih dela su izuzetne. Njihova primena se ograničava, po pravilu, samo na najteže oblike kriminala (organizovani kriminal, terorizam, korupcija, pranje novca), ali i kada se ova krivična dela otkrivaju i dokazuju, posebne radnje se koriste samo kao *ultima ratio*, odnosno kao poslednje sredstvo za kojim se poseže, ukoliko se klasičnim policijskim i istražnim radnjama ne postižu rezultati. Posebne mere se koriste izuzetno i zbog toga što se njima zadire duboko u zaštićenu zonu, ustavima i međunarodnim pravnim aktima, sloboda i prava građana. Zbog toga se i radnja kompjuterske obrade podataka može primenjivati samo pod sledećim uslovima:¹

- da je izričito predviđena zakonskim odredbama (načelo legaliteta);
- da ne postoje blaže mere za ostvarenje istog cilja (načelo supsidijarnosti);

¹ Na osnovu preporuke sadržane u Rezoluciji donetoj na XVI kongresu AIDP-a. (A. Kurtović — P. Novoselec — G. Tomašević — S. Gluščić, XVI međunarodni kongres za kazneno pravo, HLJKPP 2/1999, 1051.)

- da se radi o vrlo teškim krivičnim delima (načelo srazmernosti);
- na osnovu postojanja *osnova sumnje* da je izvršeno krivično delo;
- na osnovu odluke nadležnog sudskog organa;
- da je precizno vremenski ograničena;
- uz postojanje nadzora nad zakonitim sprovođenjem mere.

Automatska kompjuterska obrada podataka se u najvećem broju zemalja veoma uspešno koristi prvenstveno u slučajevima krivičnih dela organizovanog kriminala i terorizma. Međutim, ova mera se koristi i kod krivičnih dela vezanih za utaju poreza (kao npr. u Italiji), kao i kod ilegalnog prelaska granice, učešća u saobraćajnim nesrećama i dr. U SAD-u se na primer, ova mera koristi za pronalaženje nestalih lica ili identifikaciju lica koje protivzakonito traže ili primaju socijalnu pomoć, ali i za evidenciju i analizu poreskih prijava i finansijskih transakcija ili pranja novca.

Pristup kompjuterskim sistemima i kompjutersko automatsko obradivanje podataka ograničava sigurnost i tajnost ličnih podataka kao jedno od osnovnih prava čoveka. Građani moraju biti zaštićeni od neograničenih i prekomernih prikupljanja, pohranjivanja, korišćenja i dostavljanja ličnih podataka od strane državnih organa. Zbog toga se lični podaci, u skladu sa međunarodnim standardima, mogu prikupljati, obrađivati i upotrebljavati samo pod zakonom određenim uslovima.² Prikupljanje, informatička obrada i korišćenje podataka za potrebe stvaranja različitih baza podataka u velikom broju država je uređeno posebnim zakonima kojima se reguliše način zaštite podataka.³ Najčešće se ovim zakonima propisuju uslovi pod kojima je dozvoljeno policijsko pohranjivanje podataka, vrste i obim pohranjivanja podataka kao i korišćenje informatičkih baza podataka za potrebe kriminalističke policije.

Ni savremeni međunarodni standardi ne garantuju apsolutno pravo privatnosti, jer uvek postoje oblasti gde su ta prava značajno ograničena kao što su državna i javna bezbednost, krivičnopravna gonjenja i sl., odnosno tamo gde opšti interes preteže nad pojedinačnim. Zadiranje u pravo na zaštitu ličnih podataka dopušteno je u skladu sa ograničenjima sadržanim u čl. 8. Evropske konvencije o zaštiti ljudskih prava i osnovnih sloboda.⁴ Svako ima pravo na zaštitu svojih ličnih podataka. Takvi se podaci moraju pravično upotrebljavati u određene svrhe i to uz pristanak zainteresovanog lica, odnosno na osnovu neke druge legitimne osnove propisane zakonom. Svako lice ima pravo pristupa podacima koji se odnose na njega, kao i pravo na ispravku tih podataka. Nadzor nad poštovanjem

² Council of Europe: Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data, European Treaty Series No. 108, ugovor je potpisan 08. 01. 1981. godine, a stupio je na snagu 01. 10. 1985. godine, http://www.privacy.org/pi/intl_orgs/coe/dp_convention_108txt. Naša zemlja nije ratifikovala ovu konvenciju.

³ U Srbiji zaštitu podataka o ličnosti garantuju Ustav RS (Službeni glasnik RS br. 1/90), Povelja o ljudskim i manjinskim pravima i građanskim slobodama (Službeni list SCG br. 6/03), Zakon o zaštiti podataka o ličnosti (Službeni glasnik RS br. 24/1998) i Zakon o policiji (Službeni glasnik RS br. 101/05).

⁴ Službeni list SCG — Međunarodni ugovori br. 9/2003.

ovih pravila treba da vrši nezavisni organ. Ovde je reč o pravu koje nije sadržano u izvornom tekstu Evropske konvencije, već je artikulirano u praksi Evropskog suda za ljudska prava u okviru člana 8, tj. prava na privatni i porodični život.⁵

Uporednopravnim istraživanjem dolazi se do zaključka da se radnja kompjuterske obrade ličnih podataka koristi u kriminalističkoj praksi svih evropskih država i u SAD-u, i to u preventivne i u represivne svrhe. Srbija je jedna od retkih zemalja u kojoj je korišćenje kompjuterske obrade ličnih podataka tek na samom početku. Postoje izvesne baze podataka, ali one nisu centralizovane i objedinjene. Postoje brojne inicijative za stvaranje različitih baza podataka ne samo u okviru MUP-a, nego i u drugim institucijama koje se bore protiv kriminala. Novim Zakonikom o krivičnom postupku je u Glavi VIII koja se odnosi na posebne dokazne radnje predviđena i dokazna radnja *automatsko računarsko pretraživanje ličnih i drugih podataka*. Ova dokazna radnja se sastoji u automatskom pretraživanju već pohranjenih ličnih i drugih, sa njima neposredno povezanih podataka i njihovom automatskom poređenju sa podacima koji se odnose na neko krivično delo koje je predviđeno u čl. 155. st. 1. ZKP-a i lice koje se osnovano može dovesti u vezu s tim krivičnim delom, da bi se na taj način kao mogući osumnjičeni isključila lica u pogledu kojih ne postoji verovatnoća da su povezana sa krivičnim delom, a izdvojila ona lica u odnosu na koja se prikupe podaci iz kojih proizilaze osnovi sumnje (čl. 155. st. 3). Ovako zakonikom određena, ova radnja predstavlja negativnu raster potragu.

Posebna dokazna radnja se može preduzeti ako postoje *osnovi sumnje* da je učinjeno jedno od krivičnih dela predviđenih u čl. 155 st. 1. ZKP-a. Iako ova radnja spada u posebne dokazne radnje čija primena po pravilu ima opravdanja samo u slučajevima organizovanog kriminala, terorizma, pranja novca i korupcije, naš zakonodavac je predvideo izuzetno širok krug krivičnih dela na koja se ona može primeniti. Osim toga, Zakonikom nije predviđen nijedan poseban uslov o kojima je već bilo reči u radu, za primenu ove radnje kao što je to na primer slučaj kod posebne radnje angažovanja prikrivenog islednika (čl. 151. st. 1. ZKP-a) ili pružanja simulovanih poslovnih usluga i sklapanje simulovanih pravnih poslova (čl. 148. st. 3. ZKP-a) gde se izričito propisuje uslov *ultima ratio* za primenu mere.

Izuzetno se ova radnja može odrediti i ako osobite okolnosti ukazuju da se priprema neko od krivičnih dela predviđenih zakonom, a činjenice ukazuju da se izvršenje krivičnog dela na drugi način ne bi moglo sprečiti ili bi njegovo sprečavanje bilo znatno otežano, odnosno nastupile bi nepopravljive štetne posledice po život ili zdravlje ljudi, odnosno imovinu veće vrednosti. Treba napomenuti da se u uporednopravnim rešenjima po-

⁵ Videti npr. Leander protiv Švedske, odluka od 26. marta 1987. (Series A, Vol. 116 — o vođenju i upotrebi tajnih policijskih dosijea); Gaskin protiv Ujedinjenog Kraljevstva, odluka od 07. jula 1989. (Series A, Vol. 160 — o dostupnosti podataka o biološkoj porodici posle usvojenja) i dr.

sebnje radnje po pravilu primenjuju za otkrivanje i dokazivanje izvršenih krivičnih dela. Međutim, postavlja se pitanje opravdanosti primene posebnih radnji u slučaju da se radi o pripremanju krivičnog dela. Smatram da bi to bilo opravdano samo u slučaju da samo pripremanje predstavlja krivično delo, a osim toga, takva zakonska mogućnost nije ni u suprotnosti sa Konvencijom UN o transnacionalnom organizovanom kriminalu u kojoj, iako se ne predviđa izričito u kojim slučajevima se specijalne istražne tehnike primenjuju, odnosno da li se primenjuju samo kod izvršenja krivičnog dela ili i kod njegovog pripremanja, može se izvesti zaključak da njihova primena kod pripremanja krivičnih dela nije zabranjena. Ukoliko se radnja, u slučaju sumnje da se priprema krivično delo, primenjuje u skladu sa zakonskom regulativom i pod strogom kontrolom nema nikakve opasnosti za ugrožavanje ljudskih prava i sloboda.

Posebnu radnju kompjuterske obrade podataka naređuje istražni sudija na predlog javnog tužioca, a u slučaju postojanja okolnosti koje ne trpe odlaganje, ovu naredbu može izdati i javnu tužilač, s tim da je u roku od 24 sata mora podneti istražnom sudiji na potvrđivanje. U slučaju da je u predviđenom roku istražni sudija ne potvrdi, naredba se stavlja van snage bez odlaganja, a svi prikupljeni podaci se uništavaju pod nadzorom istražnog sudije i javnog tužioca. Ova radnja može trajati najviše tri meseca, a iz važnih razloga se njeno trajanje može produžiti za još tri meseca. Ovu radnju sprovode policija, Bezbednosno-informativna agencija, organ carinske službe ili drugi državni organ, odnosno druga pravna lica koja na osnovu zakona vrše određena javna ovlašćenja. Svi prikupljeni podaci se pod nadzorom javnog tužioca i istražnog sudije moraju uništiti ukoliko se u roku od šest meseci od završetka sprovođenja posebne dokazne radnje ne pokrene krivični postupak.

Prvni osnov za korišćenje ove radnje je različit u pojedinim zemljama. U SAD-u to su: Privacy Act iz 1974. godine,⁶ Computer Matching and Privacy Protection Act iz 1988. godine⁷ (ovaj zakon predstavlja izmenu i dopunu Zakona iz 1974. godine), Social Security Act.⁸ U Engleskoj to su: Data Protection Act iz 1984. godine,⁹ u Italiji to je Zakon br. 410 iz 1991. godine.¹⁰ U Nemačkoj i Hrvatskoj to je Zakon o krivičnom postupku.¹¹ U Srbiji to je Zakonik o krivičnom postupku.¹²

Što se tiče **svrhe korišćenja** ove radnje, ona se koristi i u represivne i preventivne svrhe: za otkrivanje i sprečavanje pranja novca (SAD, Engleska, Italija, Nemačka, Srbija) za proveru socijalnog statusa lica (SAD,

⁶ http://www.usdoj.gov/04foia/04_7_1.html

⁷ <http://www.privacilla.org/government/cmppa.html>

⁸ http://www.ssa.gov/op_home/ssact/comp-ssa.htm

⁹ <http://www.swarb.co.uk/acts/1984DataProtection02Act.html>

¹⁰ O ovome više videti: L. Cortellessa, Understood it / Preventive l'Investigazione, http://www.carabinieri.it/editoria/Rassegna/2003-04-supplemento/Capitolo_5.htm

¹¹ Zakon o krivičnom postupku Nemačke <http://www.iuscomp.org/gla/statutes/StPO.ntm>
Zakon o kaznenom postupku Hrvatske, Narodne novine br. 110/1997.

¹² Službeni glasnik RS br. 46/06.

Italija) za potrebe utvrđivanja kruga osumnjičenih lica za izvršena krivična dela (SAD, Engleska, Italija, Nemačka). Uz pomoć kompjutera i pohranjenih baza podataka u kriminalističkim evidencijama se izrađuje kompjuterski profil izvršilaca različitih krivičnih dela, što policiji služi u operativne svrhe, za stvaranje širokog kruga mogućih izvršilaca krivičnih dela prema nekim karakteristikama (npr. prema *modus operandi* sistemu). U SAD-u Državni kriminalističko-obaveštajni centar (National Criminal Intelligence Center — NCIC¹³) koji deluje u okviru FBI-a, sadrži 12 datoteka različitih podataka (o ukradenim predmetima, počiniocima teških krivičnih dela, nestalim licima, licima za kojima se traga i sl.).

Kompjutersko sravnjivanje podataka radi otkrivanja i sprečavanja pranja novca se već dugo godina veoma uspešno koristi u SAD-u. Ovu metodu kao jednu od glavnih koristi i Služba za suzbijanje finansijskog kriminala (FINCEN) u cilju otkrivanja i suzbijanja pranja novca analiziranjem postojećih evidencija poreskih prijava, finansijskih transakcija, prijava osiguravajućih društava i banaka o primanju, uplati i inostranim doznakama gotovinskih iznosa većih od 10000 američkih dolara i sl. Ova mera se u svrhu otkrivanja i sprečavanja pranja novca koristi i u Srbiji od 2002. godine. U pogledu otkrivanja i dokazivanja različitih oblika pranja novca poseban značaj imaju postupci i mehanizmi za evidentiranje sumnjivih finansijskih transakcija, a u pogledu obezbeđenja dokaza, postupak arhiviranja i obrade evidentiranih podataka i njihova dostupnost organima otkrivanja i gonjenja. U tom pogledu Zakon o sprečavanju pranja¹⁴ novca je predvideo odgovarajuća rešenja, a to se prvenstveno odnosi na formiranje centralne finansijsko-obaveštajne agencije — Uprave za borbu protiv pranja novca.¹⁵ Što se tiče korišćenja ove mere za proveru socijalnog statusa lica u SAD-u, na primer, Zakon o socijalnoj bezbednosti izričito predviđa prikupljanje podataka u periodu od po tri meseca od poslodavaca o prihodima zaposlenih lica, kao i pristup službenika izvršne vlasti podacima poreske uprave i drugim sličnim evidencijama u cilju provere dobijenih saznanja o protivpravnom ponašanju i zloupotrebama u vezi sa prijavljivanjem poreza i korišćenjem socijalne pomoći. Na taj način se istražuje da li je lice koje prima socijalnu pomoć istovremeno upisano u evidenciju vlasnika skupocenih vozila i dr. Dobijeni podaci se smeju koristiti samo u te svrhe. Zakon o privatnosti sadrži opšte odredbe o pravnoj zaštiti podataka koji su pohranjeni u evidencijama saveznih organa, čije je glavno načelo da se prikupljeni podaci mogu koristiti samo u tačno odre-

¹³ <http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm>

¹⁴ Zakon o sprečavanju pranja novca, Službeni glasnik RS br. 107/05.

¹⁵ Neophodno je istaći da je sa Upravom za sprečavanje pranja novca sarađivao tim USAID-a i Trezora SAD-a i to na operativnom osposobljavanju za rad po međunarodnim standardima, što je rezultiralo članstvom u EGMONT grupi (svetskoj mreži finansijskih obaveštajnih jedinica) i to samo godinu dana nakon osnivanja Uprave, što predstavlja najbrže pridruživanje jedne takve jedinice u istoriji EGMONT-a. Članstvo u ovoj instituciji znači efikasnu saradnju u međunarodnim granicama, što omogućava da se organima gonjenja pravo vreme obezbede informacije koje su potrebne za uspešno vođenje istrage i zamrzavanje finansijskih sredstava učiniocima krivičnih dela.

dene, svima poznate svrhe. Korišćenje ovih podataka u druge svrhe moguće je samo uz prethodno odobrenje dotičnog lica.

U Italiji se omogućavanje razmene prikupljenih kriminalističko-obaveštajnih i drugih podataka između organa državne uprave smatra jednim od osnovnih uslova za uspešnu borbu protiv organizovanog kriminala. Potvrda ovog stanovišta jeste postojanje razmene informacija između državnog tužilaštva, sudske i finansijske policije, uprave za sprečavanje pranja novca, poreske uprave, obaveštajnih službi i Komisije za borbu protiv mafije čijem predsedniku policija mora dostavljati sva prikupljena saznanja o delovanju mafije. U svakodnevnoj policijskoj praksi u Italiji se koristi tzv. *pozitivna raster potraga* koja ima za cilj utvrđivanje sumnjivih lica u grupi lica koju obeležava određena karakteristika ili sposobnost koju je imao i nepoznati izvršilac krivičnog dela. Nisu predviđena nikakva zakonska ograničenja za policijsko korišćenje prikupljenih podataka na bilo koji način, izuzev institucije službene tajne i tehničkih teškoća koje su vidljive prilikom tehničkog umrežavanja svih elektronski vođenih baza podataka u organima javne uprave. Policiji je dopušteno stvaranje i neograničeno korišćenje vlastitih baza podataka u cilju suzbijanja svih vrsta kriminalnog ponašanja.

Interesantno je da je u borbi protiv zloupotrebe droga, vlada SAD-a uvela izgradnju i objedinjavanje postojećih programa elektronske obrade podataka, u cilju da se ojača primena mera kompjuterskog istraživanja. Međutim, ovo nije slučaj i sa organizovanim kriminalom.

Primena kompjuterske obrade podataka u Nemačkoj je regulisana policijskim zakonodavstvom pojedinih saveznih pokrajina, ali i u Zakonu o krivičnom postupku (čl. 98a-c). Odredbama nemačkog ZKP-a preciziraju se uslovi primene kompjuterske obrade podataka u cilju kompjuterskog pretraživanja identifikacionih podataka lica, imalaca određenih karakteristika koji verovatno upućuju na izvršioca tačno određenih krivičnih dela da bi se isključila lica koja nisu osuđena ili suzio krug lica koja bi na osnovu utvrđenih karakteristika mogli doći u obzir kao izvršioc krivičnih dela. Ovaj način istrage se naziva negativno kompjutersko pretraživanje, odnosno *negativna raster potraga*. Negativnom raster potragom se isključuju iz dalje kriminalističke obrade lica koja nisu sumnjiva. Ova mera se može koristiti ako ima dovoljno razloga za sumnju, po oceni suda, da je izvršeno jedno od sledećih krivičnih dela: ilegalna trgovina drogom, oružjem; napad na ustavni poredak; opšte opasna krivična dela protiv života i tela, polnog integriteta, lične slobode; ili su krivična dela izvršena na profesionalan način, organizovano, iz navike, od nekog člana bande ili zločinačke organizacije. Mera se koristi kao *ultima ratio*, odnosno samo onda kada istraživanje činjeničnog stanja na neki drugi način ne bi imalo uspeha ili bi bilo povezano sa znatnim teškoćama.

U Hrvatskoj se ova radnja preduzima samo ako postoje osnovi sumnje da su izvršena tačno kataloški određena krivična dela: protiv vrednosti zaštićenih međunarodnim pravom, oružane pobude, protivdržavni teroriz-

zam, ubistva, otmice, iznude, zloupotrebe opojnih droga, prikrivanje protivzakonito dobijenog novca i narušavanja vojne i odbrambene moći države.

a) Način odobravanja mere, dužina trajanja mere i korišćenje izvoda iz kompjutera kao dokaza u krivičnom postupku

Meru kompjuterskog sravnjivanja podataka odobravaju u pojedinim zemljama različiti organi u različitim fazama postupka. Pa tako u toku kriminalističke obrade ovu meru odobrava načelnik policije (SAD, Engleska, Italija, Nemačka, Hrvatska). Za primenu ove mere u krivičnom postupku odobrenje daje sud (SAD, Engleska, Italija, Nemačka). U SAD-u je na primer poznat sudski poziv za prednošenje traženih podataka — tzv. *subpoena duces tectum*. Osim navedenih, ovu meru mogu da odobravaju i neki drugi organi, pa je u SAD-u to načelnik FINCEN-a, u Italiji šef DIA-e i državni tužilac, u Nemačkoj državni tužilac izuzetno, a u Hrvatskoj ravnatelj Službe za zaštitu ustavnog poretka RH.

U Nemačkoj, meru može naložiti samo sudija pismenim nalogom. Izuzetno u slučaju opasnosti od odlaganja to može odobriti državni tužilac, ali se u tom slučaju naknadno, u roku od tri dana mora dobiti sudski nalog. Pismeni nalog mora biti obrazložen i u njemu mora biti tačno određeno lice koje je dužno da dostavi tražene podatke ograničene prema karakteristikama mogućih izvršilaca tačno određenog krivičnog dela.

Za policijsko preduzimanje ove mere nije potreban sudski nalog, već je zakonski kontrolni mehanizam uspostavljen kroz formu izveštavanja nadležnog državnog tužioca o sadržaju prikupljenih obaveštenja.

Mera se po pravilu odobrava prema potrebi (SAD, Engleska, Italija, Nemačka), a u Hrvatskoj ova mera se primenjuje do šest meseci, a izuzetno do devet meseci.

Što se tiče korišćenja kompjuterskih izvoda u krivičnom postupku, u Engleskoj prema odredbi koja je sadržana u čl. 69. Zakona o policiji i dokazima u krivičnim stvarima,¹⁶ načelno ne smeju biti upotrebljeni kao dokaz pred sudom izvodi iz kompjutera, osim ako neka od stranaka ne dokaže da nema razumnih razloga za uverenje da je informacija netačna zbog pogrešnog rukovanja računarom. Inače, pred sud se smeju izneti samo one informacije koje govore o postojanju ili nepostojanju određenih činjenica, ako su obe stranke imale priliku da provere njihovu verodostojnost.

Mogućnost korišćenja ovih podataka u Italiji u dokazne svrhe za potrebe vođenja krivičnog postupka moguće je samo uz preciznu naznaku izvora iz kojeg je ili, od kojeg je konkretan podatak dobijen ili nastao.

U Nemačkoj se pribavljeni podaci moraju uništiti ukoliko za njima više ne postoji potreba radi uspešnog vođenja krivičnog postupka. Izuzetno, mogu se koristiti u drugom krivičnom postupku, ukoliko se dođe do

¹⁶ http://www.homeoffice.gov.uk/docs/pacencodea_textchanges.pdf

zaključka da su ti podaci potrebni za razjašnjavanje nekog drugog, kataloški određenog krivičnog dela iz čl. 98a ZKP-a. Ova mera se može koristiti i u cilju kompjuterskog usklađivanja podataka prikupljenih u jednom krivičnom postupku radi razjašnjavanja krivičnog dela, krivičnog gonjenja, izvršenja izrečene kazne, otklanjanja opasnosti ili utvrđivanja boravišta lica za kojim se traži u aktuelnom krivičnom postupku.

U Hrvatskoj, od svih prikupljenih podataka na osnovu ovog ovlašćenja, u krivičnom postupku se mogu koristiti samo oni podaci koji se odnose na identitet izvršioca kataloški određenih krivičnih dela, a ostala prikupljena obaveštenja podležu ustavnoj zabrani njihove upotrebe. Ovako prikupljeni podaci će se uništiti čim prestanu da budu potrebni za uspešno vođenje krivičnog postupka, a najkasnije u roku od šest meseci od dana pohranjivanja podataka. Ovaj rok se izuzetno može produžiti, na predlog državnog tužioca, pisanim i obrazloženim nalogom istražnog sudije za još tri meseca, ukoliko postoji verovatnoća da će se na taj način uspešno okončati raspisana potraga za određenim licem.

b) Nadzor nad zakonitim sprovođenjem mere

S obzirom da se ovom merom zadire u sferu ličnih podataka koji su po pravilu zaštićeni ustavima i pojedinim zakonskim aktima u većini zemalja, u svim zemljama u kojima se primenjuje mera kompjuterske obrade podataka predviđen je višestruki sistem kontrole sprovođenja ove mere. Najčešći oblici kontrole su *administrativna* (SAD, Engleska, Italija, Nemačka, Slovenija, Hrvatska), *sudska* (SAD, Engleska, Nemačka, Austrija, Slovenija, Hrvatska) i *parlamentarna* kontrola (Hrvatska).

c) Prikupljanje i obrada ličnih podataka na međunarodnom nivou

Svi nadležni organi koji se u pojedinim zemljama bore protiv organizovanog kriminala će se na prvom mestu složiti da je proaktivni operativni pristup u otkrivanju i sprečavanju organizovanih kriminalnih aktivnosti neophodan da bi se priveli izvršioci krivičnih dela, uništila kriminalna mreža i oduzela i konfiskovala imovina koja potiče od ove delatnosti. Informacije su neophodne da bi se razotkrio profil, motivi i *modus operandi* izvršilaca krivičnih dela, obim i trendovi organizovnog kriminala, njegov uticaj na društvo. Ove informacije isključivo se mogu naći u *operativnim bazama podataka* (baze podataka koje se odnose na pojedinačno osumnjičena lica i otkrivene slučajeve) i u *empirijskim bazama podataka* (kvalitativne i kvantitativne kriminološke baze podataka).

Nažalost, na globalnom nivou razmene operativnih i empirijskih baza podataka se vrše *ad hoc*, između individualnih organa ili čak fizičkih lica. Ovi *ad hoc* „aranžmani” povećavaju zabrinutost u pogledu poštova-

nja ili nepoštovanja domaćeg zakonodavstva koje se odnosi na zaštitu ličnih podataka. Konvencija Ujedinjenih nacija protiv transnacionalnog organizovanog kriminala u čl. 27. i 28. propisuje saradnju organa unutrašnjih poslova koja se odnosi na razmene ovih podataka.¹⁷ Tako, prema ovoj konvenciji države potpisnice treba međusobno da sarađuju u skladu sa svojim domaćim pravnim i administrativnim sistemima i svaka država treba da usvoji sledeće efikasne mere: a) za unapređenje, i tamo gde je neophodno uspostavljanje puteva za komunikaciju između svojih nadležnih organa, agencija i službi da bi olakšali sigurnu i brzu razmenu informacija koje se odnose na sve aspekte krivičnih dela obuhvaćenih ovom konvencijom; b) za saradnju sa drugim državama potpisnicama u sprovođenju istraga u vezi sa krivičnim delima obuhvaćenim ovom konvencijom koja se odnose na: identitet, mesto gde se trenutno nalaze i aktivnosti osumnjičenih lica, ili lokaciju drugih lica s tim u vezi, kretanje dobiti od kriminala ili imovine stečene izvršenjem takvih krivičnih dela, kretanje imovine, opreme ili drugih sredstava koja se koriste ili su namenjena za korišćenje u izvršenju takvih krivičnih dela; c) za obezbeđivanje, kada je potrebno, neophodnih predmeta ili količina supstanci za potrebe analiza ili istrage; d) za olakšanje efikasne koordinacije između nadležnih organa, agencija i službi za unapređivanje razmene kadrova i drugih eksperata, uključujući postavljanje oficira za vezu; e) za razmenu informacija sa drugim državama potpisnicama o specifičnim sredstvima i metodama koje koriste grupe za organizovani kriminal uključujući, tamo gde je primenljivo, rute i prevozna sredstva i korišćenje lažnih identiteta, izmenjenih ili lažnih dokumenata ili drugih metoda za skrivanje njihovih aktivnosti; f) za razmenu informacija i koordiniranje administrativnih i drugih mera koje se preduzimaju prema potrebi u cilju rane identifikacije krivičnih dela obuhvaćenih ovom konvencijom.

Sa druge strane, u okviru Evropske unije postoji nekoliko sporazuma koji se odnose na prikupljanje i analizu podataka: Zajednička akcija, usvojena 1996. godine odnosi se na ulogu oficira za vezu. Njihova funkcija se sastoji u prikupljanju podataka. Oni treba da olakšaju i ubrzaju prikupljanje i razmenu podataka kroz direktne kontakte sa nadležnim organima u drugim državama članicama i domaćom državom i da doprinesu prikupljanju i razmeni informacija, i to naročito onih strategijske prirode koji se mogu koristiti za poboljšanje mera u borbi protiv internacionalnog kriminala uključujući i organizovani kriminal.

Na nivou Evropske unije značajnu ulogu u prikupljanju i obradi ličnih podataka ima Eurojust — Evropska pravda (telo Evropske unije sa pravnim subjektivitetom, koje obezbeđuje saradnju između tužilačkih i sudskih organa država članica — o čemu će posebno biti reči kasnije u radu). U okviru svoje nadležnosti Evropska pravda sakuplja i kompjuterski obrađuje lične podatke. Postupanje sa ličnim podacima mora biti u

¹⁷ Konvencija UN protiv transnacionalnog organizovanog kriminala od 15. 12. 2000. godine, Službeni list SRJ — Međunarodni ugovori br. 6/2001.

skladu sa odredbama Konvencije Saveta Evrope od 28. januara 1981. godine o zaštiti lica prilikom kompjuterske obrade ličnih podataka¹⁸ i amandmanima na ovu konvenciju. Evropska pravda formira i održava bazu podataka koja predstavlja indeks podataka o istragama zajedno sa odgovarajućim ličnim i drugim podacima. Ovi podaci koji se obrađuju čuvaju se samo onoliko koliko je neophodno za postizanje njegovih ciljeva. Ovom odlukom su propisana ograničenja za postupanje sa ličnim podacima u smislu da kada se postupa sa njima mogu se obrađivati samo određeni podaci o licima koja su prema nacionalnom zakonodavstvu država članica kojih se ti podaci tiču, pod istragom ili krivičnim gonjenjem za jednu ili više vrsta krivičnih dela propisanih ovom odlukom i to: prezime, devojčako ime, ime, ili bilo koje ime pod kojim je lice poznato, datum i mesto rođenja, nacionalnost, pol, mesto stanovanja, zanimanje, mesto boravka, broj socijalnog osiguranja, vozačke dozvole, lične karte i pasoša, bankarski računi, kao i računi u drugim finansijskim ustanovama, opis i priroda navodnih prestupa, datum kada su oni bili izvršeni, napredak u istragama, činjenice koje ukazuju na međunarodni element krivičnog dela i detalji koji se tiču navodnog članstva u kriminalnoj organizaciji. Kada se obrađuju podaci o licima koja se, prema nacionalnom zakonodavstvu država članica kojih se to tiče, smatraju svedocima ili žrtava krivičnog gonjenja povodom jedne ili više vrsta krivičnog dela definisanih u ovoj odluci, Eurojust može da obrađuje samo najvažnije podatke o tim licima kao što su, ime, prezime, devojčako prezime, datum i mesto rođenja, nacionalnost, pol, mesto boravka i detalje vezane za krivično delo za koje se vodi istraga, a tiču se tog lica. U izuzetnim slučajevima Eurojust može u ograničenom vremenskom periodu da obrađuje i druge podatke koji se tiču okolnosti krivičnog dela kada su oni od neposrednog značaja za tekuće istrage čije koordinisanje pomaže. Evropska pravda i svaka država članica nastojace da tokom obrade ličnih podataka u okvirima ove odluke, zaštite lične podatke od slučajnog ili nezakonitog uništenja, slučajnog gubljenja ili neovlašćenog otkrivanja, izmene ili neovlašćenog pristupa ili bilo kog vida neovlašćene obrade. U cilju osiguranja zakonite obrade podataka i postupanja u skladu sa odredbama ove odluke o ličnim podacima, u okviru Evropske pravde imenovan je specijalni službenik za zaštitu podataka.

Postoji pravo uvida u lične podatke i svaki pojedinac ima pravo uvida u svoje lične podatke koji su pohranjeni u bazi podataka. Da bi iskoristio ovo svoje pravo lice mora prethodno uputiti zahtev nadležnom organu države članice po izboru, koji ga zatim prosleđuje Evropskoj pravdi. Ovo pravo uvida se vrši u skladu sa zakonima i postupkom države članice u kojoj je taj pojedinac podneo zahtev. Ipak, pravo uvida može biti uskraćeno u sledećim slučajevima: a) ako takav pristup može da ugrozi delatnost Eurojust-a; b) ako takav pristup može da ugrozi bilo koju istragu

¹⁸ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108).

koju potpomaže ovo telo; c) ako takav pristup može da ugrozi prava i slobode trećih lica.

O zahtevu lica za uvid u lične podatke odlučuju nacionalni članovi kojima je ovaj zahtev upućen i oni donose o tom zahtevu odluku u ime Evropske pravde. Rok za razmatranje zahteva je tri meseca od dana prijema. Ukoliko postoji nesaglasnost članova o ovom zahtevu, isti se upućuje Komisiji na donošenje odluke.

Lice koje ima pravo uvida može da traži ispravku ili brisanje ličnih podataka ukoliko su oni netačni ili nepotpuni ili ukoliko njihovo unošenje ili pohranjivanje nije u skladu sa odredbama odluke o ispravljenim ili izbrisanim podacima. Ukoliko nije zadovoljno, lice može predmet da uputi Zajedničkom nadzornom telu u roku od 30 dana koje vrši nadzor nad zakonitošću obrade podataka. Ovo telo čine tri stalna člana i *ad hoc* sudije koji deluju u svojstvu člana ovog tela samo tokom razmatranja žalbe u pogledu ličnih podataka iz država članice koja ih je imenovala. Sudija ko- ga imenuje država članica postaje stalni član godinu dana pre nego što njegova država članica postane predsedavajuća država Saveta Evropske unije i zadržava funkciju stalnog člana 18 meseci. Ovaj sudija predsedava Zajedničkim nadzornim telom. Ovo telo razmatra žalbe na zahtev lica za brisanje i ispravku ličnih podataka i na taj način vrši kontrolu obrade po- dataka.

Odlukom o osnivanju Evropske pravde propisana je i odgovornost za neovlašćenu ili netačnu obradu podataka. Evropska pravda je odgovor- na, shodno nacionalnom pravu države članice gde se nalazi njegovo sedi- šte, za štetu koju nanese pojedincu a koja je proistekla iz neovlašćene ili nepravilne obrade podataka.

d) Kriminalistička obaveštajna analitika

U vezi sa bazama podataka i kompjuterskim sravnjivanjem tih poda- taka, neophodno je nešto više reći o kriminalističko-obaveštajnoj analitici i njenoj ulozi u borbi protiv organizovanog kriminala, a posebno teroriz- ma. Savremena policijska delatnost se prvenstveno temelji na posedova- nju optimalne količine kriminalistički relevantnih informacija sadržanih u kompjuterizovanim kriminalističkim evidencijama koje predstavljaju svo- jevrstne elektronski uređene banke podataka. Sve klasične kriminalističke evidencije su kompjuterizovane, što omogućava brzo manipulisanje poda- cima i što je posebno važno, time se stvaraju mogućnosti promptne i efi- kasne identifikacije učinioca, odnosno stvaranja kruga osumnjičenih, na bazi npr. analize načina izvršenja.¹⁹ Kompjuterizacija klasičnih kriminali- stičkih evidencija omogućava brzo pretraživanje pohranjenih informacija i što je još važnije efikasnije i brže upoređivanje novih informacija, pre

¹⁹ M. Škulić, *Nove metode i kompjuterski sistemi u savremenoj kriminalistici*, Bez- bednost br. 1/2003, str. 17.

svega onih koje su sadržane u raznim vrstama tragova, sa onima koje su već obrađene i svrstane u odgovarajuće evidencione zbirke centralnih ili perifernih kompjuterskih sistema.

Kriminalistička obaveštajna analitika se definiše kao proces prikupljanja, obrade i interpretacije podataka koji integriše struktuiranu metodologiju sa intelektualnom sposobnošću pronalaženja principa i značenja, kreirajući proizvod, unapređeni pogled na krivično delo i/ili kriminalitet pri ostvarenju policijskih ciljeva.²⁰

Kriminalistička obaveštajna analitika ima presudan značaj u borbi protiv organizovanog kriminala, a još više u borbi protiv terorizma. U vezi sa terorizmom analitika se može opisati kao proučavanje sirovih podataka koji omogućavaju analitičaru otkrivanje mogućih trendova u terorističkim aktivnostima uz davanje preporuka za odgovarajuće rukovođenje istragama. Borba protiv terorizma zahteva da se koncepcija kriminalističke obaveštajne analitike, koja je do sada bila taktički orijentisana i pasivna, proširi na način na koji će se uključiti i aktivno prikupljanje podataka i interdisciplinarni pristup. Aktivno prikupljanje podataka mora postati sastavni deo svakodnevne analize u cilju održavanja vrednosti analitičkih rezultata i unapređenja postavljanja odgovarajućih prioriteta. Integracija analitičkih informacija sa sprovođenjem kriminalističkih obrada je jedini način efikasnog upravljanja istragom. Analitičke tehnike se mogu koristiti u proaktivnim i reaktivnim terorističkim istragama, a analitičke tehnike koje se koriste tokom proaktivnih istraga sadrže procenu potencijalne pretnje terorističke grupe. Kao rezultat procene pretnje mogu se preduzeti određene radnje u cilju povećanja bezbednosti kod nekih događaja, obezbeđenja pojedinaca ili mesta.²¹ Osnovni cilj analitičke informacije jeste davanje upozorenja nadležnim organima o pojavi terorističke pretnje ili davanju upozorenja o mogućnosti ili verovatnoći takve pretnje. Procena pretnje je strateški dokument koji obrađuje sklonost određene grupe ka nasilju ili kriminalu, ili mogućem događanju kriminalne aktivnosti u određenom vremenu i na određenom mestu, a potiče iz vojnog obaveštajnog okruženja u vezi sa analitičkim proizvodom upozorenja.²² Prikupljanjem podataka o raznim pokazateljima može se proceniti nivo potencijalne pretnje pojedine grupe. Potencijalna pretnja daje osnovani zaključak o namerama i mogućnostima terorističke grupe i može se koristiti pri usmeravanju istraga na grupe koje imaju najveću sklonost ka aktima nasilja. Kao deo procene pretnje, analitičar mora izraditi preporuke koje omogućavaju rukovodiocima da rasporede sredstva i preduzmu nužne korake. Procenjivanjem pretnje se zapravo procenjuju karakteristike, analiziraju rizici i meri potencijal mogućeg nasilja koji je povezan sa terorističkim grupama, a te

²⁰ H. Atkin, *Criminal Intelligence Analysis: A Scientific Perspective*, Ialeia Journal No. 1/2000, 3.

²¹ M. B. Peterson, *Applications in Criminal Analysis*, Praeger, 1994, 118.

²² R. Kopal, *Značaj kriminalističke obaveštajne analitike u antiterorističkoj delatnosti*, Zbornik Pravnog fakulteta u Rijeci, br. 23/2002, str. 570.

procene policija koristi u taktičke i strateške svrhe kako bi se označile i neutralizovale grupe pre nego što izvrše krivična dela.

Pravi efekat u antiterorističkoj delatnosti će se ostvariti samo prepoznavanjem indikatora i pravilnim odgovorom pre nego što grupa ili organizacija izvrši terorističko delo. Da bi se ostvario taj cilj, kriminalistički obaveštajni proces mora postati sastavni deo policijskih antiterorističkih mera i aktivnosti. Međutim, ovo se može ostvariti samo onda ukoliko se podrži policijski rad vođen analitičkim informacijama, odnosno ako se analitička informacija smatra preduslovom efikasnog policijskog rada.

AUTOMATIC COMPUTER BASED DATA PROCESSING AS A SPECIAL INVESTIGATION ACTIVITY

Tatjana Lukić, Ph.D.

Teaching assistant of the Faculty of Law in Novi Sad

Summary

The application of special investigation activities is characteristic for proactive investigations related to the organized crime. One of these special investigation activities, that became more and more important, is a computer based automatic data processing which was introduced in Serbia by the new Law on Criminal Procedure. The subject matter of this paper is legal solution in Serbia related to this special investigation activity. Apart from that, the author demonstrated its comparative regulation by analyzing legal basis for its application, terms and means of its approval, duration, use of computer excerpts as evidence in the criminal procedure and supervision over its legality. The author paid special attention to the personal data processing on the international level and issue of criminal investigation analytics in combating terrorism.

Keywords: special investigation activities, computer based data processing, organized crime