УЛОГА И ЗНАЧАЈ (ЛИСТИНГА) ТЕЛЕКОМУНИКАЦИОНИХ БАЗНИХ СТАНИЦА У КРИМИНАЛИСТИЧКО-ОПЕРАТИВНОМ РАДУ

Прегледни рад	DOI: 10.7251/BPG1603123M	УДК: 343.51/.53: 621.39

Мср Александар Миладиновић*

Апстракт: Криминалистички аспект базних станица се огледа кроз неколико сегмената који омогућавају долазак до одређених података, информација и сазнања у погледу индиција о нечијој (не)присутности на одређеном подручју за конкретан период. Оперативним кориштењем могућности које пружају базне станице, те адекватним и благовременим комбиновањем са другим оперативно-тактичким мјерама и радњама и истражним радњама може да се дође до одређених индиција у погледу нечије криминалне активности, примарно посматрајући наведено кроз присутност, односно неприсутност сумњивих лица на мјесту извршења кривичног дјела у вријеме извршења дјела. Наиме, преко базних станица се, на посредан начин, за одређено вријеме или за одређени период могу локализовати корисници одређених телефонских бројева или мобилних телефона на подручју које „покрива“ базна станица. Такође, базне станице омогућавају накнадно, посредно и прилагођено „праћење“ одређених корисника телефонских бројева или мобилних телефона лоцирањем преко базних станица преко којих остварују комуникацију.

Кључне ријечи: телекомуникационе базне станице, индицијални метод, индиција присутности на лицу мјеста, телекомуникациони саобраћај, ИМЕИ.

УВОДНА РАЗМАТРАЊА

У сузбијању криминалитета, полиција не запоставља класичне методе, средства и стратегије сузбијања и супротстављања криминалитету, али, поред наведеног, ослања се и на савремена достигнућа у разним областима науке и технологије. Такође, полиција усавршава и властите методе реаговања на криминалитет, док, исто тако, користи и методе других наука, као и вјештине и технике које су неопходне приликом

* *Јединица за полицијску обуку – Полицијска академија Бања Лука, email: aaleksandarbl@yahoo.com.*

обављања других послова, прилагођавајући их у мањој или већој мјери могућностима и потребама криминалистичке дјелатности.

То се посебно односи на савремена телекомуникациона средства и начине остваривања овог вида саобраћаја.

С обзиром на то да је евидентна и квалитативна и квантитативна експанзија телекомуникационог саобраћаја, као и мобилних јединица (уређаја) којима се ова комуникација остварује, јасно је да се наметнула потреба кориштења могућности које ове технологије пружају и у криминалистичке сврхе. Тим прије што ове могућности не пружају само увид у садржај комуникације корисника, већ адекватним кориштењем, уз криминалистичко знање, као и уз комбинацију са другим мјерама и радњама из полицијског, а поготово из криминалистичког дијапазона дјеловања, могу да дају и многобројна друга сазнања, информације и податке о криминалним активностима одређених лица.

Уколико се има у виду да криминалци, поготово искуснији, у данашње вријеме из страха од прислушкивања све мање преко телефона говоре о властитим криминалним активностима, усљед чега се на одређен начин ограничава могућност добијања одређених кривичнопроцесних и криминалистички релевантних доказа и информација примјеном посебних истражних радњи, иако мобилне телефоне и друге мобилне уређаје користе у свакодневном животу, јасно се наметнула потреба за другим криминалистичким методама и активностима у циљу доласка до релевантних информација и доказа у погледу конкретне криминалне активности корисника телекомуникационих ресурса.

У том погледу, базне станице оператера мобилне телефоније, односно телекомуникациони саобраћај остварен преко базних станица, са свим могућностима које ове станице пружају, свакако да је нашао адекватну сврху и примјену у криминалистичком оперативном раду полиције. Адекватним кориштењем могућности које пружају базне станице, односно телекомуникациони саобраћај који се одвија преко базних станица припадницима криминалистичке полиције омогућава да дођу до важних индиција у погледу нечије криминалне активности, док, с друге стране, на тај начин властиту криминалистичку активност обогаћују и могућностима које им пружају нове технологије, у овом случају техника на којој се заснива актуелни телекомуникациони саобраћај.

ТЕХНИЧКИ АСПЕКТ ФУНКЦИОНИСАЊА И ЗНАЧАЈ ТЕЛЕКОМУНИКАЦИОНИХ БАЗНИХ СТАНИЦА

Базна станица (Base Transceiver Station) је централна радио станица преко које се емитују (тј. примају и шаљу) сигнали мобилне телефоније

(Бача, 2004). Ваљски посматрач базну станицу, у ширем смислу ријечи, обично види као високи стуб на који је инсталирана антена, а крај стуба се обично налази „кућица". У њу је смјештена контролна и пратећа опрема – унутар кућице се обично налази батерија која антену напаја електричном енергијом, исправљач и сама станица. Станица „прикупља" промет са околног простора који „покрива" базна станица и усмјерава га ка централи. Када претплатник пређе из подручја „покривања" једне базне станице у друго, слиједи непримјетно „преузимање" корисника од стране друге базне станице. Ово се назива аутоматски Хандовер (Митровић, Сикимић, 2010: 87).

Улога базних станица (јединица) у телекомуникационом саобраћају мобилне телефоније би се, најједноставније, могла представити као посредничка улога између више корисника, односно више мобилних телефона (уређаја) и централе оператера мобилне телефоније. Наиме, преко бројних базних станица „посијаних" по цијелом подручју које је „покривено" сигналом оператера мобилне телефоније, одвија се сама комуникација између једног или више корисника те мреже, из чега је видљива посредничка улога базних станица.

Међутим, неопходно је навести да корисници приликом међусобне комуникације не комуницирају само преко базних станица, односно конкретна базна станица не посредује сама у комуникацији. Наиме, успостављањем комуникације корисник „комуницира" превасходно са конкретном базном станицом на чијем се подручју налази, а потом она „комуницира" са централном базом оператера мобилне телефоније (Mobile Switching Centre), након чега централа преноси „комуникацију" базној станици на чијем подручју се налази корисник који се позива, те се садржај комуникације њему прослеђује. Из овога је видљиво да се комуникација између више корисника не одвија само преко базних станица, већ и преко главне централне базе оператера мобилне телефоније. Сходно томе, базне станице су само почетна и завршна, али не и једина тачка у посредовању између корисника услуга мобилне телефоније.

У контексту наведеног, јасно је да је, да би се комуникација на овај начин одвијала несметано и беспријекорно, неопходно да подручје које је „покривено" сигналом конкретне мобилне мреже (оператера мобилне телефоније) буде „покривено" и самим базним станицама. Конкретније, само „покривање" сигналом подручја једне мреже подразумијева „покривање" тог подручја сигналима управо са тих базних станица, јер, као што је и напријед наведено, управо базне станице и служе да би се преко њих одвијала телефонска комуникација, без обзира на то да ли су у питању одлазни или долазни позиви или друга врста комуникације. Другим ријечима, управо базне станице сигналом конкретне мреже оператера мобилне телефоније „покривају" подручје на којем се

налазе, омогућавајући одлазне и долазне позиве, као и друге врсте комуникације. Наравно, комуникација мобилним телефоном на једном подручју одвија се и преко базних станица других оператера мобилне телефоније (преко друге мреже), како у подручју гдје дјелује само једна мрежа (један оператер), када други оператери користе услуге базне станице примарног (јединог) оператера мобилне телефоније, тако и у подручју гдје дјелује више оператера (више мрежа), када сваки оператер има властите базне станице. Базне станице „покривају" радијус локације на којој се налазе, с тим што је и сам тај радијус једне базне станице подијељен (испарцелисан) на три једнака дијела (подручја), која се називају ћелијама. „Покривеност" подручја базним станицама, односно величина подручја које „покривају" базне станице, а самим тим и међусобна удаљеност самих базних станица је различита, јер је условљена многобројним факторима, међу којима су најбитнији, али не и једини, сам опсег телекомуникационог садржаја који се тренутно одвија (или се планира одвијати у дужем периоду), број корисника на конкретном подручју, карактеристике тог подручја (урбано или рурално подручје), итд.

Неопходно је навести још једну битну карактеристику овако посматране комуникације преко базних станица мобилне телефоније. Успостављањем позива, односно позивањем другог корисника мобилне телефоније, са мобилног телефона тог корисника се базној станици упућује сигнал. Тај сигнал у себи инкорпорира одређене информације, од којих су, са криминалистичког аспекта, свакако најбитнији ИМЕИ мобилног телефона који позива (који се налази на подручју конкретне базне станице), телефонски број (МСИСДН) који се налази у том мобилном телефону, серијски број картице телефонског броја (ИМСИ) који се налази у том мобилном телефону, телефонски број корисника који се позива, врста комуникације (позив, СМС, ММС, електронска пошта...), вријеме успостављања и трајања позива, итд. Сигнал са (између осталог) наведеним подацима се дистрибуира и централној бази мобилне телефоније, али остаје и у својеврсној бази конкретне базне станице. С друге стране, сигнал са (између осталог) сличним подацима преко базне станице која „покрива" подручје на којем се налази позивани корисник долази и до самог корисника, односно његовог мобилног телефона. Сходно томе, и овај сигнал се налази у бази те базне станице. Са криминалистичког аспекта, ово су свакако најрелевантнији подаци које полиција користи, односно може да користи у криминалистичко-оперативном раду.

КРИМИНАЛИСТИЧКИ АСПЕКТ ТЕЛЕКОМУНИКАЦИОНИХ БАЗНИХ СТАНИЦА

Из напријед наведеног је видљиво да се преко базних станица одвија цјелокупан телекомуникациони садржај корисникā који се налазе на подручју које „покрива" та базна станица, без обзира на то да ли су они пасивни или активни субјекти позива (да ли су позивали или су позвани). Са криминалистичког аспекта, тај саобраћај, односно садржај тог саобраћаја са одређеним информацијама и подацима које садржи релевантан је и може да се користи у одређене оперативне, па и кривичнопроцесне (доказне) сврхе.

Конкретно, адекватним кориштењем могућности које омогућава базна станица, односно телекомуникациони саобраћај који се одвија преко саме станице припадницима криминалистичке полиције омогућава да дођу до важних индиција у погледу нечије криминалне активности, док, с друге стране, на тај начин властиту криминалистичку активност обогаћују и могућностима које им пружају нове технологије, у овом случају техника на којој се заснива актуелни телекомуникациони саобраћај.

Адекватним и благовременим оперативним кориштењем могућности које пружају базне станице, те комбиновањем са другим оперативно-тактичким мјерама и радњама и истражним радњама може да се дође до одређених индиција у погледу нечије криминалне активности, примарно посматрајући наведено кроз присутност, односно неприсутност сумњивих лица на мјесту извршења кривичног дјела у вријеме извршења тог дјела. Наиме, преко базних станица се, на посредан начин, могу локализовати корисници одређених телефонских бројева или одређених мобилних телефона на подручју које „покрива" базна станица у одређено вријеме или за одређени период. Преко добијеног листинга базне станице (у којој је садржан цјелокупан садржај телекомуникационог саобраћаја за конкретизовани период) лоцирају се, а потом и идентификују одређени корисници који, по разним основама, могу да буду релевантни за криминалистичку активност, без обзира на то да ли се ради о проактивној или репресивној активности. Идентификацијом самих корисника који су у критичном периоду били присутни на одређеном подручју или локацији (што се утврђује на основу телефонске комуникације остварене преко базне станице) сужава се круг осумњичених лица или се чак одређена сумњива лица елиминишу из круга осумњичених, с обзиром на индицију (не и доказ) о њиховој (не) присутности на лицу мјеста, односно у његовој ближој или релативно даљој околини. Наравно, јасно је да се наведено не може узети као доказ о неприсутности сумњивих лица на лицу мјеста уколико изостане

њихова телекомуникациона активност преко базне ћелије коришћењем услуга мобилне телефоније (с обзиром на то да је могуће да наведена лица, иако присутна на наведеној локацији у критично вријеме, нису користила мобилни телефон или нису користила услуге наведене мреже или нису користила властити број или мобилни телефон...). Исто тако, разумљиво је и да се одређена телекомуникациона активност сумњивих лица за критичан период на одређеном подручју не може узети као доказ о виности тих лица или о њиховој повезаности (на било који начин) са конкретним кривичним дјелом или конкретизованом криминалном активношћу, већ само као индиција (зато што наведена лица, без обзира на то да ли су позната по криминалној активности или не, па чак и по претходној криминалној активности конкретних кривичних дјела која су и извршена у вријеме њиховог боравка на подручју гдје је дјело извршено, на њему могу да бораве по различитим основама, затим – могуће је да су наведени број или мобилни телефон, иако постоје оперативна сазнања да их користе идентификована сумњива лица, у критично вријеме користила друга лица, док су њихови корисници били на другом подручју...). Усљед наведеног, јасно је да се листинг базне станице, преко којег се утврђује присутност одређених лица на одређеном подручју (које је „покривено" базном станицом), може користити само као индиција (углавном у криминалистичке сврхе), односно није доказ о нечијој присутности, као и о нечијој неприсутности на конкретизованом подручју усљед (не)изостанка телекомуникационе активности телефонског броја или самог мобилног телефона тог корисника за критичан период на том подручју.

Концепција криминалистике као науке која, између осталог, прилагођава методе других наука, као и начине и методе вршења одређених активности, техничке и нетехничке природе, у циљу сузбијања криминалитета, те откривања и расвјетљавања кривичних дјела, своју афирмацију је добила и када је у питању телекомуникациони садржај преко базних станица. То се најеклатантније конкретизује када је у питању једна активност која у задње вријеме све више добија на афирмацији у криминалистичком раду полиције, а односи се на могућности саме базне станице. Та активност подразумијева својеврсни посредни, накнадни и прилагођени начин „праћења" одређених корисника телефонских бројева или мобилних телефона лоцирањем базних станица преко којих, у току праћења, остварују комуникацију. Конкретно, када је у питању наведено, као што је већ речено, базне ћелије „хватају" телефонски позив упућен са подручја које „покривају", с једне стране, док с друге стране „пласирају" телефонски сигнал кориснику ком је упућен, а он се налази на подручју које „покрива" та базна станица. Разумљиво је да корисници углавном не комуницирају преко једне базне станице, с обзиром на то да се крећу. Уколико се крећу, те уколико у току тих покрета (који могу да буду од улице

до улице, од насеља до насеља, од града до града...) остварују редовну или повремену телефонску комуникацију преко телефонског броја или преко мобилног телефона који је у њиховом посједу, базне станице на чијем простору се налазе у моменту слања позива „хватају" тај њихов сигнал, те га даље просљеђују. Исто тако, и уколико се ти корисници позивају, базне станице које „покривају" подручје гдје се налазе ти корисници их региструју, те њима упућују позиве. Овдје се види једна могућност коју припадници криминалистичке полиције у задње вријеме све више потенцирају у практичном криминалистичко-оперативном раду. Наиме, уколико се за одређено лице сумња да се бави одређеним криминалним активностима на подручју више насеља или градова, а познато је вријеме (и мјесто) вршења тих активности, пуким сагледавањем листинга његовог идентификованог или унапријед познатог броја телефона или мобилног телефона, могуће је да се он локализује за критичан период. Наиме, с обзиром на то је велика могућност да је прије, у току или након извршења кривичног дјела користио услуге мобилне телефоније (примао или слао позиве или поруке или користио друге услуге), све његове активности телекомуникационог саобраћаја посматране преко телефонског броја или мобилног телефона ће се регистровати и на базним станицама подручја кроз које се кретао или на којем је боравио. На тај начин, упоређивањем мјеста његовог кретања или боравка (преко листинга његовог телефонског броја или његовог мобилног телефона) са мјестом извршења кривичног дјела, за вријеме извршења кривичног дјела или непосредно прије или након тог времена, долази се до индиције у погледу присутности или неприсутности тог лица на наведеном подручју, али и до његове (не)повезаности са конкретним кривичним дјелима извршеним на подручју више насеља, а поготово градова. Овај начин индицијалног метода у погледу расвјетљавања криминалне активности је посебно афирмативан код серијских кривичних дјела у којима се одређено лице сумњичи да је извршилац више кривичних дјелā у одређеном периоду на подручју више градова. Анализирањем листинга његовог броја телефона или његовог мобилног уређаја, на посредан начин, може да се потврди индиција о његовој (не) присутности на мјесту извршења кривичних дјела за критичне периоде. Међутим, као и у претходном случају, и овдје се наведено може користити само као индиција о нечијој (не)присутности, с обзиром на многобројне ситуације у којима осумњичени може да борави на одређеном подручју, а да се то не конкретизује и кроз телекомуникациону активност његовог телефонског броја или мобилног уређаја (никог није позивао, нити је неко њега позивао, није носио мобилни телефон са собом...), али, исто тако, треба имати у виду да осумњичени и не борави на одређеном подручју, а да се анализом листинга дође до таквог закључка (осумњичени другом дао број телефона или мобилни телефон...).

Знајући криминалистичке могућности у погледу савремених телекомуникационих технологија, све већи број криминалаца, када одређену комуникацију која је компромитујућа мора да реализује користећи се телекомуникационим услугама, користи телефонске бројеве или мобилне телефоне само за ту прилику, односно – једном или више пута кориштен телефонски број или мобилни телефон преко којег је реализовао разговор или другу телекомуникациону активност за коју сматра да је компромитујућег карактера одмах уништава или одбацује. Другим ријечима, криминалци свјесни „компромитујућих могућности" мобилних телефона или било каквог телекомуникационог саобраћаја најчешће властиту комуникацију, поготово уколико је на било који начин компромитујућег карактера, ограничавају на непосредну, али уколико она није могућа на тај начин (усљед одређених околности), компромитујућу комуникацију најчешће реализују преко мобилних телефона и/или телефонских бројева које користе само за ту прилику и које одмах уништавају или одбацују како се компромитујућа телекомуникациона активност не би могла повезати са њима. Усљед релативно ниских материјалних издатака у погледу наведеног (условљених ниским цијенама телефонских бројева и мобилних телефона), разумљиво је да криминалци, поготово они који располажу знатнијим финанијским средствима, наведено користе у комуникацији за коју сматрају да (им) је компромитујућег карактера. Поред тога што им једнократно коришћење мобилних телефона и телефонских бројева не представља значајан финансијски издатак, најчешће се и ради о осуђиваним криминалцима који су и „падали" на доказима, подацима, информацијама, сазнањима и индицијама заснованим управо на телекомуникационим ресурсима, усљед чега додатно избјегавају коришћење мобилних телефона и телефонских бројева, а поготово коришћење истих мобилних телефона и телефонских бројева више пута, и то за вршење компромитујуће комуникације. Међутим, иако наведено умногоме ограничава оперативну употребљивост телекомуникационих ресурса примарно посматраних у контексту базних станица, то никако не значи да наведено и онемогућава одређену употребљивост ових ресурса, поготово када се ради о неопрезним или необавјештеним криминалцима или криминалцима чије материјалне могућности не омогућавају једнократно коришћење мобилних телефона или телефонских бројева. Наиме, у пракси су чешћи случајеви, поготово код кривичних дјела која не потпадају под дијапазон организованог криминалитета, да извршилац за комуникацију користи више мобилних телефона и телефонских бројева, те да преко њих остварује телекомуникациону активност која може да буде компромитујућа за њега, али да најчешће те мобилне телефоне и телефонске бројеве неће одбацити, већ ће их наставити користити и након компромитујуће активности. Ово ће се,

као што је већ наведено, најчешће и радити код криминалаца који нису свјесни криминалистичких могућности у погледу телекомуникационог саобраћаја, али и код криминалаца који су дјелимично свјесни наведених могућности, али сматрају да наведено на одређени начин могу „заварати". У том погледу, ови криминалци најчешће у једном мобилним телефону користе више телефонских бројева у релативно краћем периоду, а онда са само једног од тих бројева остварују компромитујућу телекомуникациону активност или један телефонски број користе у више мобилних телефона, те тако остварују компромитујућу телекомуникациону активност, а такође је примјетно и да се картице телефонских бројева мобилних телефона све више „клонирају"... У свим овим случајевима, корисници телекомуникационих услуга настоје на овај начин да заварају евентуалну криминалистичку активност преко телекомуникационих ресурса, надајући се да ће мијењањем, односно мијешањем телефонских бројева у мобилним телефонима, онемогућити евентуално откривање, а потом и идентификовање криминалних активности и извршиоца тих активности, те цјелокупног ланца учесника у њој. Усљед наведеног, да би се предуприједила, али и превазишла одређена ограничења у погледу локализације и идентификације корисника који на овај начин покушавају да прикрију властиту криминалну активност, неопходно је редовно ажурирати постојеће податке о корисничким телефонским бројевима и мобилним телефонима сумњивих лица. Поред тога, неопходно је да се приликом оперативног кориштења базне станице или листинга телефонске комуникације за одређени број или мобилни телефон осумњиченог лица увијек обрати пажња на то да ли је он у току посматраног периода, а поготово у току критичног периода, приликом комуникације мијењао мобилни телефон (што се утврђује на основу промјене ИМЕИ-а на листингу траженог броја) или телефонски број (што се утврђује на основу промјене МСИСДН-а или ИМСИ-а на листингу мобилног телефона). Уколико јесте, криминалистички је исправно да се и за наведене бројеве телефона или мобилне телефоне (који су се у току критичног периода користили) обавезно узму листинзи, те да се и на основу тих листинга покушају утврдити криминалистички релевантне информације и сазнања. Наравно, на основу информација и података добијених и на основу тих листинга, могуће је да се криминалистичка активност прошири и усмјери у циљу идентификовања и локализовања корисника других мобилних телефона или телефонских бројева, те се у том циљу могу тражити и додатни листинзи. У суштини, резимирајући претходно наведено, у циљу онемогућавања „заваравања" од стране криминалаца кориштењем и мијењањем неколико телефонских бројева и мобилних телефона у релативно краћем периоду (за вријеме вршења кривичних дјела или криминалних активности), криминалистички је исправно да се увијек када за то има индиција, на основу добијеног

листинга базне станице или на други начин идентификованог листинга, узму и додатни листинзи за све сумњиве ИМЕИ-е, МСИСДН-е, рјеђе и за ИМСИ-е. Адекватним, садржајним и сегментираним упоређивањем података и информација за тако добијене листинге могуће је доћи до додатних и даљих информација и података који могу да представљају значајне индиције у погледу конкретне криминалне активности или криминалне повезаности више лица – корисника тих мобилних телефона или телефонских бројева.

ОГРАНИЧЕЊА МОГУЋНОСТИ КОРИШТЕЊА ЛИСТИНГА ТЕЛЕКОМУНИКАЦИОНИХ БАЗНИХ СТАНИЦА

Из претходно наведеног је јасно да се могућности које пружају телекомуникационе базне станице, односно листинг базних станица може користити углавном у оперативне сврхе, односно да наведено има индицијални карактер, поготово уколико се на основу ових листинга, тј. могућности које омогућава листинг базних станица извлачи индиција у погледу (не)присутности на лицу мјеста. Међутим, и поред наведеног, постоји још неколико ограничења која се тичу тумачења и кориштења података и информација до којих се може доћи кориштењем могућности које пружа листинг телекомуникационих базних станица.

Већ је наведено да тзв. „аутоматски Хандовер“ подразумијева непримјетно „преузимање“ корисника од стране друге базне станице приликом кретања и преласка корисника са подручја које „покрива“ једна базна станица на подручје које „покрива“ друга базна станица. На овај начин, корисник аутоматски емитује (прима или шаље) сигнал, без обзира на то што у моменту емитовања прелази са подручја које „покрива“ једна базна станица на подручје које „покрива“ друга или чак и друге базне станице. Усљед наведеног, дешава се да у току релативно дуготрајних разговора само почетна и крајња базна станица (базне станице на чијем подручју је започета и завршена телекомуникациона активност) евидентирају телекомуникациону активност, „игноришући“ базне станице преко којих се, такође, у међувремену одвијала конкретна телекомуникациона активност, односно базне станице преко чијег подручја се корисник такође кретао у току трајања ове телекомуникационе активности. Ово је чест случај у урбаним подручјима, гдје се базне станице налазе на удаљености од неколико стотина метара, усљед чега и покривају релативно мало подручје (од неколико стотина до неколико квадратних километара у радијусу), док се корисник креће у наведеном простору непрестано се користећи услугама мобилне телефоније. Наведено изискује опрезност приликом тумачења листинга

ове базне станице у погледу нечије (не)присутности на одређеном подручју, поготово уколико се за критичан период његова присутност (посматрана кроз телекомуникациону активност регистровану на подручју које „покривају“ сусједне базне станице) очитава на сусједним подручјима. Усљед наведеног, неопходно је да се његова присутност у смислу индицијалног доказивања посматра и кроз телекомуникациону активност на подручјима које „покривају“ сусједне базне станице, а да се другим оперативно-тактичким мјерама и радњама, те истражним радњама локализује његова присутност за критичан период.

Слична са претходно наведеним је и могућност „преузимања“ корисника од стране сусједне базне станице. Наиме, техничке могућности, односно ограничења саме базне станице подразумијевају да се, уколико је она „загушена“ телекомуникационим саобраћајем у одређеном периоду, сигнали (позиви) са подручја које „покрива“ та базна станица или упућени ка корисницима који се налазе на подручју које „покрива“ та базна станица преусмјеравају на најближу, сусједну базну станицу, те да се са те базне станице (без обзира на то што она примарно не „покрива“ простор са којег се или на који се упућује сигнал) емитује сигнал. Јасно је да се на овај начин корисник служи базном станицом која примарно не „покрива“ подручје на ком се он налази, усљед чега ће сама база базне станице приликом исчитавања кроз листинг имати и његов сигнал, иако се он, мјесно посматрајући, у вријеме емитовања сигнала и није налазио на подручју те базне станице, већ у непосредној близини, односно на подручју сусједне базне станице. Као и у претходном случају, и овдје наведено изискује опрезност приликом тумачења листинга ових базних станица у погледу нечије (не)присутности на одређеном подручју, поготово уколико се као критичан период посматра период када је учесталост и велика фреквентност телекомуникационог саобраћаја на одређеном подручју.

У два претходно наведена случаја која ограничавају поузданост резултата које пружају базне станице у погледу нечије (не)присутности на одређеном подручју, што се посредно (индицијално) закључује кроз његову активност на мрежи мобилне телефоније, наравно, нису технички недостаци самих базних станица, већ одређени недостаци који ограничавају (али не елиминишу) оперативну употребљивост резултата који се добијају на основу ових базних станица. Међутим, с обзиром на карактеристике наведеног, може се рећи да су ограничења у погледу кориштења информација и података добијених на основу базе базне станице свакако техничког карактера.

С друге стране, присутно је и неколико ограничења у погледу беспоговорне валидности тумачења података и информација које се односе на индицију у погледу нечије (не)присутности на одређеном подручју посматране кроз његову телекомуникациону активност на

мрежи оператера мобилне телефоније. Ова ограничења се могу назвати оперативним ограничењима, с обзиром на то да нису, као у претходним случајевима, условљени техничким, већ искључиво одређеним практичним, односно оперативним аспектима тумачења, тј. извлачења одређених закључака на основу наведеног.

Први случај се односи на могућност да на одређеном подручју које је „покривено" базном станицом, иако осумњичени на њему борави, за вријеме боравка, односно за критичан период, из разних разлога, не остварује комуникацију (подразумијевајући под наведеним да нити позива, нити се позива, односно да нема ни слања, ни примања порука и позива). С обзиром на то да је немали број лица која се баве криминалним активностима свјесно могућности које мобилна телефонија пружа у откривању њихове криминалне активности, такви најчешће приликом учествовања у вршењу криминалних активности не користе мобилне телефоне, односно не користе се услугама мобилне телефоније, без обзира на то да ли са собом носе или уопште не носе мобилне телефоне. У овом случају, ови корисници најчешће не користе услуге мобилне телефоније непосредно током вршења кривичног дјела, али је немали и број оних који немају телекомуникациону активност преко телекомуникационих ресурса и одређени период прије и послије времена извршења самог кривичног дјела. Јасно је да се на основу изостанка телекомуникационе активности преко базне станице не може а приори извлачити доказ (већ само својеврсна индиција) у погледу његове невиности, односно неумијешаности у конкретну криминалну активност, усљед чега се алиби осумњичених лица мора провјеравати и на друге начине. Међутим, неопходно је указати на још једну индицију у погледу нечије криминалне активности која се може извући управо на основу телекомуникационе активности осумњиченог лица. Наиме, управо изостанак телекомуникационе активности осумњиченог лица у вријеме извршења кривичног дјела је индиција у погледу његове умијешаности у само кривично дјело уколико је евидентна учесталост телекомуникационе активности прије и након извршења кривичног дјела, а „нападно" изостаје управо и само у току извршења кривичног дјела. Наравно, и наведено представља само индицију, али свакако значајну, у погледу конкретизоване криминалне активности осумњиченог лица, поготово у комбинацији са другим индицијама у погледу његове конкретизоване криминалне активности. Наведено се мора посматрати у склопу телекомуникационе активности осумњиченог лица у дужем периоду (од неколико дана или чак седмица), као и у односу на његову телекомуникациону активност у вријеме претходно извршених кривичних дјела, односно у односу на чињеницу да ли му је, можда, претходна криминална активност откривена управо на основу индиција, информација, сазнања и доказа до којих се дошло

преко могућности које пружају базне станице, другим ријечима – да ли је упознат са могућностима које пружа телекомуникациона активност извршиоца приликом или непосредно прије или послије извршења кривичног дјела.

Насупрот наведеном, могућа је и ситуација да се преко листинга конкретне базне станице идентификује телефонски број или мобилни телефон лица за којег постоје индиције да се бави сличним кривичним дјелима, те да се наведено а приори, без претходног провјеравања његовог алибија или других релевантних чињеница и околности, посматра као индиција у погледу његове присутности на наведеном подручју (које је, најчешће, мјесто извршења кривичног дјела) у критичном периоду (које је, најчешће, вријеме извршења кривичног дјела). Наравно, овакво закључивање и коришћење индицијалног метода је брзоплето и погрешно, и то из неколико разлога, поготово уколико се (само) на основу ове индиције, без додатног провјеравања, приступи и планирању одређене оперативне активности, а потом и предузимању одређених оперативно-тактичких мјера и радњи и истражних радњи, не у циљу провјеравања, већ у циљу „потврђивања" наведене индиције. Неколико је фактора који ограничавају (али не елиминишу) коришћење индицијалног метода на овај начин у оперативном раду. Примарно се мора узети у обзир околност да припадници полиције никад са сигурношћу не знају да ли одређени телефонски број или мобилни телефон (увијек) користи исто лице, без обзира на то да ли је он осумњичени или не, односно да ли је лице из криминалног миљеа или није. Увијек се може десити и да ова лица другим лицима дају на послугу конкретан телефонски број или конкретан мобилни телефон и том приликом ће преко њега остварити комуникацију са подручја које „покрива" базна станица, након чега ће конкретан телефонски број или мобилни телефон вратити власнику, односно кориснику. Јасно је да ће се у овој ситуацији власник мобилног телефона или телефонског броја појавити као осумњичени, односно као корисник на одређеном подручју у одређено вријеме, иако он на наведеном подручју у спорно вријеме није ни боравио. Ово условљава брижљиво планирање и поступно извођење оперативно-тактичких мјера и радњи и истражних радњи у доказивању нечије криминалне активности, поготово уколико се основи сумње у погледу одређених лица заснивају само на овако добијеним подацима, односно на подацима и индицијама које су резултат листинга конкретне базне станице.

ЗАКЉУЧНА РАЗМАТРАЊА

Телекомуникационе базне станице су, сасвим сигурно, нашле своју примјену и у криминалистичком раду полиције. Криминалистички значај базних станица је вишеструк.

С једне стране, базне станице омогућавају посредну примјену индицијалног метода у погледу расвјетљавања кривичних дјела и откривања непознатих извршилаца конкретних кривичних дјела адекватним коришћењем индиције присутности на мјесту извршења или у непосредној близини корисника конкретизованог телефонског броја или мобилног телефона. С друге стране, на основу листинга телекомуникационих базних станица адекватним, благовременим и прилагођеним коришћењем могућности које пружају телекомуникационе базне станице (на основу листинга телекомуникационог саобраћаја реализованог преко ових базних станица), може да се дође до многобројних релевантних индиција, сазнања, информација и података о самом осумњиченом, односно о кориснику конкретизованог телефонског броја или мобилног телефона.

Конкретан резултат који омогућавају базне станице, односно листинг телекомуникационог саобраћаја остварен преко базних станица односи се, примарно, на утврђивање индиције присутности корисника на одређеном подручју за критичан период. Поред наведеног, конкретна активност у погледу могућности коришћења резултата телекомуникационе активности евидентиране у телекомуникационим базним станицама односи се на могућност накнадног својеврсног „праћења" одређених корисника, што је изузетно важно, имајући у виду предности овог начина „праћења", као и недостатке класичних облика праћења лица (велика могућност деконспирације, додатно ангажовање материјално-техничких и људских ресурса, временска ограничења...), без обзира на то да ли се предузимају као оперативно-тактичке радње или посебне истражне радње. Овај облик оперативне активности полиције посебно долази до изражаја код серијских кривичних дјела, односно код низа кривичних дјела у којима се једно или више лица доводе у везу са самим кривичним дјелима. Из наведеног је видљиво да телекомуникационе базне станице, са криминалистичког аспекта, омогућавају и идентификацију и локализацију корисника на одређеном подручју у циљу коришћења тако екстрахованих података у оперативне сврхе.

Међутим, сви подаци, информације и сазнања до којих се дође екстраховањем листинга телекомуникационих базних станица се могу посматрати само као индиције у погледу нечије криминалне активности, конкретизоване за одређено подручје и у одређено вријеме, а никако као

доказ. Ово је посљедица многобројних својеврсних ограничења техничког и практичног (оперативног) карактера која дјелимично, у већој или мањој мјери, утичу на индицију о идентификацији и локализацији конкретног корисника телефонског броја или мобилног телефона, посматрано кроз листинг базне станице. Усљед наведеног, јасно је да се наведени подаци могу користи само као индиције, наравно, не ограничавајући њихову употребну и доказну вриједност и у кривичном поступку, имајући у виду индицијално доказивање у кривичном поступку.

Наравно, фокусираност кориштења индиција добијених на основу листинга телекомуникационе базне станице у криминалистичке сврхе, те ограниченост примјене у кривичном поступку кроз индицијално доказивање не елиминише неопходност законитог поступања приликом изузимања, али и кориштења ових података, с обзиром на то да ови подаци представљају личне податке самих корисника мобилне телефоније, односно – њиховим незаконитим кориштењем се нарушавају основна људска права и слободе посматране примарно, али не и једино кроз нарушавање приватности и права на несметану личну комуникацију. Усљед наведеног, јасно је да се приликом поступања са листинзима телекомуникационих базних станица мора поступати само на начин прописан законским или подзаконским актима, чиме се елиминише или бар у великој мјери ограничава могућност злоупотребе овако добијених личних података.

ЛИТЕРАТУРА

Бача, М. (2004). *Увод у рачуналну сигурност*. Загреб: Народне новине.

Водинелић, В. (1972). *Криминалистика.* II поправљено и проширено издање. Београд: Савремена администрација.

Миладиновић, А. (2008). *Значај IMEI-а приликом расвјетљавања кривичних дјела.* Зборник радова „Примјена савремених метода и средстава у сузбијању криминалитета“, Интернационална асоцијација криминалиста, Брчко.

Митровић, Д., Сикимић, Н., (2010). *Системи за лоцирање мобилних јединица (телефона),* Криминалистичко-форензичка истраживања, Интернационална асоцијација криминалиста, Бања Лука, број 1.

ROLE AND IMPORTANCE (LISTING) TELECOMMUNICATION BASE STATIONS IN CRIMINAL WORK

Aleksandar Miladinovic,* MA

Abstract: Crime aspect of the base station is reflected in several segments that allow the arrival of certain data, information and knowledge regarding the indication of someone's (not) the presence in a particular area for a specific period. Operational use of the possibilities offered by the base station, and adequate and timely combination with other operational-tactical measures and investigative actions and operations can gain certain indications in terms of one's criminal activities, primarily through observing the indicated presence or absence of suspicious persons at the place of execution a criminal offense at the time of commission of the offense. Specifically, via base stations are, in an indirect way, for a certain time or for a certain period users can localize certain phone numbers or mobile phones in the area that ''cover'' base station. Also, base stations allow subsequent, indirect and customized 'tracking' of certain phone numbers, or user of mobile phone through the locating base stations through which communication exercise.

Keywords: telecommunications base stations, circumstantial methods, indications the presence of on-site telecommunications traffic, IMEI ...

* *Police Academy in Banja Luka, email: aaleksandarbl@yahoo.com.*