UDK: 343.98

Denis Vidaković, struč. spec. crim.,
PU zagrebačka
Nikola Protrka, univ. spec. inf.,
Visoka policijska škola u Zagrebu

KRIMINALISTIČKA ANALIZA PODATAKA MOBILNE I FIKSNE TELEFONIJE U RAZRJEŠAVANJU KAZNENIH DJELA

U radu se objašnjavaju praktični aspekti korištenja podataka, prikupljenih korištenjem policijske ovlasti provjere uspostavljanja elektroničke komunikacije propisane Zakonom o policijskim poslovima i ovlastima, te provođenjem dokazne radnje provjere uspostavljanja telekomunikacijskog kontakta propisane odredbama Zakona o kaznenom postupku.

Poseban naglasak se stavlja na jednostavnije, svakodnevne aspekte kriminalističke analize podataka koje možemo pronaći u „izlistu telefona", kao i na korištenje analitičkih programa i alata. Razjasniti će se i pojmovi čije je razumijevanje izuzetno bitno pri tumačenju podataka iz „izlista", kao što su IMEI broj, IMSI broj, ćelija, lokacija, IP adresa i dr.

U radu će se obraditi i pravni izvori koji uređuju ovo područje, gdje je dana ovlast policiji u prikupljanju podataka, kao i obveze davatelja telekomunikacijskih usluga po pitanju davanja pristupa podacima kojima raspolažu.

Ključne riječi: *izlist telefona, telekomunikacijski kontakt, IMEI, ćelija, operater.*

1. UVOD

U posljednjih 20-ak godina u svijetu je došlo do rapidnog razvoja telekomunikacijskih tehnologija, zbog čega je informacija i komunikacija na daljinu postala globalno dostupna. Takav razvoj komunikacijskih tehnologija u značajnoj mjeri doprinio je razvoju i širenju svih oblika kriminala, posebice organiziranog, omogućujući nositeljima takvih aktivnosti lakšu komunikaciju i koordinaciju na daljinu.

Suočena sa brzim razvojem telekomunikacijskih tehnologija, policija već godinama, kako pravnim normama koje uređuju to područje, tako i razvojem

tehničkih metoda i alata koji se koriste pri nadzoru komunikacija pokušava održati korak sa novim tehnologijama i načinima komunikacije na području mobilne i fiksne telefonije.

Konstantan razvoj telekomunikacijskih tehnologija nažalost nije jedina stavka koja u određenoj mjeri ograničava sposobnost policije u nadzoru komunikacija koje koriste počinitelji raznih oblika kriminala. Cilj ovog rada je prikazati na koji način se najprikladnije i najefikasnije, mogu koristiti i tumačiti podaci prikupljeni tzv. „izlistima“ telefonskih poziva, koji se koriste u gotovo svim kriminalističkim istraživanjima. Pri tome će naglasak biti stavljen na one radnje koje policijski službenici koji provode određeno kriminalističko istraživanje mogu sami provesti, bez korištenja kompliciranih alata i resursa kriminalističke analitike.

2. PRAVNI TEMELJ PRIKUPLJANJA PODATAKA

Pribavljanje podataka o telekomunikacijskom prometu određenog telekomunikacijskog sredstva, odnosno telekomunikacijske adrese ili kako se to često u praksi naziva „izlista telefona“, definiran je člankom 68. Zakona o policijskim poslovima i ovlastima[1] (dalje u tekstu ZOPPO), kao ovlast „provjere uspostavljanja elektroničke komunikacije“. Navedeni članak definira kako policijski službenik može od davatelja telekomunikacijskih usluga zatražiti provjeru istovjetnosti, trajanja i učestalosti kontakta određenih elektroničkih komunikacijskih adresa i to onda kada je to potrebno radi:

- sprečavanja opasnosti,
- sprečavanja nasilja,
- traganja za osobama i predmetima,
- sprečavanja kaznenog djela koje se progoni po službenoj dužnosti i
- otkrivanja kaznenog djela koje se progoni po službenoj dužnosti.

Osim toga, Zakonom o policijskim poslovima i ovlastima je definirano i kako ovlast provjere uspostavljanja telekomunikacijskog kontakta uz provjeru istovjetnosti, trajanja i učestalosti kontakta određenih telekomunikacijskih adresa može obuhvaćati i utvrđivanje mjesta na kojima se nalaze osobe koje uspostavljaju telekomunikacijski kontakt, te identifikacijske oznake uređaja. Navedene ovlasti daju policiji odličan alat u razrješavanju kaznenih djela te je time omogućeno određivanje lokacije mobilnog telefonskog uređaja u realnom vremenu.

U praksi navedena ovlast istražiteljima pomaže u identifikaciji počinitelja kaznenih djela, ali i traženju nestalih osoba. Vrlo bitna je i odredba kojom je policiji omogućeno da osim utvrđivanja podataka o telekomunikacijskim adresama, odnosno brojeva telefona, prikupljaju i podatke o identifikacijskim oznakama telekomunikacijskih uređaja. U praksi to zapravo znači, da policija

[1] Zakon o policijskim poslovima i ovlastima, Narodne novine 76/09 i 92/14.

ima ovlast uz telekomunikacijski ispis poziva određenog broja mobilnog telefona, odnosno pripadajuće SIM kartice, zatražiti i podatke o serijskom (IMEI) broju mobilnog uređaja koji se koristi, ili se koristio uz navedenu SIM karticu. ZOPPO također definira kako se ovlast provjere uspostavljanja telekomunikacijskog kontakta može primijeniti samo na temelju pisanog odobrenja načelnika Uprave kriminalističke policije ili načelnika Policijskog nacionalnog ureda za suzbijanje korupcije i organiziranog kriminaliteta ili načelnika policijske uprave, odnosno osobe koju on za to ovlasti.[2]

U pravilu je takva ovlast delegirana na čelnike kriminalističke policije na razini policijskih uprava, odnosno na načelnike sektora/službi kriminalističke policije sukladno kategoriji policijske uprave.

Zakonom o izmjenama i dopunama Zakona o kaznenom postupku[3] u Zakon o kaznenom postupku (dalje u tekstu ZKP) je člankom 339a. normirana nova dokazna radna - provjera uspostavljanja telekomunikacijskog kontakta.

Dokaznu radnju provjere uspostavljanja telekomunikacijskog kontakta provodi policija temeljem naloga suca istrage kada postoji sumnja da je registrirani vlasnik ili korisnik počinio kazneno djelo koje se progoni po službenoj dužnosti, a primjena dokazne radnje je potrebna radi prikupljanja dokaza za kazneni postupak. Navedena odredba također predviđa i provođenje dokazne radnje provjere uspostavljanja telekomunikacijskog kontakta za registriranog vlasnika ili korisnika telekomunikacijskog sredstva za kojeg se sumnja kako je povezan sa osobom za koju postoji sumnja da je počinila kazneno djelo koje se progoni po službenoj dužnosti.[4]

Ovdje je bitno naglasiti kako je ZKP propisivao da policija dokaznu radnju provodi traženjem navedenih podataka od operatora javnih telekomunikacijskih usluga. Navedeno postupanje nije bilo u skladu sa Zakonom o sigurnosno-obavještajnom sustavu. Naime, Zakonom o sigurnosno obavještajnom sustavu osnovan je Operativno tehnički centar za nadzor telekomunikacija, kao tijelo sigurnosno-obavještajnog sustava Republike Hrvatske, zaduženo, između ostalog i za koordinacije između tijela koja su sukladno Zakonu o kaznenom postupku i Zakonu o sigurnosno-obavještajnom sustavu ovlaštena za primjenu mjera tajnog nadzora telekomunikacija (u širem smislu) i pružatelja telekomunikacijskih usluga tzv. „operatera“. Zakonom o izmjenama i dopunama Zakona o kaznenom iz 2014. godine[5] je izvršena izmjena članka 339.a na način da policija dokaznu radnju provodi traženjem navedenih podataka od Operativno tehničkog centra za nadzor telekomunikacija.

Dokazna radnja provjera uspostavljanja telekomunikacijskog kontakta obuhvaća:

- provjeru istovjetnosti, trajanja i učestalosti komunikacije s određenim

[2] čl. 68 st. 3. ZOPPO.
[3] Zakon o izmjenama i dopunama Zakona o kaznenom postupku, Narodne novine 145/13.
[4] čl. 339.a ZKP.
[5] Zakon o izmjenama i dopunama Zakona o kaznenom postupku, Narodne novine 152/14.

elektroničkim komunikacijskim adresama,
- utvrđivanje položaja komunikacijskog uređaja,
- utvrđivanje mjesta na kojima se nalaze osobe koje uspostavljaju elektroničku komunikaciju,
- identifikacijske oznake uređaja.

U slučajevima kada postoji opasnost od odgode, odnosno kada postoji vjerojatnost da sudac istrage neće na vrijeme moći izdati nalog za provođenje dokazne radnje, taj nalog može izdati i sam državni odvjetnik uz obvezu da nalog koji je izdao, državni odvjetnik u roku 24 sata dostavi sucu istrage, koji potom u roku 48 sati odlučuje o zakonitosti naloga državnog odvjetnika. Ukoliko potvrdi zakonitost naloga državnog odvjetnika, sudac u roku 48 sati izdaje rješenje o zakonitosti naloga državnog odvjetnika.

Obzirom da su policijska ovlast provjera uspostavljanja elektroničke komunikacije i dokazna radnja provjera uspostavljanja telekomunikacijskog kontakta u tehničkom smislu identične radnje, bitno je naglasiti njihovu smislenu razliku. Naime, upravo na ovim radnjama se u pravom svijetlu uočava razlika između heurističkog i silogističkog smisla kriminalističkog istraživanja. Smisao provođenja provjere uspostavljanja elektroničke komunikacije je u potpunosti otkrivačko-neformalna i kao takva je vrlo vrijedan alat u razrješavanju kaznenih djela. S druge strane, provjera uspostavljanja telekomunikacijskog kontakta je formalna, dokazna radnja koja se provodi primarno s ciljem prikupljanja dokaza za kazneni postupak. Samim time, logično je da primjena policijske ovlasti u vremenskom smislu najčešće prethodi provođenju dokazne radnje. U kvantitativnom smislu, obzirom na primarni smisao ovih radnji, jasno je kako je primjena policijske ovlasti značajno češća nego provođenje dokazne radnje.

Uz već spomenuti ZKP i ZOPPO, koji uređuju ovo područje, neophodno je spomenuti i cijeli niz drugih zakonskih i podzakonskih akata koji uređuju ovo područje.

Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske[6] kao tijelo sigurnosno-obavještajnog sustava osnovan je Operativno-tehnički centar za nadzor telekomunikacija. Primarna svrha Operativno tehničkog centra je aktivacija i upravljanje mjerom tajnog nadzora telekomunikacija (što podrazumijeva i telefonske izliste) i operativno-tehnička koordinacija između pružatelja telekomunikacijskih usluga, tzv. „operatera“ i državnih tijela koja su sukladno zakonskim propisima ovlaštena provoditi mjere tajnog nadzora telekomunikacija (policija, SOA i VSOA).

Najvažniji podzakonski akt, donesen na temelju Zakona o sigurnosno obavještajnom sustavu je svakako Uredba o obvezama iz područja iz nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama[7]

[6] Zakon o sigurnosno obavještajnom sustavu Republike Hrvatske, Narodne novine 79/06 i 105/06.
[7] Uredba o obvezama iz područja iz nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama, Narodne novine 64/08 76/13.

kojom su jasno razrađene odredbe o podacima o telekomunikacijskom prometu koje operateri telekomunikacijskih mreža moraju čuvati u razdoblju od 12 mjeseci od dana obavljene komunikacije. Uredba obveze o čuvanju podataka razgraničava na one koji se odnose na mobilnu, fiksnu i podatkovnu komunikaciju;

- kod mobilne telefonije; moraju se čuvati podaci o broju s kojeg je inicirana komunikacija, identifikacijske podatke korisnika, podatke o pozivanom broju i identifikacijske podatke korisnika pozivanog broja, točno vrijeme početka i kraja komunikacije, IMSI (identifikacijske) brojeve SIM kartica i IMEI (identifikacijske) brojeve mobilnih uređaja koji su sudjelovali u komunikaciji i dr.
- kod fiksne telefonije; moraju se čuvati podaci o broju s kojeg je inicirana komunikacija, identifikacijske podatke korisnika, podatke o pozivanom broju i identifikacijske podatke korisnika pozivanog broja, točno vrijeme početka i kraja komunikacije,
- kod raznih oblika podatkovne komunikacije (internet, e-pošta i dr.); identifikacijske podatke pretplatnika ili registriranog korisnika IP adrese, korisnički ID i broj telefona sa kojeg je obavljena komunikacija te iste podatke i za eventualnog sugovornika, točne podatke o vremenu prijave i odjave sa pristupne usluge sa naglaskom na pripadajuću vremensku zonu, dinamičku ili statičku IP adresu dodijeljenu od strane davatelja usluge i dr.
- kod nadzora lokacije korisnika; propisuje se obveza operatera da Operativno tehničkom centru za nadzor telekomunikacija pomoću odgovarajućeg sučelja omogući pristup podacima o trenutnoj zemljopisnoj, fizičkoj ili logičkoj lokaciji pojedinačnog nadziranog sredstva, bez obzira ostvaruje li sredstvo komunikaciju ili ne, a u slučaju da nije moguće dostaviti trenutnu lokaciju, dostavlja se podatak o posljednjoj zabilježenoj lokaciji. Operateri su također dužni čuvati podatke o lokaciji sredstva za komuniciranje unazad 12 mjeseci od dana obavljene komunikacije.

Zakon o elektroničkim komunikacijama[8] uređuje obveze pružatelja telekomunikacijskih usluga u smislu:

- Tajnog nadzora telekomunikacija (čl.108) jer se Zakonom obvezuje operatore javnih komunikacijskih mreža o svome trošku osigurati i održavati izravnu vezu i funkciju tajnog nadzora između operatera i operativno-tehničkog centra za nadzor telekomunikacija,
- Obveze zadržavanja podataka (čl.109) u svrhu omogućivanja provedbe istrage, otkrivanja i kaznenog progona kaznenih djela u skladu s posebnim zakonom iz područja kaznenog postupka te u svrhu zaštite obrane i nacionalne sigurnosti u skladu s posebnim zakonima iz područja obrane i nacionalne sigurnosti. Operater je podatke dužan čuvati u izvornom obliku u razdoblju od 12 mjeseci od dana obavljene komunikacije. Zakon o elektroničkim komunikacijama kao podatke koje su operateri dužni čuvati navodi:
  - podatke potrebne za praćenje i utvrđivanje izvora komunikacije,

[8] Zakon o elektroničkim komunikacijama, Narodne novine 73/08, 90/11, 133/12, 80/13 i 71/14.

- podatke potrebne za utvrđivanje odredišta komunikacije,
- podatke potrebne za utvrđivanje nadnevka, vremena i trajanja komunikacije,
- podatke potrebne za utvrđivanje vrste komunikacije,
- podatke potrebne za utvrđivanje korisničke komunikacijske opreme ili opreme koja se smatra korisničkom komunikacijskom opremom,
- podatke potrebne za utvrđivanje lokacije pokretne komunikacijske opreme.

3. PRIKUPLJANJE PODATAKA ELEKTRONIČKE KOMUNIKACIJE

Zakonom o sigurnosno obavještajnom sustavu osnovan je Operativno tehnički centar za nadzor telekomunikacija, kao tijelo sigurnosno-obavještajnog sustava Republike Hrvatske, zaduženo za obavljanje poslova aktivacije i upravljanja mjerama tajnog nadzora telekomunikacijskih usluga, djelatnosti i prometa i koordinacije između tijela koja su sukladno Zakonu o kaznenom postupku i Zakonu o sigurnosno-obavještajnom sustavu ovlaštena za primjenu mjera tajnog nadzora telekomunikacija (u širem smislu) i pružatelja telekomunikacijskih usluga tzv. „operatera".

Operativno tehnički centar osim koordinacijske uloge ima i ovlast nadzora nad pružateljima telekomunikacijskih usluga, u smislu vršenja njihovih obveza prema nositeljima ovlasti za nadzor telekomunikacija.

Sam proces nadzora telekomunikacija, koji naravno uključuje i pribavljanje izlista telekomunikacijskog prometa provodi se putem tehničkog sučelja, spojenog izravno sa bazama podataka i sustavom pružatelja telekomunikacijskih usluga. Sustav za nadzor je formiran na takav način da pružatelji telekomunikacijskih usluga ne mogu doći do podataka nad kojim se telekomunikacijskim adresama vrši tajni nadzor.

U praksi prikupljanje potrebnih podataka putem Operativno tehničkog centra funkcionira tako da specijalizirana ustrojstvena jedinica Ravnateljstva policije, Služba posebnih kriminalističkih poslova prikuplja sve zahtjeve za pribavljanje izlista telekomunikacijskog prometa, te iste prosljeđuje Operativno tehničkom centru za nadzor telekomunikacija.

Ovakav način prikupljanja podataka za policiju i tijela sigurnosno obavještajnog sustava je u znatnoj mjeri unaprijedio stručni, ali i sve druge oblike nadzora nad radom policije i sigurnosno obavještajnog sustava kada je u pitanju prikupljanje podataka o telekomunikacijama, a time posljedično i eventualnim kršenjima ljudskih prava od strane sustava.

Naime, teško je zamisliti kako bi u današnje vrijeme bilo moguće zlouporabiti sustav tajnog nadzora telekomunikacija (sadržaja ili prometa), barem kada je u pitanju policija, ako se uzme u obzir kako u cijelom procesu postoje dvije

jake kontrolne točke. Prva je svakako Služba posebnih kriminalističkih poslova Ravnateljstva policije, koja prikuplja sve zahtjeve za izlistavanje elektroničke komunikacije, dok je druga kontrolna točka svakako Operativno tehnički centar za nadzor telekomunikacija koji postupa po takvim zahtjevima. Pri tome treba naglasiti da iako su takve mogućnosti znatno sužene, one postoje i u ovako uređenom sustavu. Naime, jasno je da bi policijski službenik sustav mogao obmanuti prikazivanjem lažnih razloga izlistavanja određenog telefonskog broja, ali bi u tom slučaju svakako ostavio pisane tragove koje bi bilo vrlo teško ukloniti.

Nadzor nad primjenom policijskih ovlasti provjere uspostavljanja elektroničke komunikacije iz članka 68. ZOPPO provodi Vijeće za građanski nadzor.[9] Prilikom obavljanja nadzora Vijeće je ovlašteno od Operativno-tehničkog centra za nadzor telekomunikacija zatražiti usporedbu podataka s kojima raspolaže s podacima Ravnateljstva policije o primijenjenim ovlastima iz članka 68. ZOPPO.

Značajno opasnija i mnogo teže dokaziva situacija je ona u kojoj policijski službenik u potpunosti zaobilazi propisane kanale pribavljanja podataka i iste pribavlja „svojim kanalima“ izravno od operatera.

4. KRIMINALISTIČKA ANALIZA PODATAKA MOBILNE I FIKSNE TELEFONIJE

4.1. Osnovni pojmovi mobilne telefonije

Mobilni uređaj je radijski uređaj koji radijskim signalom raznih vrsta (GSM, GPRS, 3G, 4G) komunicira sa mobilnom mrežom i prema istoj se identificira svojim jedinstvenim IMEI (International Mobile Equipment Identity) brojem. SIM (subscriber identification module) kartica je elektronička kartica koja se umeće u mobilni uređaj, a koja sadrži pozivni broj operatera.

IMEI broj, osim što je policijskim službenicima iznimno važan u nadzoru komunikacija, jer omogućuje praćenje SIM kartica koje se mijenjaju u određenom mobilnom telefonu je izuzetno bitan i pružateljima telekomunikacijskih usluga, jer im omogućuje da u slučaju bilo kakvog zlonamjernog korištenja mobilnog uređaja, (kao što je to primjerice čest slučaj kod maloljetnika koji iz šale pozivaju brojeve hitnih službi) uređaju zabrane pristup mreži, bez obzira koja se kartica nalazi u njemu. Značajno je napomenuti i kako većina mobilnih telefona omogućava i obavljanje hitnih (tzv. SOS) poziva prema hitnim službama, kada se u istima ne nalazi SIM kartica, pa ih je u slučaju obavljanja takvih poziva moguće locirati, kao da se u njima nalazi SIM kartica.

IMEI broj mobitela moguće je provjeriti na 3 načina:

1. IMEI broj je većini mobitela fizički lociran na stražnjoj strani uređaja ispod baterije u obliku naljepnice ili laserski ugraviran na kućište mobitela

[9] čl. 102.a ZOPPO.

2. ukucavanjem koda *#06# u mobitel, nakon čega će se isti prikazati na početnom ekranu
3. posredno, pribavljanjem izlista telekomunikacijskog prometa za SIM karticu koja se nalazi u mobilnom telefonu

IMSI broj (International mobile subscriber identity) je broj karakterističan i jedinstven za svaku SIM karticu u svijetu, a možemo ga nazvati i svojevrsnim „elektroničkim" serijskim brojem SIM kartice. Ovaj broj je u tehničkom smislu vrlo bitan jer putem navedenog broja mobilna mreža identificira SIM karticu koja se nalazi u određenom mobilnom telefonu. Dakle, prilikom spajanju na određenu mobilnu mrežu mobilni telefon i umetnuta SIM kartica djeluju kao cjelina i mobilnoj mreži se identificiraju istovremeno IMEI i IMSI brojem. IMSI broj nije vidljiv u fizičkom obliku, odnosno nije otisnut na SIM kartici.

ICCID (jedinstveni serijski broj SIM kartice) je broj koji je u fizičkom obliku otisnut na samoj SIM kartici, dok je u elektroničkom obliku spremljen u memoriji SIM kartice. Putem ovog broja je moguće identificirati pozivni broj SIM kartice i njezin IMSI broj u slučajevima kada je ista neaktivna (isključena od strane operatera telekomunikacijskih usluga) ili eventualno fizički oštećena, pa ju nije moguće koristiti u mobilnom telefonu. Osim navedenih brojeva, naravno mora se spomenuti i kako je za svaku SIM karticu karakterističan i jedinstveni pozivni broj.

Osim pojmova koji su karakteristični za mobilni telefon i SIM karticu, potrebno je razjasniti i određene pojmove vezane za mobilnu mrežu. Jedan od najvažnijih pojmova, barem u kriminalističkom smislu, je pojam bazne stanice, koja se često naziva i „repetitor". Bazna stanica je u pravilu skup antena montiran na metalnu konstrukciju, stup ili vrh nekog višeg objekta, a sastoji se od više primopredajnih panela, koji se nazivaju i ćelije.

Iako u tehničkome smislu bazna stanica djeluje kao cjelina, u funkcionalnom te posebno kriminalističkom smislu, ćelija je jedan od najvažnijih pojmova u analizi podataka mobilne telefonije. Nakon što se mobilni telefon spoji, odnosno prijavi na određenu ćeliju, na temelju karakterističnih tehničkih podataka o određenoj ćeliji može se doći do određenih zaključaka o lokaciji mobilnog telefona.

U kriminalističkom smislu najbitnije tehničke karakteristike ćelije su:

- podatak o lokaciji ćelije i njezinoj usmjerenosti, koji se prikazuje kao geografska lokacija ćelije te njezina usmjerenost. Usmjerenost se prikazuje kao kut odmaka od sjevera, npr. ćelija na adresi Avenija Dubrava 34, usmjerena 90 stupnjeva od sjevera vidljivo na slici 1.;
- kut primopredaje ćelije - podatak iz kojeg je vidljiva okvirna širina terena koji ćelija pokriva sa svoje lijeve i desne strane, u odnosu na osnovnu usmjerenost, navedeno područje se širi udaljavanjem od ćelije;
- najveći domet - podatak koji odražava maksimalan domet na kojem ćelija može ostvariti funkcionalan kontakt sa mobilnim telefonom. Ovaj podatak se

mora uzeti sa određenom rezervom jer zbog vremenskih prilika i opterećenosti mreže taj podatak može varirati.

Slika 1 –prikaz tehničkih karakteristika ćelije *(Izvor: vlastita izrada, programom Google Earth)*

Na temelju navedenih podataka mogu se prikupiti određeni, iako dosta široki, ipak vrlo bitni podaci o lokaciji određenog mobilnog telefona i to u kontekstu:

- trenutne lokacije mobilnog telefona,
- lokacije mobilnog telefona u vrijeme ostvarivanja određenog telefonskog poziva (retroaktivna lokacija).

Međutim treba naglasiti kako navedeni podaci mogu dati i značajno točniju informaciju o lokaciji mobitela, sve do razine kruga od otprilike 100 metara, ako se mobitel koji se locira u realnom vremenu, nalazi u urbanom području, u kojem je pokrivenost ćelijama zbog niza prepreka značajno gušća. U tom slučaju mobitel je moguće locirati metodom triangulacije signala.

Navedeni sustav, pojednostavljeno rečeno, funkcionira na način da sustav prvo odredi područje koje pokriva određena ćelija na koju je spojen mobitel, te se potom mobitel isključi sa navedene ćelije, čime ga se „prisili“ da se spoji na

sljedeću najbližu ćeliju. Preklapanjem područja pokrivanja svake slijedeće ćelije na koju se mobitel spoji, može se u značajnoj mjeri smanjiti područje na kojem se locira mobitel.

Vodeći se idejom triangulacije, policijski službenik koji provodi kriminalističko istraživanje može prikupiti kriminalistički izuzetno značajne podatke o lokaciji mobilnog telefona, koristeći se podacima o ćelijama putem kojih je određeni mobilni telefon komunicirao, a koje policiji, kao dio izlista poziva, dostavlja Operativno tehnički centar za nadzor telekomunikacija.

Koristeći se podacima o baznim stanicama i ćelijama nekog od operatera u RH pomoću programa Google Earth,[10] koji je besplatan i dostupan svim djelatnicima kriminalističke policije, i datotekama u kmz[11] formatu koje se mogu samostalno kreirati ili pribaviti od operatera, mogu se postići iznimni rezultati u kriminalističkim istraživanjima.

4.2. Analiza i primjena podataka mobilne telefonije u kriminalističkom istraživanju

Vodeći se činjenicom da se kriminalistika kao empirijska znanstvena disciplina temelji na iskustvu, u nastavku rada biti će objašnjeni praktični aspekti analize i korištenja podataka mobilne telefonije u kriminalističkim istraživanjima, pri čemu će se naglasak staviti na onu razinu analize koju svaki policijski službenik sa prosječnim informatičkim znanjem može samostalno provesti, bez korištenja naprednih alata i tehnika kriminalističke analitike.

Takav pristup (bez korištenja resursa kriminalističke analitike) je izuzetno bitan pri provođenju kriminalističkih istraživanja, kada policijskim službenicima takvi resursi nisu dostupni.

Provođenjem preliminarne analize policijski službenik koji provodi kriminalističko istraživanje će zasigurno primijetiti i neke indicije koje analitičar, koji nije izravno involviran u kriminalističko istraživanje možda i ne bi primijetio. Tu se primarno misli na asocijacije koje mogu izazvati kontakti osumnjičenika s određenim osobama ili njegov boravak na određenim lokacijama, poznatim policijskom službeniku iz prethodnih istraživanja.

4.2.1. Primjena podataka s ciljem dokazivanja počinjenja kaznenog djela

Analiza podataka s ciljem dokazivanja kaznenog djela, barem kada se radi o onim najmasovnijim oblicima kaznenih djela imovinskog kriminaliteta se najčešće zasniva na analizi lokacije mobilnog telefonskog uređaja u određenom

[10] Google Earth, https://www.google.com/earth/, datum pristupa 2. rujna.2014.
[11] File Informations Extension, http://www.fileinfo.com/extension/kmz, datum pristupa 2. rujna.2014.

vremenskom razdoblju. Takva analiza zapravo ima za cilj prikazati gdje se mobilni telefon nalazio u kritično vrijeme.

Samu analizu, barem kada je u pitanju utvrđivanje lokacija telefona osumnjičene osobe, policijski službenik može provesti bez korištenja posebnih analitičkih alata i znanja. Za provođenje analize neophodni su:

- moderno računalo sa instaliranim besplatnim Google Earth programom i pristupom internetu,
- datoteka sa podacima o baznim stanicama mobilnih operatera u kmz formatu i
- izlist telekomunikacijskog prometa za određeni broj telefona ili IMEI broj.

Prethodno svakako treba razjasniti koje to podatke je moguće analizirati u samom izlistu telefonskih poziva. Izlist sadrži slijedeće podatke:

- vrijeme uspostavljanja poziva i trajanje poziva,
- broj telefona koji se izlistava
- broj telefona sa kojim izlistavani broj komunicira,
- IMSI broj SIM kartice broja koji se izlistava,
- IMSI broj SIM kartice telefona sa kojim izlistavani broj komunicira,
- IMEI broj mobilnog telefona u kojem se nalazi SIM kartica izlistavanog broja,
- IMEI broj telefona sugovornika, ali isključivo ako se broj telefona sugovornika nalazi u istoj mreži, odnosno kod istog operatera kao i broj koji se izlistava.
- brojčanu oznaku ćelije na koju je broj mobilnog telefona koji se izlistava bio spojen u vrijeme uspostavljanja poziva,
- brojčanu oznaku ćelije na koju je broj mobilnog telefona koji je komunicirao sa brojem koji se izlistava, bio spojen u vrijeme uspostavljanja poziva, ali isključivo ako se broj telefona sugovornika nalazi u istoj mreži, odnosno kod istog operatera kao i broj koji se izlistava.

Korištenjem podataka iz izlista u Google Earth programu sa učitanim KMZ datotekama, pronalazi se zemljopisna lokacija određene ćelije i prikazuju se prethodno objašnjeni tehnički podaci o karakteristikama navedene ćelije.
Obzirom da se u većini slučaja radi o urbanom području, u kojem je prisutnost ćelija veća, zbog raznih građevina koje ometaju signal mobilnih operatera, moguće je da u vrlo kratkom razdoblju od samo nekoliko minuta mobilni telefon u više navrata bude zabilježen na dvije ili više susjednih ćelija.

Takva situacija je vrlo pogodna za dokazivanje činjenice da se određeni mobilni telefon nalazio na nekoj užoj lokaciji, jer se preklapanjem područja pokrivanja susjednih ćelija dobiva znatno uže područje. Primjerice, ako bi se u nekoj situaciji dogodilo da se mobilni telefon istovremeno prijavljuje i na neku drugu ćeliju, tada bismo ocrtavanjem područja pokrivanja navedene ćelije dodatno suzili područje na kojem se mobilni telefon nalazio.

Bitno je naglasiti kako je ovom metodom, s relativno visokom točnošću moguće odrediti područje na kojem se mobilni telefon počinitelja nalazio u vrijeme izvršenja kaznenog djela samo u urbanim gradskim područjima. Naime, područja izvan gradova, posebice u ravničarskim područjima pokrivena su u pravilu vrlo snažnim ćelijama, velikog dometa i područja pokrivanja, pa je zbog toga i puno rjeđa situacija preklapanja baznih stanica.

Kako najveći dio počinitelja kaznenih djela redovno mijenja SIM kartice u mobilnim telefonima, izlist telekomunikacijskog prometa je kao cjelinu moguće pribaviti i po IMEI broju. Izlist poziva će u konkretnom slučaju izgledati potpuno jednako kao i u slučaju izlistavanja po broju telefona, ali će referentna točka izlista biti IMEI broj telefonskog uređaja, a prikazati će se promet svih SIM kartica koje su se u mobitelu nalazile, za vrijeme dok su se koristile u tom mobilnom telefonu.

U kontekstu dokazivanja počinjenja kaznenog djela IMEI broj je značajan i kod pronalaska otuđenih mobilnih telefona. Nažalost, zabilježeni su slučajevi u praksi, u kojima su počinitelji u servisima mobilnih telefona elektroničkim putem mijenjali IMEI brojeve telefona i na taj način onemogućavaju policiju u pronalasku otuđenih mobilnih telefona.

Međutim, za razliku od prije navedenih situacija u kojima policija u trenutku provođenja analize ima saznanja o identitetu počinitelja, u najvećem broju slučajeva počinitelj policiji nije poznat. Policija u takvim situacijama, barem kada su u pitanju značajnija kaznena djela ili serije kaznenih djela ima na raspolaganju vrlo efikasnu metodu prikupljanja podataka o mobilnim telefonskim uređajima koji su zabilježeni na određenoj lokaciji u nekom (užem) vremenskom razdoblju. Pri tome se na određenoj lokaciji prethodno prikupljaju podaci o ćelijama koje pokrivaju navedeno područje. Takvo prikupljanje je moguće u odnosu na:

- na sve mobilne telefone koji su ostvarili komunikaciju na određenoj ćeliji u određeno vrijeme (za posljednjih godinu dana),
- na sve mobilne telefone koji su zabilježeni na određenoj ćeliji, bez da su ostvarivali ikakvu komunikaciju (samo za posljednjih 48 sati).

Podaci o ćelijama se u praksi prikupljaju korištenjem klasičnih mobilnih telefona, sa funkcijom očitanja identifikacijskog broja ćelije određenog mobilnog operatera.

Naravno, nije potrebno dodatno pojašnjavati kakvu praktičnu vrijednost u kriminalističkom istraživanju (bilo u otkrivačkom, bilo u dokaznom smislu) ima činjenica da je mobitel počinitelja zabilježen u blizini mjesta događaja. Činjenica da je telefon počinitelj zabilježen na mjestu počinjenja može Međutim, kao što je već naglašeno, prikupljanje podataka na takav način je ipak ograničeno na prioritetna kaznena djela i serije kaznenih djela (npr. ubojstva, razbojništva, serije provala u domove i dr.), zbog činjenice da se takvim prikupljanjem podataka angažiraju značajni resursi kriminalističke analitike.

Osim informacija koje se mogu prikupiti iz podataka o lokaciji mobilnog telefona počinitelja, značajne informacije se mogu pribaviti i iz podataka o brojevima telefona sa kojima je izlistavani broj kontaktirao. Osim podataka o poznatim vlasnicima registriranih telefona i analize istih kroz kriminalističke evidencije, iz izlista se uz korištenje dostupnih javnih izvora mogu prikupiti iznimno važni podaci za kriminalističko istraživanje.

Iako su telefoni počinitelja kaznenih djela često neregistrirani, kao i brojevi telefona sa kojima isti komuniciraju, pretraživanjem interneta po brojevima telefona korištenjem klasičnog internetskog pretraživača, kao npr. Google, mogu se prikupiti podaci od iznimne važnosti za kriminalističko istraživanje. Takvim internetskim pretraživanjem često se može doći do podataka povezanih sa raznim oglasima, forumima ili sličnim web stranicama na kojima je spomenut broj telefona koji pretražujemo. Analizom podataka sa takvih web stranica može se, primjerice doći do podataka o vozilu koje je osoba prodavala, pa samim time i posredno do identiteta vlasnika neregistriranog telefona. Isto tako kod istraživanja kaznenih djela imovinskog kriminaliteta, internetskim pretraživanjem brojeva sa kojima je izlistavani telefon komunicirao može se doći do vrlo interesantnih podataka o osobama koje putem raznih oglasnika otkupljuju zlatni nakit, tehniku, mobitele i slično.

4.2.2. Primjena podataka s ciljem uhićenja osoba u bijegu

Iako je metodika koja se primjenjuje pri analizi podataka mobilne telefonije, pri traganju za osobama u bijegu vrlo slična, u ovom slučaju je karakteristična činjenica da se podaci analiziraju upravo sa ciljem lociranja i uhićenja neke osobe. Baš iz navedenog razloga ovaj je dio rada izdvojen kao zasebna cjelina kako bi se prikazale metode koje su se u praksi prikazale kao najefikasnije.

Prije svega, bitno je naglasiti da je značajan broj serijskih počinitelja kaznenih djela, određeni dio svoje „karijere“ proveo u bijegu pred policijom. Naime ovakve osobe karakterizira posebna upornost u vršenju kaznenih djela, koja su im vrlo često jedini izvor prihoda. Najveći broj takvih počinitelja je često vrlo dobro poznat policiji, što istima značajno smanjuje manevarski prostor u prikrivanju činjenice da su upravo oni počinitelji kaznenih djela.

Upravo zbog navedenih činjenica, izuzetno je čest slučaj da policija traga za počiniteljima koji istovremeno na snazi imaju i desetak potraga zbog sumnji na počinjenje kaznenih djela. Takve počinitelje možda najbolje opisuje fraza „žive od dana do dana“, jer gotovo svakodnevno vrše kaznena djela, pritisnuti činjenicom da će prije ili kasnije završiti u zatvoru. Svakako treba spomenuti i recidiviste kojima je pravomoćnom presudom određeno izdržavanje kazne zatvora, pa nemaju drugog izbora nego vršenjem kaznenih djela financirati svoj bijeg, a često i visoke troškove odvjetničkih usluga. Tako se svakako zatvara

„začarani krug“.

Prije svega, jasno je da najznačajniji dio počinitelja u bijegu u današnje vrijeme redovito mijenja SIM kartice u mobitelu, pa i same mobilne telefone kako bi onemogućio policiju da ih otkrije i locira putem IMEI broja. Međutim u ovom dijelu rada umjesto na tehničke, treba skrenuti pozornost na neke subjektivne faktore ljudskog ponašanju i komunikaciji, karakteristične za većinu ljudi, koji policiji mogu znatno doprinijeti u pronalasku osobe za kojom se traga. Pri tome se primarno misli na činjenicu da „nijedan čovjek nije otok“, odnosno da smo svi mi društvena bića i imamo potrebu za socijalnim kontaktom.

Tako je praksa pokazala kako značajan broj počinitelja u bijegu ipak nije toliko odlučan u namjeri da se sakrije od policije, da bi u potpunosti prekinuo sve kontakte sa bliskim osobama, bili to članovi obitelji, prijatelji ili djevojka. Upravo zbog toga, kada osobu nije moguće locirati jer njezin broj mobitela nije poznat policiji, naglasak treba staviti na analizu njezinih kontakta prije bijega, umjesto kako bi to možda bilo logično u vrijeme bijega.

Naime, analizom određenog razdoblja prije bijega osobe, kada je ista još koristila mobilni telefon poznat policiji, mogu se prikupiti vrlo značajni podaci za daljnje traganje. Tu se prije svega misli na analizu kontakata osobe za kojom se traga i identificiranje osoba sa kojima ista kontaktira ili je eventualno sa istom stanovala na istoj adresi.

Nakon identificiranja takvih osoba, daljnjom analizom vrlo je lako pronaći referentnu vremensku točku nakon koje je osoba u bijegu promijenila komunikacijsko sredstvo. Upravo od te vremenske točke težište analize telefonskih poziva prebacuje se na mobilne telefone koje koriste osobe bliske osobi u bijegu. Pri tome pažnju svakako treba obratiti na nove, neregistrirane mobilne telefone koji su se u komunikaciji bliskih osoba pojavili nakon prestanka korištenja „starog“ broja mobitela osobe za kojom se traga. Vrlo često će se već iz same frekvencije i načina komunikacije (pozivi ili SMS) moći prepoznati novi broj telefona osobe za kojom se traga.

Nije rijedak slučaj da na području RH obitavaju i stranci (često sa područja susjednih država) koji se bave vršenjem raznih kaznenih djela, a često su za istima raspisane i međunarodne potrage. Iako takve osobe često imaju vrlo sužen krug socijalnih kontakata na području RH, iste je također moguće locirati putem kontakata u matičnoj zemlji, vodeći se gore navedenom logikom.

U takvim situacijama, zahvaljujući dostupnim internetskim telefonskim imenicima, ponekad nije potrebno ni koristiti međunarodnu policijsku suradnju. Naime, sustav kojime se koristi Operativno tehnički centar za nadzor komunikacija omogućuje izlistavanje podataka o mobilnim telefonima koji su pozivani sa nekog stranog telefonskog broja ili koje je taj strani telefonski broj pozivao u RH. U takvoj situaciji je lociranje osobe čak i nešto jednostavnije, nego u prije opisanom slučaju, jer sustav u značajnoj mjeri „profiltrira rezultate“. Da pojednostavimo, ukoliko znamo da na području Grada Zagreba boravi osoba sa područja Sarajeva

za kojom tragamo, putem međunarodne policijske (zahtjev za dostavu podataka putem Interpola, Europola ili drugih oblika međunarodne policijske suradnje) suradnje ili putem internetskih servisa je potrebno pribaviti brojeve telefona članova obitelji te osobe, te potom zatražiti izlistavanje telekomunikacijskog prometa za navedene, strane brojeve telefona. Ukoliko su navedeni telefoni pozivali ili bili pozivani od strane brojeva telefona koji su se nalazili na području Zagreba, isto će biti jasno vidljivo u izlistu telekomunikacijskog prometa.

U kontekstu analize telekomunikacijskog prometa pri traganju za osobama svakako treba spomenuti i mogućnost skeniranja mobilnih telefona prisutnih na nekoj fizičkoj lokaciji. U praksi to znači da policija ima mogućnost korištenjem uređaja, tzv. IMSI catcher-a očitati sve uključene mobilne telefone, odnosno umetnute SIM kartice, koje su aktivne na određenoj fizičkoj lokaciji.

U kontekstu traganja za osobama, takva mogućnost je vrlo bitna u situacijama kada osobe koje kontaktiraju sa osobom u bijegu imaju poseban mobilni telefon koji koriste sa za komunikaciju sa istim, pa taj broj logično, nije poznat policiji. U takvoj situaciji je dakle potrebno uspostaviti tajni nadzor (pratnja) nad osobom za koju se sumnja da komunicira sa osobom u bijegu, te skenirati prisutnost svih mobilnih telefona u njezinoj blizini, kako bi se zabilježio i sporni broj telefona koji osoba koristi za komunikaciju sa osobom u bijegu.

4.3. Analiza i primjena podataka fiksne telefonije u kriminalističkom istraživanju

Iako se o samoj fiksnoj telefoniji, u kontekstu teme ovog rada ne može govoriti niti približno toliko široko, kao što je učinjeno u poglavlju koje se odnosi na analizu podataka mobilne telefonije, ipak postoji nekoliko podataka, koji u kriminalističkom smislu mogu biti itekako interesantni pri analizi podataka prikupljenih izlistom telekomunikacijskog prometa.

Prije svega treba naglasiti kako je kod većine fiksnih telefona vlasnik i lokacija samog telefonskog priključka poznata, jer se radi o fiksnim kabelom povezanim telefonskim linijama. Ipak i u slučaju fiksne telefonije postoji iznimka, a pri tome se prvenstveno misli na „fiksne“ telefonske linije, koje to *de facto* nisu jer za komunikaciju koriste mobilnu telefonsku mrežu. Takve se linije koriste prvenstveno u slučajevima kada davatelj usluga zbog tehničkih nemogućnosti ne može korisniku osigurati telefonski liniju putem fiksne mreže, pa mu onda uslugu pruža putem mobilne mreže, po komercijalnim uvjetima jednakim ili sličnim uvjetima za pružanje usluga fiksne mreže (npr. VIP Homebox).

U takvim situacijama korisnik je obvezan uređaj držati na lokaciji, odnosno adresi na koju je prijavljen, a operater zadržava pravo blokirati telefonski priključak, ako ga korisnik prebaci na drugu adresu. Međutim, određene zlouporabe oko mijenjanja lokacije uređaja su svakako moguće, budući da operater lokaciju uređaja može kontrolirati jedino putem ćelije na koju je uređaj

spojen. Kao što smo već naglasili u prijašnjim poglavljima, ako se radi o ćeliji koja pokriva veliko područje, korisnik može premještati uređaj na više lokacija a da to ne bude primijećeno od strane davatelja usluga.

Prije svega treba naglasiti kako sam izlist telekomunikacijskog prometa za neku fiksnu telefonsku liniju izgleda jednako kao i obrazac izlista telekomunikacijskog prometa za mobilnu liniju, ali kao što je i logično ne sadrži podatke o IMSI i IMEI brojevima.

Kada se govori o kriminalističkoj analizi podataka fiksne telefonije, mora se spomenuti korištenje javnih telefonskih govornica, kao jedan od načina prikrivanja identiteta osobe koja se govornicom koristi. Počinitelji kaznenih djela govornice u praksi najčešće koriste pri počinjenju kaznenih djela poput iznuda, prijetnji ili pak prije provala u stanove, kada pozivom na fiksni broj telefona oštećene osobe provjeravaju da li se tko nalazi u stanu.

Iako su mogućnosti izravne identifikacije pozivatelja koji koristi javne govornice vrlo sužene, ipak postoji mogućnost posredne identifikacije pozivatelja. Naime, javna telefonska govornica kao sredstvo plaćanja koristi telefonsku karticu određene nominalne vrijednosti koja se može iskoristiti za telefoniranje, a u sebi sadrži elektronički dio u kojem je pohranjen serijski broj kartice.

Nakon utvrđivanja točnog vremena poziva sa određene telefonske govornice, od Operativno-tehničkog centra za nadzor komunikacija se može zatražiti dostavu podataka o serijskom broju kartice koja je korištena pri spornom pozivu. Upravo taj podatak može biti presudan u kriminalističkom istraživanju, jer se pribavljanjem izlista telekomunikacijskog prometa, odnosno identificiranjem i drugih telefonski poziva koji su obavljeni korištenjem navedene kartice, po serijskom broju, može posredno identificirati počinitelj.

4.4. IP adresa kao izvor podataka u kriminalističkom istraživanju

Internet protokol ili IP adresa, je pojednostavljeno rečeno brojčana oznaka koja korisnika određenog internetskog priključka identificira pri korištenju mreže, odnosno interneta. IP adresa je binarni broj od 32 bita, koji se zapisuje u dekadskoj notaciji na način da se 32-bitni broj podijeli na četiri 8-bitna broja, koji se prikazuju kao četiri decimalna broja odvojena točkom (npr. 94.123.104.25). Ova specifikacija se odnosi na IP adrese verzije 4, dok se u slijedećih nekoliko godina očekuje prijelaz na verziju 6 dodijele IP adresa.

Primarna svrha IP adrese nije sigurnosne naravi, već tehničke. Naime IP adresa je kao jedinstveni identifikacijski broj neophodna da bi se podaci sa jednog računala, izvora podataka mogli preusmjeriti na odredište- drugo računalo. Kako IP adrese moraju biti jedinstvene za cijeli svijet, obzirom na činjenicu da je internet globalna komunikacijska mreža, postoje međunarodne organizacije zadužene za dodjelu IP adresa kao npr;

- The Internet Assigned Numbers Authority (IANA)[12] međunarodna organizacija sa sjedištem u SAD-u**.** IANA određene raspone IP adresa zadužuje regionalnim Internet registrima,
- RIPE Network Coordination Centre[13] sa sjedištem u Amsterdamu, zadužen za dodjelu određenog raspona adresa operaterima telekomunikacijskih usluga na području Europe

IP adresa je u pravilu dinamička, što znači da ju davatelj usluge dodjeljuje korisniku usluge u pravilu na razdoblje od 24 sata, nakon čega se ista mijenja. Postoji i tehnička mogućnost korištenja statičke IP adrese, kao dodatne usluge, a takvu uslugu koriste poslovni korisnici, odnosno najčešće poduzeća čija je djelatnost vezana uz internet te im je vrlo bitno da imaju stalan identitet na internetu.

Ovdje je neophodno naglasiti kako IP adresa nije identifikacijski broj karakterističan za mrežnu opremu (PC, tablet, smartphone) koja ima mogućnost pristupa internetu, već identifikacijski broj određenog internetskog priključka. To u praksi znači kako IP adresa može biti dodijeljena privatnom fiksnom telefonskom, odnosno internetskom priključku u privatnome stanu, kojime se koristi nekoliko ljudi ili pak javnoj pristupnoj wi-fi internetskoj zoni, na koju se spaja velik broj građana.

No kako IP adresa može biti korisna policijskim službenicima u kriminalističkom istraživanju? U posljednje vrijeme korištenje interneta više nije „rezervirano“ za počinitelje kaznenih djela karakterističnih za internet, kao primjerice dječje pornografije, već se sve češće koristi i pri počinjenju masovnih kaznenih djela kao što su to primjerice prijevare.

Naravno da će razrješavanje složenih kaznenih djela na mreži, poput primjerice dječje pornografije od policijskih službenika zahtijevati posebnu specijalizaciju, stručna znanja i međunarodnu pravnu pomoć u slučajevima kada se podaci nalaze na serverima lociranim u drugim zemljama. Međutim postoji cijeli niz situacija u kojima policijski službenik uz malo truda u kriminalističkom istraživanju, bez korištenja kompliciranih alata i resursa kriminalističke analitike može samostalno putem IP adrese prikupiti podatke od elementarne važnosti za kriminalističko istraživanje i daljnji kazneni postupak.

Jedan od takvih primjera je cijeli niz prijevara koje se putem internetskog oglasnika ‘’Njuškalo.hr’’ – www.njuskalo.hr vrše u posljednjih nekoliko godina, na način da se počinitelj lažnim identitetom registrira na internetski oglasnik i potom na prodaju nudi mobilne telefone i slično. Nakon što oštećena osoba sukladno dogovoru sa počiniteljem uplati novac na račun koji počinitelj navede, počinitelj ne isporuči kupljenu robu.

Obzirom da je u konkretnom slučaju riječ o pravnoj osobi registriranoj u RH (Njuškalo.hr), policijski službenici mogu od pravne osobe zatražiti

[12] Internet Assigned Numbers Authority, http://www.iana.org, datum pristupa 4. rujna 2014.
[13] Regional Internet Registries, http://www.ripe.net, datum pristupa 4. rujna 2014.

dostavljanje podataka o IP adresi koja je korištena prilikom postavljanja spornog oglasa na web stranicu oglasnika.

Po pribavljanju podataka o IP adresi policijski službenici su sukladno ovlasti provjere uspostavljanja telekomunikacijskog kontakta propisanoj u članku 68. Zakona o policijskim poslovima i ovlastima ili pak ovlasti iz čl.339.a ZKP-a, temeljem naloga suca istrage ovlašteni Operativno tehničkom centru za nadzor telekomunikacija dostaviti IP adresu kojom se koristio počinitelj, uz zahtjev za provjeru korisnika konkretne IP adrese. Uz zahtjev je potrebno priložiti točno vrijeme kada se navedena IP adresa koristila uz podatak o vremenskoj zoni u kojoj je IP adresa korištena.

Ako je IP adresa počinitelja prijevare bila dodijeljena nekome od pružatelja javnih komunikacijskih usluga s područja Republike Hrvatske, Operativno tehnički centar za nadzor telekomunikacija će policiji dostaviti podatak o broju telefona sa pristupom internetu ili podacima korisnika koji je vlasnik internetskog priključka, ako je priključak registriran.

5. Zaključak

Logično pitanje, koje su si autori ovog članka, prije izrade samog članka postavili je svakako pitanje u kojoj mjeri će ovakav tekst „razotkriti“ postupanje policije u onim sferama kriminalističkog istraživanja, za koje je do sada u pravilu vrijedila dogma kako se radi o sferama postupanja policije, koje bi u pravilu trebale ostati skrivene od očiju javnosti. Naravno, sasvim je jasno kako policija pribavljajući podatke mobilne i fiksne telefonije postupa po detaljno uređenim zakonskim i podzakonskim aktima, pri tome provodeći samo one mjere koje su zakonom izričito dopuštene. S tehničke strane, ne može se ne primijetiti da su na internetu dostupni apsolutno svi podaci koji se tiču tehničkog segmenta rada mobilne i fiksne telefonije. Dakle, ako se i može govoriti o tajnosti postupanja policije u prikupljanju podataka putem mobilne i fiksne telefonije, ta tajnost se može odnositi isključivo na konkretne predmete i osobe prema kojima se takve mjere provode, ali ne i na same metode prikupljanja podataka.

Vrijednost ovakvih metoda prikupljanja podataka u kriminalističkom istraživanju je svakako nemjerljiva. Analizom izlista telefona određene osobe, mogu se pribaviti podaci ili indicije koje mogu u značajnoj mjeri olakšati kriminalističko istraživanje ili pak na njega u značajnoj mjeri utjecati. Primjenom novih radnih procesa i korisničkih sučelja, primjena policijske ovlasti provjere uspostavljanja elektroničke komunikacije je postala lako dostupna većini policijskih službenika kriminalističke policije. Ako se uzme u obzir da je primjena ove ovlasti dobrodošla u razrješavanju apsolutno svih vrsta kaznenih djela koja se progone po službenoj dužnosti, bod onih najlakših pa do serija najtežih kaznenih djela i najkompliciranijih modernih oblika kriminaliteta, mišljenja smo da bi razina znanja koja je prikazana u ovom članku, trebala biti opći minimum znanja

svakog službenika kriminalističke policije koji radi na razrješavanju kaznenih djela.

Ipak, mora se primijetiti kako je posljednjih godina, posebice kada se radi o linijama rada suzbijanja organiziranog kriminaliteta i korupcije zabilježen trend sve veće ovisnosti kriminalističke policije o podacima koji se zasnivaju isključivo na analizama telekomunikacijskog prometa. Iako je prilagodba novim tehnologijama nužna, obzirom na sve značajnije korištenje raznih telekomunikacijskih tehnologija pri vršenju kaznenih djela, nužno je zadržati određeni balans između korištenja telekomunikacijskih tehnologija i tradicionalnih metoda kriminalističkog prikupljanja podataka.

Literatura

1. Dujmović, Z. Karas Ž.; Kolar-Gregorić, T.; Šuperina, M., Kriminalistika, Zagreb, MUP RH, Policijska akademija, 2007.
2. Gluščić, S., Veić, P.: Zakon o policijskim poslovima i ovlastima, Zagreb, Ministarstvo unutarnjih poslova, 2015.
3. Modly, D. i Mršić, G., Uvod u kriminalistiku, Zagreb, Hrvatska sveučilišna naklada, 2014.
4. Pavišić B., Uvod u kriminalistiku, Zagreb, Ministarstvo unutarnjih poslova, 2002.
5. Pavišić, B. i dr., Kriminalistika I, Zagreb, Tehnička knjiga, 2006.
6. Zakon o policijskim poslovima i ovlastima, Narodne novine 76/09, 92/14.
7. Zakon o kaznenom postupku, Narodne novine 152/08, 76/09, 80/11, 91/12, 143/12, 56/13 145/13, 152/14.
8. Zakon o sigurnosno obavještajnom sustavu Republike Hrvatske, Narodne novine 79/06 i 105/06.
9. Zakon o elektroničkim komunikacijama, Narodne novine 73/08, 90/11, 133/12 i 80/13.
10. Uredba o obvezama iz područja iz nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama, Narodne novine 64/08 76/13.
11. Pravilnik o načinu provođenja posebnih dokaznih radnji (NN102/2009).

Internet izvori:

12. Internet Assigned Numbers Authority http://www.iana.org, datum pristupa 4. rujna 2014.
13. Regional Internet Registries http://www.ripe.net, datum pristupa 4. rujna.2014.
14. Schmidt, K.: Cell Phone Tower Types and Information, http://www.

steelintheair.com/Cell-Phone-Tower.html#.U6iEOJSSz3Q, datum pristupa 3. rujna 2014.
15. Paganini, P.: Smart Phone Monitoring and Malware… Up close and personal…http://securityaffairs.co/wordpress/7756/security/smart-phone-monitoring-and-malware-up-close-and-personal.html, datum pristupa 3. rujna 2014.
16. File Informations Extension http://www.fileinfo.com/extension/kmz, datum pristupa 2. rujna 2014.
17. Google Earth, https://www.google.com/earth/, datum pristupa 2. rujna 2014.

Summary

Criminal data analysis of mobile and fixed telephony to solve crimes

This paper explains practical aspects of analysing data collected using police powers, checks the connections of electronic communications in the Act on police duties and powers, and the implementation of evidence collection checking establishing telecommunication contact prescribed by the provisions of the Criminal Procedure Law.

Particular emphasis is given to simple, everyday aspects of criminal analysis data that can be found in "phone connection list", as well as the use of analytical software and tools. Article will clarify concepts whose understanding is very important in the interpretation of data from the "listing", such as the IMEI number, IMSI number, cell location, IP address and others.

The paper will present legal sources which regulating this area, where the police is authority for collecting data, as well as the obligations of the telecommunications services providers in terms of providing access to available information.

Keywords: phone communication list, telecommunications contacts, IMEI, cell operator.