Dr Darko MARINKOVIĆ,
docent Kriminalističko-policijske akademije u Beogradu
Dr Zoran ĐURĐEVIĆ,
docent Kriminalističko-policijske akademije u Beogradu

UDK: 343.985 : 004.6
Primljeno: 28. februara 201 1. god.

RAČUNARSKO PRETRAŽIVANJE I UPOREĐIVANJE PODATAKA U OTKRIVANJU I DOKAZIVANJU KRIVIČNIH DELA*

Prikupljanje najraznovrsnijih informacija o građanima i njihovo smeštanje u odgovarajuće baze, predstavlja realnost savremenog društva. Rast količine ovih informacija prevazišao je čovekove moći da tradicionalnim sredstvima obrađuje i analizira tako velike količine podataka, iziskujući kompjuterizovane metode za ove potrebe. Iako godinama unazad ima široku primenu u poslovima javne uprave i privrede, kompjutersko pretraživanje i upoređivanje podataka do sada nije dovoljno eksploatisano u kriminalistici i forenzici. Policijske agencije i forenzičke laboratorije sakupljaju velike količine različitih podataka, koji nastaju kao rezultat obrade brojnih kriminalnih aktivnosti. Sam uspeh njihovog automatskog pretraživanja i upoređivanja u krivičnim istragama u presudnoj meri zavisi od raspoloživosti i karakteristika podataka (obeležja, rastera) koja se odnose na lica, predmete ili događaje. Od 2006. godine i srpsko krivično zakonodavstvo, kao posebnu dokaznu radnju, predviđa automatsko računarsko pretraživanje ličnih i drugih sa njima povezanih podataka, što je bio odlučujući motiv za pisanje ovog rada.

Ključne reči: kompjutersko pretraživanje i upoređivanje podataka, data mining, computer matching, raster pretrage, nadzor lica kroz podatke, forenzičke baze podataka, specijalne istražne metode.

* *Članak predstavlja rezultat rada na projektu Ministarstva za nauku i tehnološki razvoj Republike Srbije koji se vodi pod brojem 179045.*

1. Uvodne napomene

Izuzetna organizovanost ljudskog društva koja je danas prisutna širom sveta, za sobom nužno povlači prikupljanje i raspolaganje najraznovrsnijim podacima koji se odnose na njegove članove. Efikasno funkcionisanje državnog aparata i nedržavnog sektora zahteva postojanje brojnih evidenija sa informacijama o fizičkim i pravnim licima, njihovom životu i delanju u vezi sa konkretnom oblašću ili problematikom povodom koje se takve evidencije i baze podataka vode. Sa druge strane, sam razvoj računarske tehnologije (kompjuterizacija) u velikoj meri je povećao mogućnosti prijema, obrade i praćenja takvih podataka, pa čak i u svrhe nadzora nad pojedincem i njegovim ponašanjem. Suštinski značaj računarske obrade i skladištenja informacija nije samo u brzini izvođenja raznih operacija, već pre svega u mogućnosti pristupa integrisanim, međusobno povezanim elementarnim podacima koji potiču iz različitih izvora. Na sadašnjem stepenu razvoja informatičkih tehnologija moguće je da se ovakvi podaci dobiju za nekoliko sekundi ili delova jedne sekunde, umrežavanjem banaka (baza) podataka unutar velikih državnih i društvenih područja, kao što su javna uprava, privreda ili nauka.

Prikupljanje odgovarajućih informacija o građanima u najrazličitije svrhe, te njihovo smeštanje u odgovarajuće baze, predstavlja realnost savremenog društva, jednako kao što je realna (i nužna) činjenica da lica na koja se takvi podaci odnose ne mogu nad njima imati apsolutnu vlast. Ipak, oni i te kako imaju pravo da se osećaju bezbednim od eventualnih zloupotreba korišćenja takvih podataka. Zato se pitanje pravne zaštite podataka građana danas sve više potencira, naročito dolazeći do izražaja u funkcionisanju i obavljanju delatnosti organa državne uprave i pravosuđa, uključujući i policiju. U tom smislu, građani u vezi sa raspolaganjem podacima koji se odnose na njih moraju trpeti određena ograničenja zarad opštih interesa, na isti ili sličan način kao i kada je reč o ograničavanju drugih sloboda i prava građana. Zadatak pravne nauke, zakonodavca i pravničke prakse jeste da definiše normativne osnove prikupljanja i upravljanja najraznovrsnijim podacima, odnosno uslove pod kojima se oni mogu koristiti u društveno opravdane svrhe. Sa druge strane, iz dana u dan se uvećavaju faktičke (u prvom redu tehničke) mogućnosti za što obuhvatnije, složenije i sofisticiranije eksploatisanje podataka o čoveku i njegovom delanju na svim poljima života i rada. Između ostalog, eksploatisanje takvih podataka može dati dobre rezultate i u suprotstavljanju kriminalu.

Eksplozivni rast količine podataka i baza u kojima se oni smeštaju prevazišao je čovekove moći da tradicionalnim sredstvima obrađuje i analizira tako velike količine podataka, iziskujući nove i drugačije tehnike i sredstva automatske analize u raspoloživim bazama. Automatsko pretraživanje i upoređivanje podataka, nezavisno od toga u koje se svrhe primenjuje, zasniva se sa jedne strane na bazama u kojima su smešteni određeni podaci, i, sa druge strane, primeni računara (shvaćenog kao hardver) i odgovarajućih programa (softver) kojima se ti podaci pretražuju, upoređuju i analiziraju.

Tokom XX veka poslovi javne uprave su sve više obuhvatali intenzivno korišćenje podataka o pojedincima. Ekspanzija mrežnog saobraćaja i protoka informacija dodatno je doprinela da ogromne količine podataka koji se razmenjuju budu široko dostupne. Nadzor nad pojedincima putem njihovih podataka postao je lako ostvariv, a istovremeno i mnogo jeftiniji i jednostavniji od konvecionalnih tehnika fizičkog ili elektronskog nadzora. Kao rezultat toga počelo se razvijati nadgledanje putem podataka – *data surveillance*. Reč je o metodu nadziranja velikog broja lica upoređivanjem i uparivanjem podataka koji se na njih odnose, a koji su prikupljeni iz velikog broja izvora. Od početka primene metoda nadziranja podacima, ono je postalo predmet brojnih vladinih publikacija, a o njegovim efektima i uticajima su raspravljali i brojni sociolozi, u manjoj meri i pravnici.

Uobičajeno, nadziranje podacima se u anglo-saksonskoj literaturi skraćeno naziva *dataveillance*, i suštinski predstavlja kontrolu, komparaciju i analizu sistematizovanih podataka o licima u istragama ili praćenju njihovih aktivnosti. Dva su osnovna modaliteta nadziranja lica kroz podatke, i to: 1) nadziranje pojedinca, odnosno individue (*personal dataveillance*), poput provere ili dokazivanja autentičnosti konkretnih, neuobičajenih, odnosno vanrednih poslova i transakcija, koje su u suprotnosti sa internim propisima određene službe ili organizacije, i 2) nadziranje velikog, obično nedefinisanog broja lica (*mass dataveillance*), kao što je provera i dokazivanje autentičnosti svih transakcija koje su u suprotnosti sa internim propisima određene organizacije. Pored dve prethodno navedene, imamo i tehnike za olakšavanje i podršku (*facilitative techniques*), poput tehnika za integraciju podataka smeštenih u razasutim bazama podataka. U odnosu na konvencionalne oblike nadzora, nadziranje podacima je automatizovano, pa prema tome i jeftinije i pouzdanije. Zato je njegova primena tokom poslednjih 30 godina doživela puni procvat, u početku u bogatim društvima sa razvijenim i sofisticiranim informacionim tehnologijama, ali u poslednje vreme i u državama u razvoju, od kojih značajan broj ima legislativnih problema, usled nedovoljno razvijenih mehanizama zaštite građanskih sloboda.

2. Pojam i različiti modaliteti kompjuterskog pretraživanja i upoređivanja podataka

Smatramo da bi terminološki trebalo praviti razliku između pojmova (kompjuterskog) pretraživanja i upoređivanja podataka. Pretraživanje se sastoji u sagledavanju i analizi podataka sadržanih u određenim bazama s ciljem da se u njima pronađu informacije koje na prvi pogled nisu vidljive, a odnose se na određenu osobu, radnju ili proces. Ovako definisano, kompjutersko pretraživanje je najvećim delom sadržano u tehnikama *data minig*-a. S druge strane, upoređivanje podrazumeva da se unapred raspolaže izvesnim podatkom, odnosno obeležjem, koje se provlači i upoređuje sa drugim podacima iz određene baze, s ciljem da se između njih pronađu zajedničke karakteristike, koje ih povezuju i čine sličnim ili

istovetnim (uparivanje). Postupak kompjuterskog upoređivanja se gotovo u potpunosti izjednačava sa procedurom *computer matching*-a.

U raznim oblastima istraživanja (pre svega statistici i veštačkoj inteligenciji) razvijene su procedure automatizovane analize kojima se otkrivaju skriveni sadržaji u velikim skupovima podataka. Proces kojim se to postiže uobičajeno se naziva *data mining – rudarenje podataka*[1]. On označava automatizovani analitički proces oblikovan za efektivnu i efikasnu eksploraciju u velikim zbirkama podataka, s ciljem otkrivanja i korišćenja vrednih, „skrivenih" informacija, koje se tiču novih, do tada neznanih činjenica i relacija. Drugim rečima, *data mining* se može shvatiti kao pronalaženje prethodno nepoznatih i potencijalno korisnih informacija ili saznanja iz velikih skupova podataka. Osnovni princip je da se osmisle kompjuterski programi koji skeniraju takve skupove podataka i automatski tragaju za određenim, unapred definisanim obrascima. Potencijal *data mining* tehnologija u mnogome zavisi od prirode dostupnih skupova podataka i uspešno se primenjuju u oblastima različitih profesija, npr. daljinskom upravljanju resursima, biometriji, prepoznavanju govora ili poslovanju i marketingu. Postupak *data mining* koristi algoritme kako bi u velikim skupovima bili otkriveni značajni skriveni sadržaji, čije tumačenje i razumevanje omogućava bolje dijagnostikovanje stanja stvari, bolje predviđanje i, samim tim, bolje odlučivanje.

Osnovne funkcije *data mining*-a su: 1) klasifikovanje, odnosno ispitivanje svojstava entiteta i njihovo razvrstavanje u unapred određene klase; 2) klasterizovanje, tj. segmentiranje heterogenog skupa entiteta u homogene podgrupe, klastere; 3) ocenjivanje, odnosno predviđanje nepoznatih vrednosti kontinuiranih varijabli; 4) detekcija promena i odstupanja u podacima od prethodno izmerenih ili normativnih vredosti; 5) otkrivanje asocijacija i nalaženje stavki u transakciji koje impliciraju na prisutnost drugih stavki u istoj transakciji, itd. Neki autori[2] klasifikuju funkcije *data mining*-a u dve skupine – prva je usmerena analiza, zasnovana na nadziranom učenju, obuhvatajući klasifikaciju, ocenjivanje i predviđanje, a druga neusmerena analiza, bazirana na nenadziranom učenju, uključujući grupisanje, asocijaciona pravila, deskripciju i vizuelizaciju. Dominantno shvatanje o prirodi nalaza *data mining*-a jeste da se posredstvom njega mogu otkriti samo hipoteze o složenim činjenicama i njihovim odnosima.[3]

Jedna od *mass surveillance* tehnika je i kompjutersko sravnjivanje, odnosno uparivanje podataka, koje podrazumeva upoređivanje mašinski (kompjuterski,

1 Ovim nazivom se u stvari metaforički želi predstaviti ovaj proces, upoređujući se sa iskopavanjem rude. Jednako kao što je samo rudarenje težak i neizvestan posao, u kome se traga za određenom dragocenom rudom u utrobi zemlje, to se i u ovom postupku prekopava, odnosno pretražuje po mnoštvu podataka, u potrazi za onim koji su od koristi.

2 Berry M., Linoff G., Mastering Data Mining, New York, 2000, str. 10.

3 Fayyad U. M. et al.: From Data Mining to Knowledge Discovery: An Overview.- U: Advances in Knowledge Discovery and Data Mining, Cambridge, 1996, str. 18.
Internet: http://www.daedalus.es/fileadmin/daedalus/doc/MineriaDeDatos/fayyad96.pdf

automatski) čitljivih zapisa koji sadrže lične podatke (generalije) velikog broja lica, u cilju otkrivanja i razjašnjavanja interesantnih slučajeva. Ova tehnika se u SAD-u naziva *computer matching*, odnosno *data matching* u Australiji i Kanadi. Postala je ekonomski izvodiva u ranim 1970-tim, kao rezultat razvoja informacionih tehnologija, od kada je postepeno razvijana, da bi danas imala široku primenu, posebno u sferama državne uprave. Neke od preteča *computer matching*-a mogu se pronaći u tzv. programima upoređivanja prihoda (*Income matching programs*), koji su dugo korišćeni od strane poreske administracije u SAD-u, ili sistemu za pomoć roditeljima, odobrenom od strane američkog Kongresa amandmanom na Zakon o socijalnom osiguranju (*Social Security Act*) iz 1974 godine, koji je izvorno bio namenjen pronalaženju i osposobljavanju roditelja koji su prekršili ugovore u vezi sa izdržavanjem svoje dece, da takve ugovore ispoštuju i sprovedu u delo.[4]

Tehnika *computer matching* se koristi u različite svrhe, od kojih se većina odnosi na društvenu kontrolu i efikasan rad organa državne uprave (saobraćaj, policija, zdravstveno osiguranje i sl.), dok se njeni ciljevi generalno mogu podeliti na primarne i sekundarne. Neki od primarnih ciljeva bi bili: 1) otkrivanje greške u programu organa uprave (npr. pogrešna procena određene dobiti, izdavanje računa više puta itd.); 2) provera ispunjenosti uslova za dalje korišćenje određenih pogodnosti, u skladu sa unapred definisanim kriterijumima; 3) otkrivanje nezakonitog ponašanja poreskih obveznika, korisnika određenih beneficija, vladinih službenika i sl. (lažna ili višestruka potraživanja, neprijavljeni prihodi ili imovina, neprikladno ponašanje, sukob interesa); 4) praćenje regularnosti postupaka dodele koncesija ili sklapanja ugovora; 5) pronalaženje adresa osoba prema kojima vladine agencije imaju određena potraživanja; 6) identifikacija onih koji imaju pravo na određenu dobit, ali to pravo trenutno ne koriste; 7) kontrola valjanosti podataka; i 8) ažuriranje

4 Clarke R.: Dataveillance By Governments: The Technique of Computer Matching.- U: Information Technology & People, December 1994, str. 47-48.
Internet: http://www.rogerclarke.com/DV/MatchIntro.html
Clarke navodi da je prvi računarski program namenjen upoređivanju i uparivanju podataka bio tzv. Project Match, sproveden 1977. godine u SAD-u od strane tadašnjeg Zavoda za zdravstvo, obrazovanje i socijalnu pomoć (Department of Health, Education & Welfare). Project Match je upoređivao podatke približno 78% od ukupnog broja porodica koje su primale pomoć za izdržavanje dece, sa podacima iz platnih spiskova oko 3 miliona federalnih službenika. Prijavljeno je 33.000 sirovih pogodataka, koji broj je zatim smanjen na 7100, iz kojih su rezultirala 638 slučaja internih istraga sa 55 optužbi. Procenjuje se da je do 1982. godine u SAD-u od strane državnih i saveznih agencija rutinski sprovođeno oko 200 programa namenjenih sređivanju i upoređivanju podataka. Administracija predsednika Regana (Reagan) pokrenula je akciju povećanja efikasnosti vlade, a Predsednički odbor za integritet i efikasnost Vlade (President's Council on Integrity and Efficiency in Government – PCIE) postao je najoštriji zagovornik uvođenja metoda computer matching-a u savremeni menadžment. Odbor Kongresa za procenu tehnologija (Congress' Office of Technology Assessment) ocenio je da je broj primene metoda kompjuterskog upoređivanja u periodu 1980-1984. godine tri puta povećan, dok Laudon ističe da je taj broj 1986. godine iznosio oko 500.

podataka smeštenih u jednu zbirku zapisa na osnovu podataka iz druge grupe (baze). U okviru sekundarnih ciljeva primene *computer matching*-a izdvaja se: 1) podrška akcijama sa povoljnim finansijskim efektima, poput prekida saradnje sa neurednim platišama, smanjenja prekomernih isplata, naknada za netačne uplate agencijama, neisplaćene poreze ili zaostale isplate dugova, ostvarivanja naknada u korist drugih vladinih agencija, izbegavanja budućih nepravilnih ili prekomernih isplata, zastrašivanje i odvraćanje od budućih nepoštenih ponašanja; i 2) izgradnja i održavanje baza podataka u svrhe socijalne kontrole, istraživanja i statistike, unapređenja strateških programa, te procedura i kontrolnih mehanizama.

Pored *computer matching*-a postoje i druge, usko povezane tehnike koje služe za potporu sprovođenja nadzora širokih slojeva stanovništva kroz podatke. Jedna od njih je *data-linkage* (spajanje, uvezivanje podataka), koja je namenjena skladištenju pojedinačnih zapisa u jedan dosije (fajl) osobe, preko koga se identifikuje jedan ili više drugih dosijea, koji omogućavaju brz i pouzdan međuodnos između podataka u budućnosti. Druga tehnika, poznata kao *data concentration* (koncentrisanja podataka) uključuje spajanje i udruživanje baza podataka ili kreiranje novih, za potrebe podrške brojnim funkcijama državne administracije i privrednih subjekata. Treća tehnika obuhvata korišćenje prostih, višenamenskih identifikatornih obeležja (*common, multi-purpose identifier*), što je podstaklo brojne debate o formiranju širokih nacionalnih programa namenjenih identifikaciji pojedinaca, poput baza sa brojevima socijalnog osiguranja u SAD-u i Kanadi.

Nisu retki slučajevi u kojima osoba želi postići određenu dobit na prevaran način, npr. primati veću penziju prikazujući lažno porodično stanje, ili plaćati niže poreze zato što poreska služba nema realna saznanja o njegovim prihodima; ili dobiti kredit iako za to ne ispunjava uslove, iz razloga što kreditor nije upoznat sa činjenicom da primalac zajma već ima neizmirene, prispele obaveze. U takvim okolnostima, organizacije će verovatno tražiti potvrdu tačnosti i potpunosti podataka priloženih od strane zainteresovanih lica. Da bi zaštitili svoje interese, oni preduzimaju *verification* proceduru, odnosno proveravaju tačnost prikazanih podataka. Pojam *verification* (provera, dokazivanje) se koristi kao zajednički za ove svrhe, ali s obzirom da podrazumeva viši standard dokazivosti i tačnosti nego što je to uopšte moguće utvrditi u ovim slučajevima (van sudskog postupka), to je izraz *cross-checking* (unakrsna provera) svakako primereniji.

Veliki deo obrade i manipulisanja podacima je interne prirode i sprovodi se za potrebe jedne organizacije. Međutim, unakrsne provere generalno podrazumevaju korišćenje, odnosno otkrivanje i obelodanjivanje podataka u konkretnim slučajevima, koji su ranije prikupljeni i obrađeni za druge funkcije i/ili u okviru drugih organizacija. *Cross-checking* se može realizovati u *ad hock* situacijama, prema potrebi, ili prema unapred propisanim sporazumima između pojedinih organizacija. Provere mogu biti učinjene sa ili bez znanja i/ili pristanka pojedinca, kao i sa ili bez eksplicitnog zakonskog ovlašćenja. Brojne *cross-checking* aktivnosti se pokreću i

povodom aplikacija određenih lica, npr. za posao, penziju ili kredit, u kom slučaju se uobičajeno nazivaju *front-end verification*. Obrnuti ili inverzivni aranžman uključuje nagodbu između organizacija, koja podrazumeva automatsko međuobaveštavanje u slučaju da dođe do promene određenih podataka, npr. adrese lica. Takva procedura bi se mogla označiti kao *front-end notification*. *Front-end verification* i *front-end notification* su modaliteti nadzora putem podataka, kao skupa tehnika kojima se jedno ili više lice kontrolišu ali ne direktnim, fizičkim nadzorom, već kroz podatke. Prethodno navedeni slučajevi, u kojima je praćenje u stvari specifična identifikacija lica koja proizlazi iz rezultata transakcija koje uključuju podatke vezane za to lice, predstavljaju forme *personal dataveillance*. Osoba koja je podvrgnuta toj vrsti nadzora može se označiti kao *digital persona* („digitalna osoba").

Cross-checking se može preduzimati i uz odsustvo inicijative od strane subjekta koji bi trebao da obavi transakciju vezanu za određeno lice. Razlozi za to mogu biti sadržani u otklanjanju sumnje u poštenje klijenata i verovanja u sklonost prevarama istih, kao i provera tačnosti podataka u vezi sa osobama sa kojima organizacija sarađuje, kako bi se izbegle potencijalne štetne posledice. Osim pomoći u realizaciji *personal dataveillance*-a, *cross-checking* može dati veliku podršku i realizaciji *mass dataveillance*-a, koji se može preduzeti iz razloga što se unapred ne mogu identifikovati oni pojedinci koji spadaju u kategoriju sumnjivih, odnosno sklonih malverzacijama.

3. Zakonski aspekti kompjuterskog pretraživanja i upoređivanja podataka u krivične svrhe – nemačko i srpsko zakonodavstvo

Nemačka je zemlja koja se može smatrati *kolevkom* automatskog pretraživanja određenih podataka u svrhe suzbijanja kriminala u Evropi. Raster pretrage su u njoj razvijene krajem 70-tih godina prošlog veka, nakon bezuspešnih pokušaja pronalaska pripadnika terorističke organizacije RAF (nm. *Rote Armee Fraktion*, en. *Red Army Faction*, poznata i kao teroristička grupa *Baader-Meinhof*). Uz pomoć ove metode je 1979. godine lišen slobode Heissler, njen istaknuti član.[5] Smisao i cilj raster pretraga u Nemačkoj je da se dođe do određene, tražene osobe, koja je najčešće učinilac teškog krivičnog dela, u pogledu čijeg identiteta se raspolaže samo određenim saznanjima, tj. karakteristikama (obeležjima, rasterima), koje su zajedničke izvesnoj grupi (broju) lica. Da bi se do takve grupe došlo, neophodno je poći od odgovarajućih javnih i privatnih baza podataka o građanima, koje se vode u najrazličitije svrhe i kroz koje se automatski provlače raspoloživi rasteri. Lica čija u bazi definisana „bića", između ostalih obeležja imaju i ona koja poseduje tražena osoba, izdvajaju se u posebnu grupu, tj. ona se na specifičan način

5 Grötker R: Eene meene muh: Rasterfahndung in Deutschland – Teil 1; Internet: http://www.heise.de/tp/r4/artikel/11/11411/1.html

pomoću rastera „filtriraju" iz jedinstvene baze. Time se dolazi do individualno određenih lica sa karakteristikama tražene osobe, koja se daljim merama i radnjama trebaju detaljno proveriti u cilju neposredne konkretizacije traženog. Dakle, s obzirom da ne postoje tačne i precizne informacije o traženom licu, na osnovu raspoloživih saznanja o njemu i njegovim karakteristikama, koje ipak nisu dovoljne da se on individualizuje i pronađe, automatskim putem se, uz pomoć računara, dolazi do grupe potencijalno traženih osoba. Često se na osnovu raspoloživih karakteristika i obeležja tražene osobe, do kojih se dolazi uobičajenim istražnim postupcima, sačinjava tzv. „autorski profil" (profil tražene osobe),[6] koji se zatim unosi u odgovarajuće, prikladne baze podataka. Osobe iz takvih baza podataka, čije se karakteristike poklapaju sa karakteristikama traženog lica, na osnovu kojih je i urađen autorski profil, automatski se izdvajaju iz jedinstvene baze i kasnije detaljno proveravaju.

U martu 2004. godine prihvaćen je predlog nemačkog ministra unutrašnjih poslova da se raster pretrage počnu koristiti u celoj Evropskoj uniji u borbi protiv organizovanog terorizma.[7] Aprila 2006. godine Savezni Ustavni sud je, na osnovu žalbe marokanskog studenta koji je lišen slobode zato što je, nakon događaja od 11. septembra 2001. godine, raster pretragom definisan kao potencijalni terorista, ograničio primenu raster pretraga samo na slučajeve postojanja „konkretne opasnosti" za bezbednost Nemačke ili život njenih građana.[8]

Izmenama nemačkog Zakona o krivičnom postupku iz 1992. godine, kao posebna dokazna radnja je u krivični postupak uvedeno kompjutersko sravnjivanje i prosleđivanje podataka za elektronsku obradu.[9] Prema odredbama člana 98a ZKP-a, u slučaju da postoji dovoljno činjenično uporište da je izvršeno krivično delo iz oblasti nedozvoljenog prometa opojnih droga ili oružja, falsifikovanja novca ili znakova za vrednost, iz oblasti zaštite države, opšte opasnih krivičnih dela, protiv života i tela, seksualnih ili ličnih sloboda, iz zanata ili navike, od strane člana bande ili na drugi način organizovanog učinioca, dozvoljeno je da se uzeti lični podaci, koji se u odnosu na učinioca sa verovatnoćom podudaraju sa znacima i podacima koji se ispituju, kompjuterski sravne radi isključenja lica koja ne podležu sumnji ili radi utvrđenja koja lica ispunjavaju bitna obeležja za dalje vođenje istrage. Ova mera se može narediti samo ako se utvrđivanje stvarnog stanja stvari ili boravišta učinioca u konkretnom slučaju na drugi način teško može sprovesti, ili se očekuje da će to biti znatno otežano. Radi ostvarenja svrhe navedene mere, organ koji prikuplja podatke je dužan da organu krivičnog gonjenja sredi i prosledi one

6 Tako npr. sledeće karakteristike mogu konstruisati profil potencijalnog člana Ruske mafije u Nemačkoj: građanin države bivšeg SSSR-a, nema državljanstvo ili prebivalište u Nemačkoj, uzima učešće u akcijama domaćih kompanija ili kupovini nekretnina u Nemačkoj po izuzetno visokim cenama itd.

7 Geschichte der Rasterfahndung in Deutschland; Internet: http://de.wikipedia.org/wiki/Rasterfahndung

8 Ibid.

9 *Strafprozeßordnung*; Internet: http://dejure.org/gesetze/StPO

podatke koji su nužni za sravnjivanje, a na njegov zahtev može pružiti i pomoć organu koji vrši sravnjivanje. U slučaju da se podaci koje treba sravniti ne mogu bez većih troškova izdvojiti od drugih podataka, tada će se na osnovu naredbe dostaviti zajedno sa njima, pri čemu korišćenje ovih drugih nije dopušteno. Član 98b predviđa da sravnjivanje podataka može biti naređeno samo od strane istražnog sudije, a u slučaju postojanja opasnosti od odlaganja to može učiniti i državni tužilac, u kom slučaju njegovu naredbu u roku od tri dana mora potvrditi sud. Naredba mora biti u pisanom obliku i određivati ko je obavezan da vrši prosleđivanje podataka, pri čemu sam obim podataka mora biti sveden na nužne potrebe konkretnog slučaja. Nije dopušteno prosleđivanje onih podataka čijoj se upotrebi protive posebni savezni ili odgovarajući državni propisi, a prosleđeni podaci se po završetku sravnjivanja neizostavno moraju vratiti. Lični podaci koji se odnose na druge činjenice moraju se brisati čim postanu nepotrebni za krivični postupak, a oni podaci do kojih se došlo sravnjivanjem ličnih podataka mogu u dokazne svrhe u drugom krivičnom postupku biti upotrebljeni samo ako se prilikom njihovog korišćenja dođe do saznanja da su neophodni za razjašnjenje nekog od krivičnih dela kod kojih se mera automatskog sravnjivanja i inače može primeniti. Prema članu 98c dopušteno je da se, radi razjašnjenja krivičnog dela, krivičnog gonjenja, izvršenja izrečene kazne, otklanjanja opasnosti ili utvrđivanja boravišta nekog lica koje se goni radi sprovođenja krivičnog postupka, lični podaci iz jednog krivičnog postupka mašinski sravne sa podacima iz drugog postupka, pri čemu se ne dira u posebne savezne ili odgovarajuće državne zakonske propise kojima se reguliše upotreba takvih podataka.

Pored navedenih odredbi koje se odnose na raster pretrage (tj. sravnjivanje, upoređivanje podataka), nemački ZKP u članu 163d propisuje i meru prikupljanja podataka radi elektronske obrade (*Schleppnetzfahndung*), koja se u teoriji naziva i kompjuterskom vrškom.[10] Njena sadržina je da se, u slučaju postojanja određenih činjenica koje opravdavaju sumnju da je izvršeno određeno, u ZKP-u taksativno navedeno krivično delo, pri graničnoj policijskoj kontroli ili ličnoj kontroli mogu prikupljati podaci o identitetu nekog lica i okolnostima koje su od značaja za razjašnjenje krivičnog dela i hvatanje učinioca, uključujući i podatke do kojih se dolazi uvidom u pasoš i druga dokumenta, a zatim takvi podaci unositi u elektronske baze i upoređivati. Sprovođenje ove mere, odnosno prikupljanje podataka o licima, može narediti samo sud, a u slučaju opasnosti od odlaganja i državni tužilac, s tim što njegova naredba u roku od tri dana mora biti sudski verifikovana. Naredba o prikupljanju podataka se donosi pismeno i u njoj se moraju tačno navesti sva poznata lična obeležja i osobine lica osumnjičenog za izvršenje određenog krivičnog dela. Naredba mora biti prostorno ograničena, kao i vremenski na tri meseca, uz mogućnost produženja za još tri meseca. Podaci o kontrolisanim licima se brišu odmah nakon prestanka potrebe za njima u krivičnom postupku, a nije

10 Feješ, I., Savremeni kriminalitet i dokazno pravo, Novi Sad, 2002, str. 90-94.

dopušteno ni skladištenje podataka duže od tri meseca od isteka roka za sprovođenje mere. O brisanju podataka se obaveštava državno tužilaštvo. Podaci prikupljeni ovom merom mogu se koristiti samo za potrebe krivičnog postupka, a upotreba u druge svrhe je dozvoljena samo kada se ukaže potreba da se njihovim korišćenjem dođe do saznanja ili razjašnjenja nekog drugog krivičnog dela, ili kada su takvi podaci potrebni za pronalaženje lica za kojim se traga, utvrđivanje mesta boravišta lica za kojim se traga ili drugog lica za potrebe krivičnog postupka, ili radi izvršenja kazne.

Dakle, suština kompjuterske vrške je da se na osnovu pisane naredbe suda, pri graničnoj ili ličnoj kontroli od strane policije, izdvajaju i u posebnu bazu unose i čuvaju podaci o licima čije se određene karakteristike poklapaju sa obeležjima i osobinama navedenim u naredbi, a koje su poznate istražnim organima i vezuju se za osumnjičenog kao mogućeg izvršioca. Na taj način se formira posebna, specifična elektronska kartoteka lica za konkretan slučaj i za određeno vreme, čijom pretragom i analizom iste može biti stvorena slika o kretanju traženog lica, izuzetno i njegov identitet.

Kada je reč o Srbiji, računarsko pretraživanje podataka je u naše procesno zakonodavstvo uvedeno ZKP-om iz 2006. godine, u okviru glave VIII koja se odnosila na posebne dokazne radnje. To je i razumljivo, s obzirom na činjenicu da se ova istražna tehnika u teoriji i zakonodavstvima širom sveta tretira kao specijalna (posebna), što za sobom povlači i njen *ultima ratio* karakter i suženi opseg primene, u dokazivanju teških krivičnih dela. Kako je istaknuto u obrazloženju predloga ZKP-a iz 2006. godine, reč je o potpuno novoj dokaznoj radnji kod nas, koja u razvijenijim državama ima veliki značaj, naročito u vezi sa izraženom kompjuterizacijom ličnih i drugih podataka, te velikim mogućnostima koje ti podaci pružaju u prikupljanju dokaza. U tom smislu, prema članu 155. ZKP-a, automatsko računarsko pretraživanje ličnih i drugih sa njima povezanih podataka i njihova elektronska obrada se mogla preduzeti ako su postojali osnovi sumnje da je učinjeno: 1) krivično delo protiv ustavnog uređenja i bezbednosti Srbije; 2) krivično delo protiv čovečnosti i drugih dobara zaštićenih međunarodnim pravom; 3) krivično delo organizovanog kriminala; 4) krivično delo protiv polne slobode; 5) krivično delo protiv bezbednosti računarskih podataka (uvedeno izmenama i dopunama ZKP-a iz 2006. godine), 6) ubistvo, teško ubistvo, razbojništvo, razbojnička krađa, falsifikovanje novca, pranje novca, falsifikovanje i zloupotreba platnih kartica (uvedeno izmenama i dopunama ZKP-a iz 2006 godine), neovlašćena proizvodnja i stavljanje u promet opojnih droga, nedozvoljeno držanje oružja i eksplozivnih materija, trgovina ljudima, trgovina decom radi usvojenja, davanje i primanje mita, zloupotreba službenog položaja, ucena, iznuda i otmica. Ova dokazna radnja se izuzetno mogla odrediti i ako su osobite okolnosti ukazivale da se priprema neko od navedenih krivičnih dela, pri čemu se njegovo izvršenje 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 i

imovinu veće vrednosti. Njena sadržina je bila u automatskom pretraživanju već pohranjenih ličnih i drugih, sa njima neposredno povezanih podataka i njihovom automatskom poređenju sa podacima koji se odnose na krivično delo i lice koje se osnovano može dovesti u vezu sa tim krivičnim delom, da bi se na takav 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 proizlaze osnovi sumnje.

Računarsko pretraživanje podataka je prema ZKP-u iz 2006. godine naređivao istražni sudija na predlog javnog tužioca, a u slučaju postojanja okolnosti koje ne trpe odlaganje javni tužilac je mogao sam doneti naredbu, koju je u roku od 24 časa morao podneti istražnom sudiji na potvrđivanje. Ako istražni sudija ne bi potvrdio takvu naredbu u roku od 24 časa od kada je primio, ona se bez odlaganja stavljala van snage, a svi prikupljeni podaci su se odmah morali uništiti pod nadzorom istražnog sudije i javnog tužioca. Naredba kojom se određivala ova dokazna radnja sadržala je zakonski naziv krivičnog dela, određivanje podataka koje je potrebno automatski prikupljati i prosleđivati, određivanje državnog organa koji je dužan da automatski prikuplja tražene podatke i dostavlja ih javnom tužiocu i policiji, te obim posebne dokazne radnje i vreme njenog trajanja. Računarsko pretraživanje podataka je moglo trajati najviše tri meseca, a iz važnih razloga njeno trajanje se moglo produžiti za još tri meseca. Radnju je realizovala 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 do kojih se došlo primenom ove radnje su se pod nadzorom javnog tužioca i istražnog sudije uništavali, u slučaju da u roku od šest meseci od završetka njenog sprovođenja ne bude pokrenut krivični postupak.

Izmenama i dopunama ZKP-a iz 2009. godine, dokazna radnja automatskog računarskog pretraživanja ličnih i drugih sa njima povezanih podataka zadržata je ZKP-u iz 2001. godine, u okviru mera organa gonjenja za otkrivanje i dokazivanje krivičnih dela iz člana 504a ZKP-a, pri čemu treba napomenuti da je ona u velikoj meri regulisana na sličan način kao i u ZKP-u iz 2006. godine. Tako član 504lj ZKP-a propisuje da se automatsko računarsko pretraživanje ličnih i drugih sa njima povezanih podataka i njihova elektronska obrada može preduzeti ako postoje osnovi sumnje da je učinjeno krivično delo iz člana 504a ovog zakonika, ako se na drugi način ne mogu prikupiti dokazi za krivično gonjenje ili bi njihovo prikupljanje bilo znatno otežano. Mera se izuzetno može odrediti i ako postoje osnovi sumnje da se priprema neko od krivičnih dela iz člana 504a ovog zakonika, a okolnosti slučaja ukazuju da se na drugi način delo ne bi moglo otkriti, sprečiti ili dokazati, ili bi to izazvalo nesrazmerne teškoće ili veliku opasnost. Mera se sastoji u automatskom pretraživanju već pohranjenih ličnih i drugih, sa njima neposredno povezanih podataka i u njihovom automatskom poređenju sa podacima koji se odnose na krivično delo iz člana 504a ovog zakonika i na osumnjičenog, da

bi se kao mogući osumnjičeni isključila lica u pogledu kojih ne postoji verovatnoća da su povezana sa krivičnim delom. U tom smislu, može se zaključiti da se ova mera, s obzirom na navedeno zakonsko rešenje, ne može koristiti u cilju identifikacije osumnjičenih lica, odnosno potencijalnih učinilaca, već samo da bi se kao mogući osumnjičeni eliminisala ona lica u pogledu kojih, nakon pretrage i upoređivanja, ne postoji verovatnoća da su povezana sa krivičnim delom povodom čijeg se izvršenja, odnosno sprečavanja izvršenja mera realizuje.[11] Automatsko računarsko pretraživanje ličnih i drugih sa njima povezanih podataka i njihovu elektronsku obradu naređuje istražni sudija, na predlog javnog tužioca, pri čemu sama naredba istražnog sudije sadrži zakonski naziv krivičnog dela iz člana 504a ovog zakonika, opis podataka koje je potrebno automatski prikupiti i proslediti, označenje državnog organa koji je dužan da automatski prikuplja tražene podatke i dostavlja ih javnom tužiocu i organu unutrašnjih poslova, obim posebne dokazne radnje i vreme njenog trajanja. Primena mere može trajati najviše šest meseci, a iz važnih razloga njeno trajanje se može produžiti za još tri meseca. Meru sprovode organi unutrašnjih poslova, Bezbednosno-informativna agencija, Vojno-bezbednosna agencija, organi carinske službe ili drugi državni organi, odnosno druga pravna lica koja na osnovu zakona vrše određena javna ovlašćenja.

Ako javni tužilac ne pokrene krivični postupak u roku od šest meseci od dana kada se upoznao sa podacima prikupljenim primenom mere, ili ako izjavi da ih neće koristiti u postupku, odnosno da protiv osumnjičenog neće zahtevati vođenje postupka, istražni sudija će postupiti u skladu sa odredbom člana 504z stav 3. ovog zakonika.[12]

U bliskoj vezi sa računarskim pretraživanjem podataka nalaze se i odredbe Zakona o policiji, prema kojim policija prikuplja, obrađuje i koristi lične podatke, obezbeđuje zaštitu i vodi evidencije o ličnim i drugim podacima na čije je prikupljanje ovlašćena, radi sprečavanja i otkrivanja krivičnih dela i prekršaja i pronalaženja njihovih učinilaca. Zakonom je navedeno da policija vodi sledeće evidencije: 1) lica kojima je po bilo kojem osnovu ograničena ili oduzeta sloboda (dovođenje, zadržavanje, ograničenje kretanja, lišavanje slobode i drugo); 2) lica za koje postoje osnovi sumnje da su učinila krivična dela i prekršaje; 3) učinjenih krivičnih dela za koja se goni po službenoj dužnosti, prekršaja i lica oštećenih tim delima; 4) učinjenih krivičnih dela nepoznatih učinilaca za koja se goni po privatnoj tužbi; 5) traženih lica i predmeta i lica kojima je zabranjen ulazak u zemlju; 6) provera iden-

11 Reč je o tzv. negativnim raster pretragama.

12 U tom smislu, ako javni tužilac ne pokrene krivični postupak u roku od šest meseci od dana kada se upoznao sa materijalom dobijenim primenom mere, ili ako izjavi da ga neće koristiti u postupku, odnosno da protiv osumnjičenog neće zahtevati vođenje postupka, istražni sudija će doneti rešenje o uništenju prikupljenog materijala. O donošenju rešenja istražni sudija može obavestiti lice prema kome je sprovođena mera, ukoliko je u toku sprovođenja mere utvrđen njegov identitet. Materijal se uništava pod nadzorom istražnog sudije, o čemu istražni sudija sastavlja zapisnik.

titeta lica; 7) lica nad kojima je sprovedeno utvrđivanje identiteta, daktiloskopiranih lica, fotografisanih lica i DNK analiza; 8) operativnih izveštaja, operativnih izvora saznanja i lica pod posebnom policijskom zaštitom; 9) primenjenih operativnih i operativno-tehničkih sredstava i metoda; 10) događaja; 11) upotrebljenih sredstava prinude; 12) pritužbi. Brojčani podaci o krivičnim delima, prijavljenim i oštećenim licima, kao i ostali podaci mogu se koristiti u statističke i analitičke svrhe u Ministarstvu, a mogu se i dati na korišćenje nadležnim stručnim i naučnim ustanovama za potrebe naučno-istraživačkog rada. Lični podaci mogu se dostavljati drugim organima pod uslovima da je organ koji traži podatke zakonom ili drugim propisom ovlašćen da traži i prima te podatke, da su organu koji traži podatke ti podaci neophodni za izvršavanje poslova iz njegove nadležnosti, da te podatke nije moguće pribaviti na drugi način ili ako bi njihovo pribavljanje zahtevalo nesrazmerno visoke troškove. Lični podaci mogu se dostaviti i inostranim policijskim organima i određenim međunarodnim organizacijama na njihov zahtev, u skladu sa utvrđenim pravilima o međunarodnoj policijskoj saradnji.[13]

Ono što se smatra posebno problematičnim kod raster pretraga kao istražne tehnike jeste njena sukobljenost sa pretpostavkom nevinosti, s obzirom da sve osobe izdvojene kao rezultat njene primene, a koje zadovoljavaju određene kriterijume (npr. veličina, pol, nacionalnost, imovno stanje, vlasništvo nad određenom stvari i sl.), predstavljaju osumnjičene i potencijalno tražene osobe, najčešće moguće izvršioce teških krivičnih dela. Takve osobe se dalje izlažu detaljnim proverama, od kojih u krajnjem slučaju i zavisi da li će se osumnjičenost lica „izvučenih" iz odgovarajuće baze podataka, eliminisati ili produbiti i konkretizovati. Takođe, može se reći i da je sa aspekta zaštite ljudskih prava, pre svega prava na privatnost i informaciono samoodređenje, diskutabilna mogućnost povezivanja i korišćenja podataka iz brojnih izvora i baza, sačinjenih u najraznovrsnije svrhe, u krivičnim istragama, bez obzira na preteću opasnost po pojedinca i društvo u celini od izvesnih oblika kriminalnog manifestovanja, posebno organizovanog kriminala. Zato su u bliskoj vezi sa radnjama pretraživanja, analiziranja i upoređivanja podataka, kako u svrhe suprotstavljanja kriminalu, tako i u druge svrhe, odredbe zakona koje regulišu proceduru prikupljanja, obrade, skadištenja i eksploatacije ličnih podataka, u cilju sprečavanja njihove zloupotrebe. Kod nas je to Zakon o zaštiti podatka o ličnosti[14], koji pored toga što obezbeđuje zaštitu podataka propisuje mogućnost da organ vlasti obrađuje podatke bez pristanka lica, ako je obrada neophodna radi obavljanja poslova iz svoje nadležnosti određenih zakonom ili drugim propisom u cilju ostvarivanja interesa nacionalne ili javne bezbednosti, odbrane zemlje, sprečavanja, otkrivanja, istrage i gonjenja za krivična dela,

13 Zakon o policiji reguliše i pitanje zaštite ličnih podataka (član 78), ispravljanje i brisanje ličnih podataka iz evidencija (član 79), postupanje sa podacima (član 80), rokove čuvanja ličnih i drugih podataka u evidencijama, kao i nadzor organa nadležnog za zaštitu ličnih podataka (član 82).

14 „Službeni glasnik", broj 97/2008.

ekonomskih, odnosno finansijskih interesa države, zaštite zdravlja i morala, zaštite prava i sloboda i drugog javnog interesa, a u drugim slučajevima na osnovu pismenog pristanka lica (član 13).

4. Neki kriminalistički aspekti kompjuterskog pretraživanja i upoređivanja podataka

Kompjutersko pretraživanje, analiziranje i upoređivanje podataka u kriminalističke svrhe može biti veoma raznovrsno, sa različitim očekivanjima i rezultatima primene. Jednako kao što veliki broj podataka smeštenih u odgovarajuće baze služi efikasnom obavljanju poslova javne uprave, administracije ili bankarstva, on može biti od velike koristi i u isleđivanju krivičnih dela.

Sa aspekta delatnosti suzbijanja kriminala, baze podataka se mogu podeliti na primarne i sekundarne. Primarne baze podataka su one koje se formiraju i vode prvenstveno za potrebe kriminalističkih istraga i subjekata koji ih vode, dok se pod sekundarnim smatraju one koje se organizuju i kojima se upravlja za potrebe državne uprave, u privredi ili zdravstvu, ali se u određenim slučajevima mogu koristiti i u kriminalističke svrhe. Tako se npr. u primarne baze podataka uobičajeno ubrajaju baze otisaka prstiju ili DNK profila učinilaca krivičnih dela[15], dok bi u sekundarne spadale baze podataka o novčanim transakcijama koje vode određene banke ili baze poreskih obveznika.

Faktori koji pomažu u evaluaciji relevantnosti primene *data mining* tehnika u suzbijanju kriminala kreću se u rasponu od aktivnosti iz kojih zbirke podataka rezultiraju, pa do njihovog kvaliteta (stepen nesigurnosti, preciznosti i kompletnosti). Policijske agencije i kriminalističke laboratorije sakupljaju velike količine različitih podatka, koji nastaju kao rezultat obrade brojnih kriminalnih aktivnosti.

15 INTERPOL-ova automatizovana baza podataka otisaka prstiju (AFIS) sadrži oko 90.000 otisaka prstiju prestupnika, kao i otiske sa 1.600 mesta izvršenja krivičnih dela. DNK (DNA) baze podataka se sastoje od DNK profila koji se dele na referentne profile (profili okrivljenih, osumnjičenih, oštećenih...) i profile tragova (profili dobijeni iz bioloških tragova). Prema podacima INTERPOL-a, u 2008. godini se u većini zemalja članica radila forenzička DNK analiza, 53 zemlje imaju DNK bazu podataka, dok je u 29 zemalja ona u fazi formiranja. Tako u SAD-u nacionalna baza podataka obuhvata profile više od pet miliona lica, dok je nacionalna baza podataka u Velikoj Britaniji slične veličine, uprkos manjem broju stanovnika (podaci iz 2007. godine). Na nivou INTERPOL-a postoji konsenzus o tome da bi svaka zemlja trebalo da poseduje DNK bazu podataka, te da mora postojati međunarodna saradnja na polju razmene DNK profila. Polemika postoji o tome čiji DNK profili treba da se nađu u bazama podataka. Zakonska rešenja u zemljama članicama INTERPOL-a su vrlo raznolika, od Belgije, gde se samo profili osuđenih za teška krivična dela nalaze u DNK bazi podataka, do Velike Britanije, gde se u bazi nalaze profili osumnjičenih i osuđenih za sva krivična dela i većinu prekršaja, kao i profili drugih građana, dobrovoljnih davalaca.
Nav. prema: *INTERPOL – Forensic*; Internet: http://www.interpol.int/Public/Forensic
National DNA database; Internet: http://en.wikipedia.org/wiki/National_DNA_database

Tako u okviru kriminalističke obrade lica mesta dobijeni podaci čine grupu koja se sastoji od informacija koje se tiču prikupljenog materijala fizičkog porekla (npr. biološki tragovi, tragovi oruđa, otisci prstiju, otisci obuće, zaplene ilegalnih droga). Ova vrsta podataka može biti predstavljena numerički i podložna kategorizaciji. Obeležja izdvojena iz ovih materijala često su neprecizna (načelno zbog instrumenata kojima se vrše analize i merenja), nepotpuna (fragmentarna) i nesigurna.

Uobičajeno, otkriveni i obrađeni uzorci materijala se kategorizuju u tri grupe: 1) *nekoristan uzorak* (npr. očita jasnoća sadržaja bez ikakvih proračuna ili je on irelevantan za problem koji se razmatra), 2) *koristan uzorak*, koji pruža neposrednu, značajnu informaciju sa kojom se može raditi, i 3) *obrazac koji treba tumačiti*, i koji se ne može svrstati u dve prethodne kategorije, zbog čega mora biti proučen od strane eksperata u datoj oblasti.[16]

Istraživači su razvili različite automatizovane tehnike *data mining*-a za potrebe suzbijanja kriminala, kako u oblasti lokalnih policijskih poslova, tako i na nacionalnom nivou. Tako tehnika *ekstrakcije (izdvajanja) entiteta* identifikuje obrasce iz baza podataka kao što su tekstovi, slike ili audio materijali. Koristi se za automatsku identifikaciju lica, adresa, vozila i ličnih karakteristika iz narativnih policijskih izveštaja. Ova tehnika obezbeđuje osnovne podatke za analizu kriminala, ali njena dostignuća u velikoj meri zavise od dostupnosti velike količine čistih ulaznih podataka. *Klaster tehnike* sistematizuju podatke u grupe sa sličnim karakteristikama, kako bi se maksimizirala ili minimizirala sličnost podataka unutar određene grupe – npr. za identifikovanje osumnjičenih koji krivična dela izvršavaju na sličan način ili za razlikovanje kriminalnih grupa koje pripadaju različitim bandama. *Otkrivanje pravila asocijacije* pronalazi grupe podataka koje se često javljaju u jednoj bazi podataka, a obrasci njihovog javljanja definišu se kao zakonomernosti. Ova tehnika se koristi za otkrivanje upada u kompjuterske mreže, kako bi se izvela određena pravila asocijacije iz istorije interakcije među korisnicima. Istražitelji takođe mogu primeniti ovu tehniku na profilisanje lica koja vrše upade u mreže, kako bi pomogli u otkrivanju eventualnih napada na mrežu.

Otkrivanje obrasca sekvenci (ili obrasca nizova) pronalazi sekvence koje se često javljaju u jednom setu transakcija koje su se dogodile u različito vreme. Ukazivanje na skrivene obrasce korisno je za analizu zločina, ali da bi se dobili smisleni rezultati potrebna je bogata i visoko struktuirana baza podataka. *Detekcija devijacije* koristi određene mere za proučavanje podataka koji se upadljivo razlikuju od ostalih podataka. Istražitelji mogu da primene ovu tehniku za otkrivanje prevara, upada u mrežne sisteme i druge analize kriminala. Međutim, ovakve aktivnosti nekada na prvi pogled mogu izgledati i uobičajene, što otežava identifikaciju odstupajućih podataka. *Klasifikacija* pronalazi zajednička svojstva između različitih kriminalnih entiteta i organizuje ih u unapred definisane klase. Ova tehni-

16 Terrettaz-Zufferey A. L. et al.: Assesment of Data Mining Methods for Forensic Case Data Analysis.- U: *Varstvoslovje*, Fakulteta za varnostne vede, Ljubljana, 2006, str. 350-354.

ka koristi se za identifikaciju izvora tzv. spam poruka u elektronskoj pošti, na osnovu lingvističkih obrazaca i strukturalnih odlika pošiljaoca. Često korišćena za predviđanje kriminalnih trendova, klasifikacija može smanjiti vreme koje je potrebno za identifikaciju kriminalnih entiteta.

Komparativne tehnike data mining-a porede parove tekstualnih polja u bazama podataka i izračunavaju sličnosti između zapisa. Ove tehnike mogu da otkriju lažne informacije kao što su imena, adrese i brojevi socijalnog osiguranja. Istražitelji mogu da koriste komparaciju za analiziranje tekstualnih podataka, ali ove tehnike često zahtevaju intenzivna proračunavanja. *Analiza socijalne mreže* opisuje ulogu i interakcije između tačaka granjanja (čvorova) unutar jedne konceptualne mreže. Ova tehnika se može koristi ako bi se konstruisale mreže koje ilustruju uloge pojedinih kriminalaca, protok materijalnih i nematerijalnih dobara i informacija, kao i veze između ovih entiteta. Dalja analiza može otkriti kritične uloge i podgrupe, kao i ranjivost, odnosno slabosti unutar mreže.[17]

Jedan od aspekata primene tehnika *data mining*-a u kriminalističke svrhe je pri analiziranju zaplenjenih droga, kako bi se što potpunije definisalo stanje narkotržišta.[18] U ovom slučaju se metode prepoznavanja uzoraka droga sistematski testiraju na mnoštvu uzoraka zaplenjenog heroina i kokaina, kako bi se otkrile eventualne pravilnosti koje mogu dati informacije vezane za obim i razvoj ilegalne trgovine. Klasični algoritmi, kao što je analiza glavnih komponenti i različiti grupišući i klasifikacioni algoritmi, uspešno se mogu primeniti na heroinske baze podataka. U osnovi, proces razređivanja i mešanja heroina se događa na različitim nivoima nelegalne trgovine, ali se najčešće realizuje pri kraju procesa distribucije, kako bi količina čistog heroina bila što je moguće manja, odnosno zarada veća. Zato su supstance za mešanje sa heroinom od posebnog značaja za lakše razumevanje lokalne mreže trgovine. Prisustvo ili odsustvo ovih supstanci sistematski se detektuje laboratorijskim tehnikama hemijske analize. Jedan te isti uzorak zaplenjenog heroina istovremeno može sadržati različite supstance (šećer, mleko, puding ili kakao u prahu, brašno, paracetamol i sl.), čija određena kombinacija i odnos može biti pokazatelj različitih nivoa lanca snabdevanja. Stoga dinamika javljanja ovih kombinacija može biti dobar indikator stanja i razvoja lokalnog tržišta, uz mogućnost prikazivanja pomoću kombinatorne analize i teorije grafikona. Baza podataka kreirana za ove potrebe trebala bi da sadrži sledeće varijable:[19]

17 Chen H. et al.: Crime Data Mining: A General Framework and Some Examples.- U: *Computer*, Published by the IEEE Computer Society, April 2004, str. 50-56.
Prestupnici često razvijaju kriminalna udruženja – mreže u okviru kojih formiraju grupe ili timove radi vršenja različitih nezakonitih delatnosti. Primena data mining tehnika se u ovim slučajevima sastoji u identifikovanju podgrupa i ključnih članova u tim mrežama, kao i proučavanju obrazaca interakcije u cilju razvijanja delotvorne strategije za neutralisanje tih mreža.

18 Ratle F. et al.: Learning Manifolds in Forensic Data.- U: Lecture Notes in Computer Science, Heidelberg, 2006, str. 894-903; Internet:
http://resources.metapress.com/pdf-preview.axd?code=fkgv59020149w601&size=largest

19 Terrettaz-Zufferey A. L. et al., op. cit., str. 353.

– lokaciju i vremenski period zaplene;
– prisustvo/odsustvo supstanci koje služe za mešanje;
– kombinacije supstanci za mešanje.

Kada je reč o primeni metoda kompjuterskog upoređivanja podataka u kriminalistici, polaznu osnovu čine raspoloživa obeležja određene osobe ili stvari i vrsta događaja (krivično delo, prekršaj, postupak utvrđivanja vlasništva i sl.) povodom kojeg se upoređivanje i preduzima. Na osnovu njih se određuju baze podataka u kojima se mogu očekivati komplementarni podaci vezani za ta lica, stvari ili događaje. Čovekova obeležja, odnosno karakteristike, mogu se odnositi na njenovu ličnost, shvaćenu u psihofizičkom (pol, starost, otisak prsta, DNK profil, obolenje itd.), odnosno društvenom smislu (nacionalnost, državljanstvo, političko opredeljenje, bankovni račun, bračno stanje, članstvo u nekom udruženju itd.). Takođe, sama obeležja mogu biti takva da su svojstvena samo jednom licu, tako da se njihovim povezivanjem nedvosmisleno utvrđuje identitet osobe, ili mogu biti zajednička za jednu širu ili užu grupu lica, koja se nakon pretrage i upoređivanja izdvajaju iz baze podataka i dalje obrađuju. U tom smislu, možemo razlikovati dve vrste kopjuterskog upoređivanja podataka:

1. upoređivanje podataka koje za rezultat ima utvrđivanje identiteta lica (npr. pretraživanjem DNK profila uzorka krvi sa mesta ubistva kroz bazu DNK profila učinilaca krivičnih dela ili otiska prsta NN leša kroz bazu ličnih karti građana);
2. pretraživanje podataka koje za rezultat ima određivanje kruga, odnosno grupe lica (npr. pretraživanje kroz bazu podataka vozila registrovanih u određenom registarskom području, s ciljem izdvajanja vozila određene marke, tipa i boje karoserije, odnosno vlasnika takvih vozila, povodom određene saobraćajne nezgode).

Danas policijske službe širom sveta koriste automatizovane sisteme za identifikaciju prestupnika preko otisaka prstiju (*Automatic Fingerprint Identification Systems* – AFIS). U ovim slučajevima reč je o primarnim bazama podataka, s obzirom na činjenicu da su takve evidencije upravo i sačinjene u istražne svrhe.[20] Međutim, u

20 Ruski kompjuterizovani sistem za identifikaciju lica putem otisaka prstiju (ADIS Papilon) oformljen je 1995. godine i predstavlja prvi automatizovani informacioni sistem otisaka prstiju u Rusiji. U proteklom periodu su, uz pomoć Papilona, automatskom komparacijom otisaka iz baze i onih nađenih na licu mesta, na hiljade krivičnih predmeta bili gotovo odmah rešeni. Tako se npr. u aprilu 2007. godine desilo oružano razbojništvo nad vozačem teretnog motornog vozila KAMAZ od strane više nepoznatih lica. Tokom uviđaja na licu mesta pronađen je otisak prsta koji je već bio registrovan u bazi Papilon. Prestupnik je brzo identifikovan i pritvoren, da bi kasnije priznao saučesništvo u zločinu. Još jedan ilustrativan slučaj dogodio se pre nekoliko godina, u Jekaterinburgu, gde su dve starije žene ubijene u svom stanu. Istražitelji su na licu mesta uspeli da pronađu tragove otisaka ruku. U roku od nekoliko sati, pretragom kroz bazu podataka Papilon, došlo se do osobe koja je u prethodnom periodu bila daktiloskopirana. Agenti su osumnjičenog pronašli u jednom selu – bio je iznenađen i uplašen, nije mogao da razume kako ga je policija našla samo dan nakon izvršenog zločina, daleko od lica mesta.
Navedeno prema: Ministry of the Interior of Russian Federation: Service of verity;
Internet: http://www.eng.mvd.ru/news/13795/

poslednje vreme se počinju formirati takve baze otisaka prstiju ili drugih biometrijskih obeležja koje obuhvataju širok opseg stanovništva, bez nekog posebnog kriterijuma, osim npr. životnog doba ili ulaska na teritoriju određene države.[21] U prvom slučaju povod je izdavanje takvih identifikacionih dokumenata građana (lična karta, pasoš) koja u sebi sadrže, između ostalog, i neke biometrijske karakteristike, najčešće fotografiju lica i njegov potpis,[22] a u drugom službeni, turistički ili bilo koji drugi dolazak u državu koja zahteva određenu proceduru.

Sa kriminalističkog aspekta poseban značaj ima upoređivanje podataka u slučajevima kada se raspolaže obeležjima materija pronađenih na mestu kriminalnog događaja ili drugom mestu i koji su (ili se pretpostavlja da su) u vezi sa krivičnim delom, sa obeležjima materija te vrste koje se, za potrebe komparacije, uzimaju od osumnjičenih lica. Na taj način se, u slučaju komplementarnosti ovih obeležja, jednostavnom procedurom utvrđuje njihova veza, ili u slučaju odsustva podudarnosti, eliminacija osumnjičenih lica.

Može se reći da uspeh kompjuterskog upoređivanja podataka u krivičnim istragama u presudnoj meri zavisi od raspoloživosti karakteristika (rastera, obeležja) lica i njihovih svojstava. U tom smislu, ako se raspolaže sa malo karakteristika, manja je i verovatnoća da će pretraga uspeti. Sa druge strane, ako su karakteristike previše uopštene, može se pojaviti veliki broj lica koja će se upoređivanjem izdvojiti i koja treba dalje kriminalistički obraditi, što će umnogome povećati troškove istrage. Zato neki autori pod veliki znak pitanja stavljaju samu efikasnost ove dokazne radnje.[23]

21 Tako program US-VISIT (United States Visitor and Immigrant Status Indicator Technology) zahteva od svih posetilaca SAD-a da se pre ulaska u zemlju fotografišu i daju otisak prsta. Ovi podaci se ne koriste samo za verifikaciju putnika pri ulasku u SAD, već su povezani sa više od 20 drugih baza podataka Vlade. Cilj je da se na ovaj način u značajnoj meri spreči ulazak u zemlju traženih, opasnih lica, koja se pri tome koriste lažnim identitetom. Slično US-VISIT-u, i u Japanu se sprovodi J-VIS program.
Više u: Homeland Security: Fact Sheet - Expansion of US-VISIT Procedures to Additional Travelers;
Internet: http://www.dhs.gov/files/programs/gc_1231972592442.shtm
United States Visitor and Immigrant Status Indicator Technology;
Internet::
http://en.wikipedia.org/wiki/United_States_Visitor_and_Immigrant_Status_Indicator_Technology

22 Takva situacija je prisutna i u Republici Srbiji, donošenjem Zakona o ličnoj karti, prema kome ovaj osnovni identifikacioni dokument sadrži, između ostalog, i fotografiju lica, potpis i otisak prsta. Na taj način će MUP, tokom postupka izdavanja novih ličnih karti, oformiti takvu bazu podataka u kojoj će se naći biometrijska obeležja svakog građanina Srbije starijeg od 16 godina, izuzetno i mlađeg.

23 U Nemačkoj je 2004. godine iznet podatak da je pretraga čak 8,3 miliona podataka rezultirala samo jednom istragom, što je dalo snažan argument kritičarima u njihovom stavu da raster pretrage u stvari predstavljaju čist promašaj. Navedeno prema Rasterfahndung - Kritik; Internet:
http://de.wikipedia.org/wiki/Rasterfahndung

Literatura

Berry, M., Linoff G., Mastering Data Mining, New York, 2000.

Fayyad, U. M. et al.: From Data Mining to Knowledge Discovery:An Overview. – U: Advances in Knowledge Discovery and Data Mining, Cambridge, 1996; Internet: http://www.daedalus.es/fileadmin/daedalus/doc/MineriaDeDatos/fayyad96.pdf

Clarke, R., Dataveillance By Governments: The Technique of Computer Matching. – U: Information Technology & People, December 1994.
Internet: http://www.rogerclarke.com/DV/MatchIntro.html

Grötker, R., Eene meene muh: Rasterfahndung in Deutschland – Teil 1;
Internet: http://www.heise.de/tp/r4/artikel/11/11411/1.html

Geschichte der Rasterfahndung in Deutschland;
Internet: http://de.wikipedia.org/wiki/Rasterfahndung

Strafprozeßordnung; Internet: http://dejure.org/gesetze/StPO

Feješ, I., Savremeni kriminalitet i dokazno pravo, Novi Sad, 2002.

INTERPOL – Forensic; Internet: http://www.interpol.int/Public/Forensic

Terrettaz-Zufferey A. L. et al.: Assesment of Data Mining Methods for Forensic Case Data Analysis.- U: Varstvoslovje, Fakulteta za varnostne vede, Ljubljana, 2006, str. 350-354.

Chen H. et al.: Crime Data Mining: A General Framework and Some Examples.- U: Computer, Published by the IEEE Computer Society, April 2004, str. 50-56.

Ratle F. et al.: Learning Manifolds in Forensic Data.- U: Lecture Notes in Computer Science, Heidelberg, 2006, str. 894-903; Internet:
http://resources.metapress.com/pdf-preview.axd?code=fkgv59020149w601&size=largest

Ministry of the Interior of Russian Federation: Service of verity;
Internet: http://www.eng.mvd.ru/news/13795/

Homeland Security: Fact Sheet - Expansion of US-VISIT Procedures to Additional Travelers;
Internet: http://www.dhs.gov/files/programs/gc_1231972592442.shtm
United States Visitor and Immigrant Status Indicator Technology; Internet:
http://en.wikipedia.org/wiki/United_States_Visitor_and_Immigrant_Status_Indicator_Technology

Rasterfahndung – Kritik; Internet: http://de.wikipedia.org/wiki/Rasterfahndung

Dr Darko Marinković,
Docent, The Academy of Criminalistic and Police Studies, Belgrade
Dr Zoran Đurđević,
Docent, The Academy of Criminalistic and Police Studies, Belgrade

COMPUTER SEARCH AND DATA COMPARISON IN THE CRIME DETECTION AND PROVIDING EVIDENCE

Collection of various information about citizens and their storage in appropriate data bases are realities of modern societies. Ever-increasing amount of that information has triumphed over human capacity to deal and analyse them in traditional manner requiring development of computerised methods. Being widely applied in public administration and economy for many years, computer search and data comparison has not been sufficiently exploited in criminalistics and forensic. Police agencies and forensic laboratories collect a significant amount of various data resulting from the analysis of numerous criminal activities. A success of the automatic search and comparison in criminal investigations essentially depends on the availability and characteristics of the existing data about persons, objects or events. From 2006 onwards, automatic computer search of personal and other related data has become available as particular evidential act within Serbian criminal legislation which was a decisive motive for writing this article.

Key words: *Computer research and data comparison, data mining, computer matching, raster research, surveillance of persons through data, forensic data bases, special investigative techniques.*