Univerza v Mariboru

Fakulteta za varnostne vede

Marko Furlan

MOBILNI TELEFON KOT DOKAZ V PREDKAZENSKEM POSTOPKU

Diplomsko delo
visokošolskega študijskega programa Varnost in policijsko delo

Ljubljana, november 2023

Univerza v Mariboru

Fakulteta za varnostne vede

MOBILNI TELEFON KOT DOKAZ V PREDKAZENSKEM POSTOPKU

Diplomsko delo

Študent: Marko Furlan

Študijski program: Visokošolski študijski program Varnost in policijsko delo

Mentor: prof. dr. Bojan Dobovšek

ZAHVALA

Zahvaljujem se mentorju prof. dr. Bojanu Dobovšku za vodenje pri pripravi diplomskega dela, obilo strokovnosti in vso ostalo pomoč. Hvala tudi moji družini, ki me je s svojo potrpežljivostjo in razumevanjem podpirala, dodatno motivirala in spodbujala med študijem.

MOBILNI TELEFON KOT DOKAZ V PREDKAZENSKEM POSTOPKU

Ključne besede: mobilni telefon, preiskava, zakonska podlaga.

UDK: 343.98.06(043.2)

Povzetek

Predmet raziskovanja diplomskega dela je mobilni telefon, katerega storilci kaznivih dejanj uporabljajo pri izvršitvi kaznivih dejanj, podatki na mobilnem telefonu pa pri preiskavi nato služijo kot ključni dokazi. Do vpogleda v podatke, ki so v mobilnem telefonu, ima pravico policija, vendar le na podlagi pisne izjave lastnika mobilnega telefona, da dovoljuje vpogled in zavarovanje podatkov mobilnega telefona. V kolikor lastnik mobilnega telefona ne dovoljuje vpogleda in zavarovanja podatkov, mora policija oziroma tožilstvo pridobiti odredbo od preiskovalnega sodnika, da lahko vpogled in zavarovanje opravi. Drugače je s podatki, ki jih hrani operater na podlagi telefonske številke naročnika, katere lahko policija pridobi le na podlagi pisne odredbe preiskovalnega sodnika, ki je izdana na upravičeno zahtevo državnega tožilstva, in sicer, če so podani razlogi za sum, da je bilo storjeno, da se izvršuje ali da se pripravlja oziroma organizira kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti in je za odkritje tega kaznivega dejanja ali storilca potrebno pridobiti podatke o prometu v elektronskem komunikacijskem omrežju. V diplomskem delu bomo predstavili, kako lahko mobilni telefon oziroma podatki na njem, služijo kot dokaz v predkazenskem postopku, saj storilci kaznivih dejanj s seboj nosijo mobilne telefone in imajo na njih ključne dokaze. Mobilne telefone policija nato v skladu z zakonom zaseže in izvede preiskovalne ukrepe v skladu z zakonom. Analizirali bomo dva praktična primera, ki sta javno dostopna, kjer je uporaba mobilnega telefona pri izvršitvi kaznivih dejanj služila kot ključen dokaz v predkazenskem in kazenskem postopku (Zakon o kazenskem postopku ZKP, 2021).

MOBILE PHONE AS EVIDENCE IN PRE-CRIMINAL PROCEDURE

Keywords: mobilephone, investigation, legal basis.

UDC: 343.98.06(043.2)

Abstract

The subject of the thesis research is a mobile phone, which criminals use to commit crimes, and the data on the mobile phone then serve as key evidence during the investigation. The police have the right to inspect the data contained in the mobile phone, but only on the basis of a written statement from the owner of the mobile phone that they allow the inspection and securing of the mobile phone data. If the owner of the mobile phone does not allow the inspection and securing of the data, the police or the prosecutor's office must obtain an order from the investigating judge in order to perform the inspection and securing. It is different with the data stored by the operator based on the telephone number of the subscriber, which the police can only obtain on the basis of a written order of the investigating judge, which is issued at the justified request of the state prosecutor's office, namely if there are reasons for suspecting that it has been committed , that a criminal act is being committed or that a criminal act is being prepared or organized, for which the perpetrator is being prosecuted ex officio, and in order to discover this criminal act or the perpetrator, it is necessary to obtain traffic data in the electronic communication network. In the thesis, we will present how a mobile phone or the data on it can serve as evidence in pre-trial proceedings, since criminals carry mobile phones with them and have key evidence on them. Mobile phones are then confiscated by the police in accordance with the law and investigative measures are carried out in accordance with the law. We will analyze two practical cases that are publicly available, where the use of a mobile phone in the commission of criminal acts served as key evidence in pre-trial and criminal proceedings (Act on Criminal Procedure ZKP, 2021).

KAZALO VSEBINE

KAZALO GRAFOV

KAZALO SLIK

UPORABLJENI SIMBOLI IN KRATICE

IMEI: International Mobile Equipment Identity (Mednarodna identiteta mobilne opreme)

IMSI: Mobile Subscriber Identity (Identiteta mobilnega naročnika)

SIM: Subscriber Identity Module (Modul identitete naročnika)

SMS: Short message (Kratko sporočilo)

MMS: Multimedia Messaging Service (Storitev večpredstavnostnega sporočanja)

KZ-1: Kazenski zakonik

RS: Republika Slovenija

TUL: Temelji na ustavni listini

ZEKom-1: Zakon o elektronskih komunikacijah

ZNPPol: Zakon o nalogah in pooblastilih policije

ZKP: Zakon o kazenskem postopku

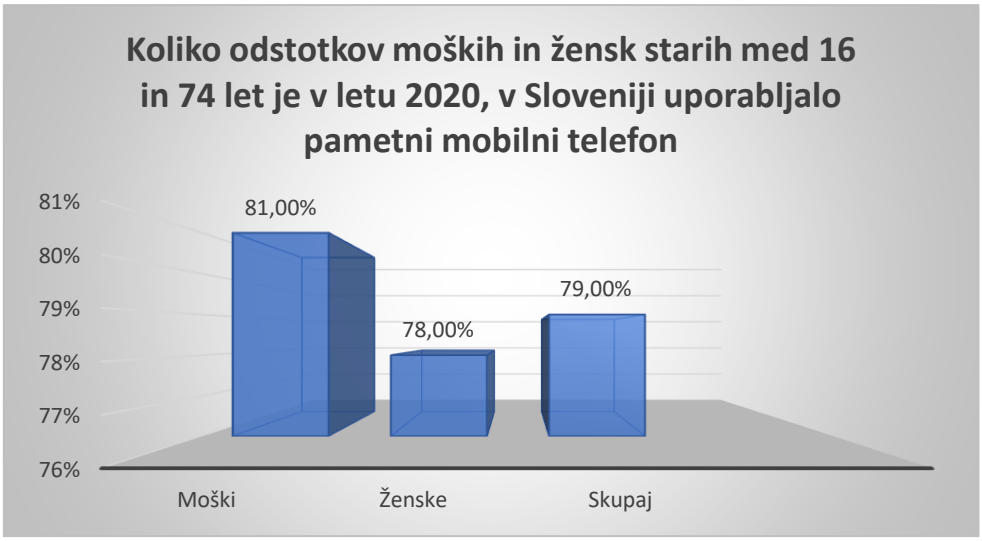
ZP-1: Zakon o prekrških

1 UVOD

Mobilni telefon je elektronska telekomunikacijska naprava, popolnoma prenosna in ne potrebuje žične povezave s telefonskim omrežjem, ima pa tudi osnovne zmožnostmi, ki so enake običajnemu stacionarnemu telefonu. Mobilni telefon je dandanes nepogrešljivo sredstvo, katerega uporablja 97% Slovencev in Slovenk starih med 16 in 74 let (Statistični urad RS 2020). Z mobilnim telefonom lahko uporabnik kliče, fotografira, brska po spletu in pridobiva podatke. Po definiciji je mobilni telefon imenovan tudi kot prenosni telefon ali mobitel, elektronska komunikacijska naprava, ki ima enake zmožnosti kot klasičen stacionaren telefon. Za razliko od stacionarnega telefona je mobilni telefon popolnoma prenosen in brez žice, povezan je s telefonskim omrežjem. Večina sodobnih mobilnih telefonov se v omrežje povezuje z oddajanjem in sprejemanjem radijskih valov, komunikacija pa poteka preko omrežja baznih postaj, s katerimi upravljajo različni operaterji oziroma ponudniki mobilnih storitev. V Sloveniji so to največji operaterji Telekom Slovenije, A1 in Telemach. Poleg zvočnega pogovora ima mobilni telefon številne dodatne storitve, kot so video klic, pošiljanje kratkih besedilnih sporočil ali na kratko imenovano SMS. Prav tako ima mobilni telefon, paketni prenos podatkov za dostop do svetovnega spleta – interneta in sprejemanja MMS sporočil (fotografije in video posnetki). Najsodobnejše naprave oziroma mobilni telefoni so tako imenovani pametni mobilni telefoni, kateri so zmožni opravljati naloge, za katere so bile do nedavnega potrebne posebne naprave. S pametnimi telefoni lahko predvajamo glasbo, posnemamo kvalitetne fotografije in video posnetke, poslušamo radio, igramo igrice in predvsem lahko uporabljamo aplikacije, ki nam pomagajo v vsakodnevnem življenju. Pametni mobilni telefoni imajo naprednejše računalniške sposobnosti in so znani tudi kot dlančniki, ki imajo vgrajen mobilni telefon. Pametni mobilni telefoni so zmožni pogajati najzahtevnejše aplikacije, ki so razvite na Java ME platformah, poganjajo pa platforme, ki so narejene v prid aplikacijskim razvijalcem. Pametne telefone lahko smatramo kot osebne žepne računalnike z dodanimi funkcijami mobilnega telefona, saj

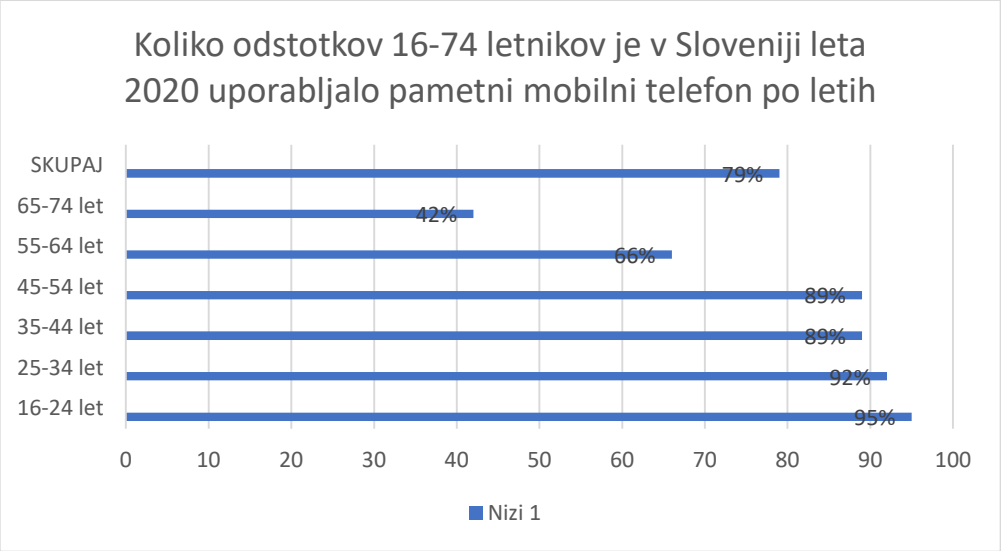
so ti telefoni navadni računalniki, le veliko manjši. Največji svetovni proizvajalci mobilnih telefonov so Apple, Samsung, Huawei, LG in ostali (Litchfield, 2010).

Statistični urad Republike Slovenije je za leto 2020, izvedel raziskavo o uporabi mobilnih telefonov med prebivalci Slovenije starih med 16 in 74 leti, in sicer po spolu (graf 1.1), po letih (graf 1.2) in po vrsti mobilnega telefona, katerega uporabljajo prebivalci Slovenije (graf 1.3) (Statistični urad RS , 2023).



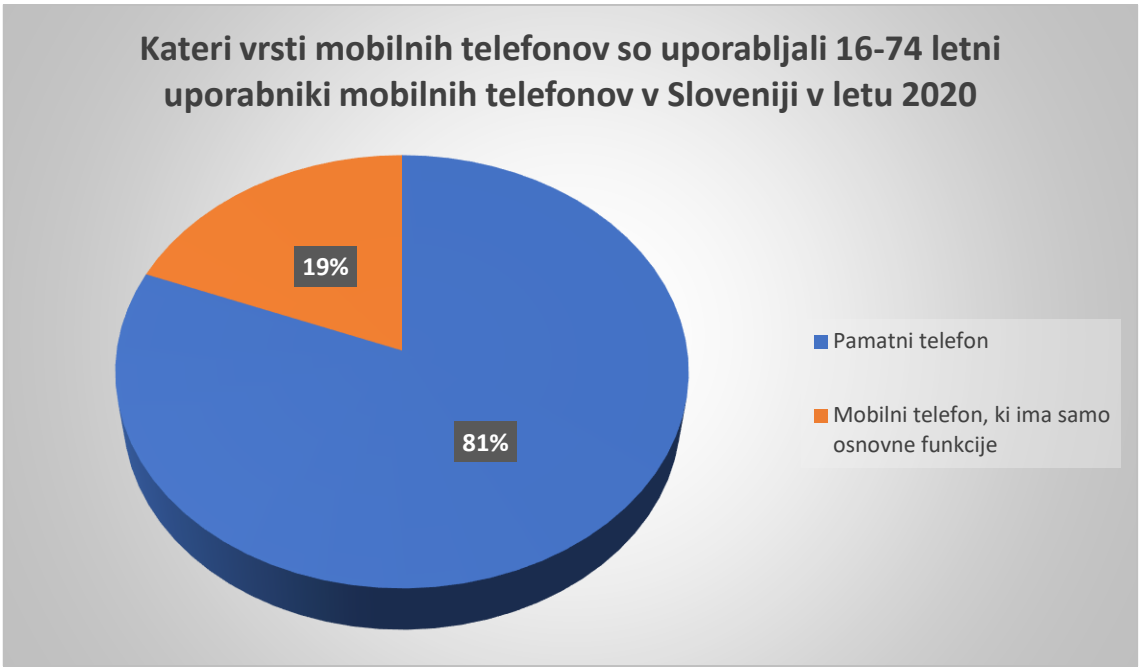
Graf 1. 1: Uporaba pametnih mobilnih telefonov v letu 2020 po spolu

(Statistični urad, 2023)



Graf 1. 2: Uporaba pametnih mobilnih telefonov v letu 2020 po starosti

(Statistični urad, 2023)



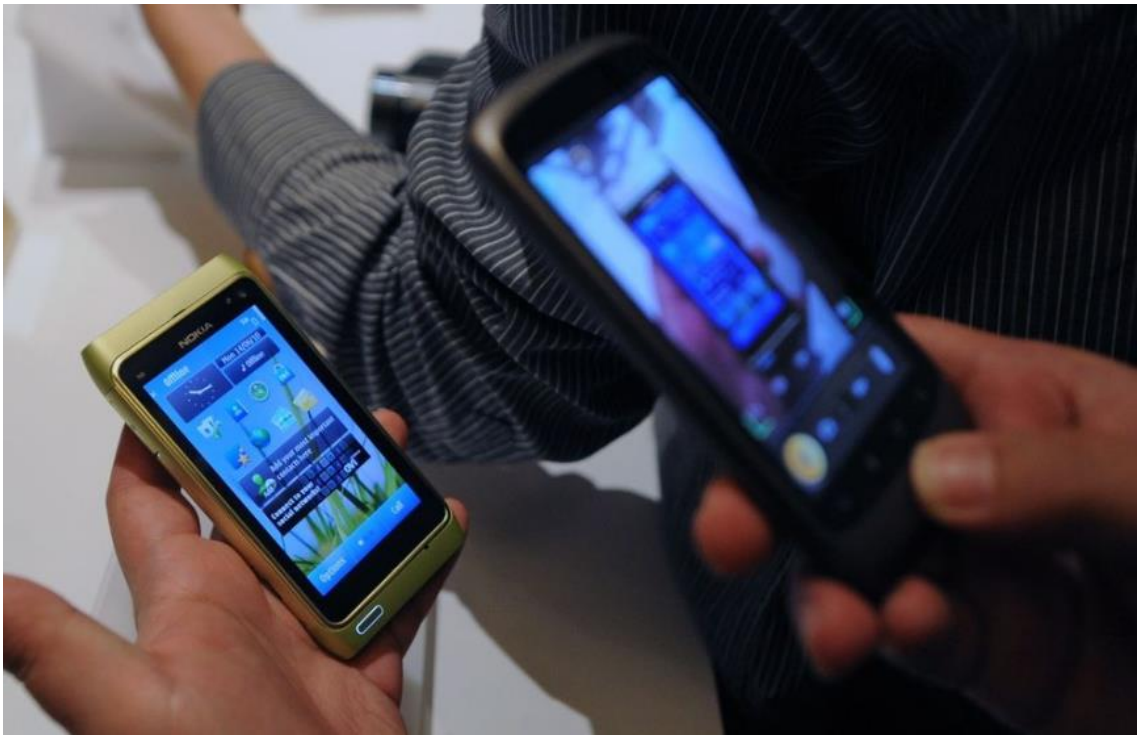
Graf 1. 3: Vrste uporabljenih mobilnih telefonov v letu 2020

(Statistični urad, 2023)

Ker je kot navedeno, uporaba mobilnih telefonov, predvsem pametnih mobilnih telefonov, ki služijo kot majhni prenosni računalniki, v populaciji tako razširjena, se tukaj takoj pojavijo razne nevarnosti in zlorabe pri uporabe mobilnih telefonov. Predvsem imamo tukaj v mislih odtujitev mobilnega telefona, na katerem so hranjeni razni podatki in je le-te mogoče zlorabiti. Prav tako je v današnjem sodobnem času, pri zelo razviti računalniški tehnologiji, vedno večja grožnja mobilnim telefonom, vdor v informacijski sistem mobilnega telefona, pri tem pa lahko pride do zlorabe osebnih podatkov, hranjenih fotografij in video posnetkov, bančnih podatkov in ostalih podatkov. Da zaščitimo sebe in podatke na mobilnem telefonu, pri zavarovanju uporabljamo razna gesla, vzorce in biometrijo, da hekerjem in tatovom onemogočimo dostop do naših osebnih podatkov, ki so hranjeni na mobilnem telefonu.

Mobilni telefon prav tako oddaja in prejema radijske valove, kateri potekajo preko baznih postaj, teh pa je na območju Slovenije vedno več. Z baznimi postajami na območju Slovenije, upravljajo naši največji operaterji Telekom Slovenije, A1 in Telemach. Preko baznih postaj potekajo vsi klici, ki jih opravljamo z mobilnim telefonom, poslana

SMS in MMS sporočila in brskanje po spletu. Bazne postaje ali javna mobilna in hibridna radijska omrežja so mobilna komunikacijska omrežja, ki delujejo v licenciranem spektru, katerih uporabo določata 2. in 3. odstavek, 33. člena Zakona o elektronskih komunikacijah, in sicer za mobilne komunikacije, kjer se učinkovita uporaba določene radijske frekvence lahko zagotovi le z omejitvijo števila izdanih določb o delitvi radijskih frekvenc in za mobilne komunikacije zagotovljenih javnih komunikacijskih storitev končnim uporabnikom. Javne mreže so mobilni sistemi, za katere je terminale mogoče kupiti v prosti prodaji, v sistemu pa jih je možno uporabljati samo s sklenjenim naročniškim razmerjem oziroma dovoljenjem operaterja. Med tovrstne sisteme uvrščamo GSM, UMTS, LTE, 5G, MMDS, BWA in MWS. Najsodobnejša tehnologija v današnjem času poteka preko 5G omrežja, ki bo vseboval veliko več inteligence in bo sposoben usklajevati manjše celice tako po velikosti kot pokrivanju. Zraven velikih celic bo vseboval tudi manjše celice, ki bodo omogočale veliko gostoto prenosnih hitrosti na posameznem področju. 5G omrežje je peta generacija mobilne telefonije, ki nadgrajuje prejšnje generacije 1G, 2G, 3G in 4G. Po definiciji Mednarodne komunikacijske zveze je 5G (NR) nova generacija mobilne telefonije, ki skladno z zahtevami Mednarodne telekomunikacijske zveze, na radijskem delu zagotavlja tri glavne uporabniške primere, in sicer podpora ekstremnih hitrosti prenosa za ekstremne količine podatkov in zakasnitve na uporabniškem nivoju največ 4 ms, podpora omrežnih komunikacij (minimalna zahteva milijon naprav na kvadratni kilometer) in podpora ultra zanesljivi komunikaciji in hitri komunikaciji z zakasnitvami na uporabniškem nivoju največ 1 ms (Agencija za komunikacijska omrežja in storitve Republike Slovenije). Iz vseh navedenih podatkov je mogoče sklepati, da vsa opravila, ki jih počnemo z mobilnim telefonom, potekajo preko baznih postaj in na podlagi tega je mogoče videti tudi lokacijo mobilnega telefona, kateri je označen z identifikacijsko številko IMEI. Da pa podatkov ne bi zlorabljali operaterji, ki z baznimi postajami in našimi osebnimi podatki upravljajo, je z Zakonom o elektronski komunikaciji (ZEKom-1), natančno določeno, kako morajo operaterji upravljati s podatki, ki jih ustvarja njihov naročnik (Zakon o elektronskih komunikacijah – ZEKom-1, 2017).



Slika 1. 1: Pametni mobilni telefoni prevzemajo prevlado

(Delo, 2010)

Podatki, kateri se ustvarjajo na in z uporabo mobilnih telefonov, spadajo v rubriko občutljivih osebnih podatkov do katerih lahko dostopa samo uporabnik mobilnega telefona, razen v izrednih situacijah lahko do teh podatkov dostopa policija, katera preiskuje kaznivo dejanje, ki se preganja po uradni dolžnosti. V zakonodaji mobilni telefoni ali mobilne naprave spadajo med elektronske in z njo povezane naprave ter nosilce elektronskih podatkov oziroma na kratko elektronske naprave, med katere spadajo tudi, telefaks, računalnik, disketa, optični mediji in spominske kartice. Policija pa do podatkov, ki se ustvarijo na in z uporabo mobilnega telefona, ne sme dostopati brez pisne privolitve lastnika mobilnega telefona, oziroma če se lastnik z vpogledom ne strinja, do podatkov ne sme dostopati brez odredbe sodišče. Izrecno lahko policija do podatkov dostopa samo z odredbo sodišča, katere hrani operater komunikacijskega omrežja. Vpogled v podatke mobilnega telefona in podatke, katere o naročniku hrani operater, pa je za policijo v današnjem času nujno potreben, saj se v mobilnih telefonih nahajajo podatki, ki lahko služijo kot dokaz v predkazenskem in kasneje tudi v kazenskem postopku (ZKP, 2021).

1.1 Cilji diplomskega dela

Cilj izdelave diplomskega dela je ugotoviti, kako lahko mobilni telefon, katerega uporablja storilec kaznivega dejanja pri izvršitvi kaznivega dejanja, vpliva na dokazovanje v predkazenskem in kasneje v kazenskem postopku.

Raziskovalna vprašanja:

- Kako so lahko podatki na mobilnem telefonu ključni za uspešno raziskovanje v kriminalističnih postopkih?
- Kako so lahko podatki baznih postaj pomemben vir za informacije pri ugotavljanje storilca na kraju izvršenega kaznivega dejanja?
- Ali obstaja povezanost med podatki, ki so hranjeni na mobilnem telefonu in samimi podatki iz baznih postaj, kakor tudi med ostalimi dokazi, ki so bili ugotovljeni pri preiskavi kaznivega dejanja?

1.2 Metode raziskovanja

Za izdelavo diplomskega dela bomo uporabili metode, kot so literatura, ki je navedena med viri, spletne strani, s katerimi si bomo pomagali pri pisanju in pridobivanju statističnih podatkov. Predvidoma bomo opravili analizo dveh primerov iz prakse, ki sta javno objavljena, s čimer bomo potrdili, da je mobilni telefon oziroma podatki na njem dokazno gradivo v predkazenskem postopku in kasneje tudi v kazenskem postopku.

2 ZAKONSKA PODLAGA ZA OBRAVNAVO KAZNIVIH DEJANJ

Najvišji pravni akt v Republiki Sloveniji (RS) je Ustava Republike Slovenije , ki je bila sprejeta 23. decembra 1991 in temelji na ustavni listini (TUL), ki je uredila razglasitev Republike Slovenije za samostojno in neodvisno državo in s tem povezana vprašanja ter zagotovitev varstva človekovih pravic in temeljnih svoboščin. V I. poglavju Ustave so določene splošne določbe akta, takoj v II. poglavju pa so določila glede človekovih pravic in svoboščin, katere v prvi vrsti mora upoštevati tudi policija pri opravljanju svojega dela. Ustavi nato sledi zakon, ki je v pravu osrednji pravni akt in pravni vir. Z njim se na ravni države urejajo najpomembnejša pravno relevantna družbena razmerja. Kot pravni akt je zakon voljno in zavestno dejanje, s katerim zakonodajalec (v moderni državi je to praviloma parlament) za neko področje na splošno določi norme (načela in pravila) družbenega vedenja in ravnanja. Kot pravni vir pa je zakon obvezno formalno izhodišče nadaljnjega, podzakonskega pravnega urejanja. Zakonu sledi podzakonski akt, ki je pravni akt z nižjo stopnjo od zakona, kar pomeni, da mora biti sprejet in izvajan v skladu s postopkom, ki ga postavi zakon, njegova vsebina mora biti v skladu z zakonom. Podzakonski akt sprejme državni organ, organ lokalne skupnosti ali nosilec javnega pooblastila. Podzakonski akti državnih organov so uredbe in sklepi vlade, navodila, pravilniki ministrstev, upravne odločbe in sklepi upravnih enot, inšpektoratov in drugih organov v sestavi ministrstev ter javnih agencij, javnih skladov in javnih zavodov ter javnih podjetij, splošni akti za izvrševanje javnih pooblastil od nosilcev javnih pooblastil, sodbe in sklepi sodišč. Za sprejetje je načeloma potrebno izrecno zakonsko pooblastilo (Miro Cerar, 2009 in Europena Justice, 2019).

Policija mora pri svojem vsakodnevnem delu upoštevati Ustavo RS, zakonske in podzakonske akte, katere je določil zakonodajalec. Krovni zakon, kjer ima policija navedena vsa svoja pooblastila, je Zakon o nalogah in pooblastilih policije (v nadaljnjem besedilu: ZNPPol), pri preiskavi kaznivih dejanj pa mora policija postopati po Zakonu o kazenskem postopku (v nadaljnjem besedilu: ZKP), kjer so navedene vse podrobnosti

postopkov, ki so pomembni za obravnavo kaznivih dejanj. Sankcije, ki sledijo nekomu, ki je izvršil kaznivo dejanje, pa so navedene v Kazenskem zakoniku Republike Slovenije (v nadaljnjem besedilu: KZ-1).

V ZNPPol so določene naloge policije, ki izhajajo iz njenih temeljnih dolžnosti, med katere sodi tudi preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, odkrivanje in prijemanje storilcev kaznivih dejanj, zbiranje dokazov ter raziskovanje okoliščin, ki so pomembne za ugotovitev premoženjske koristi, ki izvira iz kaznivih dejanj (ZNPPol, 2021, čl. 4). Vsa nadaljnja pooblastila policije, ki se nanašajo na obravnavo in preiskovanje kaznivih dejanj, pa policiji in ostalim organom narekuje ZKP.

Ko obstajajo razlogi za sum, da je bilo storjeno kaznivo dejanje, katero se preganja po uradni dolžnosti, mora policija ukreniti potrebno, da se izsledi storilec kaznivega dejanja, da se storilec ali udeleženec ne skrije ali ne pobegne, da se odkrijejo in zavarujejo sledovi kaznivega dejanja in predmeti, ki utegnejo biti dokaz in da se zberejo vsa obvestila, ki bi utegnila biti koristna za uspešno izvedbo kazenskega postopka. To je krovno pooblastilo policistom, s katerim imajo policisti zakonsko podlago, da sploh začnejo s preiskovanjem kaznivega dejanja (ZKP, 2021).

Ko je bilo izvršeno kaznivo dejanje, katero se preganja po uradni dolžnosti, so policisti dolžni kaznivo dejanje od naznanitelja sprejeti in opraviti postopek zbiranja obvestil s katerim bodo lahko prišli do storilca kaznivega dejanja in bodo zbrali vse potrebne dokaze, kateri bodo služili kot dokaz v kazenskem postopku. Prav tako morajo policisti v določenih kaznivih dejanjih opraviti ogled, pri čemer morajo zavarovati vse predmete in sledi, s katerimi se bo kaznivo dejanje v kazenskem postopku dokazovalo na sodišču (ZKP, 2021).

2.1 Zbiranje obvestil

ZKP daje policiji generalno pooblastilo za izvajanje ukrepov pri preiskovanju kaznivih dejanj. Temeljna podlaga za njeno delovanje v predkazenskem postopku je 148. člen ZKP (ZKP, 2021).

V prvem odstavku 148. člena ZKP je določeno, da mora policija, v kolikor so podani razlogi za sum, da je bilo storjeno kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti, ukreniti vse potrebno, da se storilec izsledi ali da se prepreči, da bi se storilec ali udeleženec skril ali pobegnil. Prav tako mora policija ukreniti vse potrebno, da se odkrijejo in zavarujejo vse sledi kaznivega dejanja in tudi predmeti, ki bi v nadaljnjem kazenskem postopku lahko služili kot dokaz ter da se zberejo vsa obvestila, ki bi utegnila biti koristna za nadaljnjo uspešno izvedbo kazenskega postopka (ZKP, 2021).

V drugem odstavku 148. člena ZKP je določeno, da če policija izvrši naloge iz prvega odstavka 148. člena ZKP, sme zahtevati potrebna obvestila od oseb, opraviti potreben pregled prevoznih sredstev, potnikov in prtljage, za nujno potreben čas omejiti gibanje na določenem prostoru, ukreniti, kar je potrebno v zvezi z ugotavljanjem istovetnosti oseb in predmetov; razpisati iskanje osebe in stvari, ki se iščejo, v navzočnosti odgovorne osebe opraviti pregled določenih objektov in prostorov podjetij in drugih pravnih oseb ter pregledati njihovo določeno dokumentacijo ter ukreniti in storiti vse drugo, kar je potrebno. O dejstvih in okoliščinah, ki se ugotovijo pri posameznih dejanjih in utegnejo biti pomembne za kazenski postopek in o predmetih, ki so bili najdeni ali zaseženi, se napravi zapisnik ali uradni zaznamek (ZKP, 2021).

V nadaljnjih odstavkih 148. člena ZKP je navedeno, kako mora policija postopati z osumljenci kaznivih dejanj, pritožba, razgovor s priporniki in da policija, ko zbere vsa obvestila in dokaze, o tem obvešča pristojno Okrožno državno tožilstvo z kazensko

ovadbo ali poročilom. S poročilom policija Okrožno državno tožilstvo obvešča, če na podlagi zbranih obvestil ni podlage za kazensko ovadbo (ZKP, 2021).

2.2 Ogled in zaseg predmetov

Policija zavaruje vse dokaze na ta način, da na kraju storitve kaznivega dejanja lahko opravi tudi ogled kraja. Ogled kraja kaznivega dejanja je procesno dejanje, opravilo in se ga opravi vedno, ko je za ugotovitev ali razjasnitev kakšnega pomembnega dejstva v postopku nujno neposredno opazovanje. Je hkrati tudi kriminalistično opravilo, saj z ogledom iščemo in zavarujemo sledi kaznivega dejanja, ki bodo policiji pomagale razjasniti njegove okoliščine in izslediti storilca. Ogledna dejavnost je enkratno in neponovljivo dejanje, zato je dolžnost izvedbe prvih nujnih ukrepov na kraju. Ogled kraja kaznivega dejanja se opravi, kadar je za ugotovitev ali razjasnitev katerega pomembnega dejstva v postopku nujno neposredno opazovanje oziroma zaznavanje, in sicer zavarovanje sledi in ostalih dokaznih predmetov (ZKP, 2021).

Splošno pooblastilo za zaseg predmetov, ki se morajo po kazenskem zakonu vzeti ali tisti, ki utegnejo biti dokazilo v kazenskem postopku, je policistom naloženo v 4. odstavku 220. člena ZKP, kateri določa, da policisti smejo zaseči predmete, ki se morajo po kazenskem zakonu vzeti ali ki utegnejo biti kot dokazilo v kazanskem postopku, kadar postopajo po 148. in 164. členu ZKP ali kadar izvršujejo nalog sodišča (izvršitev odredbe za hišno preiskavo) (ZKP, 2021).

2.3 Preiskava stanovanja in drugih prostorov po odredbi sodišča

Po samem zbiranju dokazov mora policija in njeni preiskovalci pretehtati ali obstajajo utemeljeni razlogi za sum, da je neka oseba storila kaznivo dejanje, na podlagi česar policija poda predlog za izvedbo hišne preiskave. Utemeljeni razlogi za sum je dokazni standard, ki je določen za nekatere najgloblje posege v pravice ljudi.

ZKP v 214. členu določa, da se preiskava stanovanja in drugih prostorov obdolženca ali drugih oseb sme opraviti, če so podani utemeljeni razlogi za sum, da je določena oseba storila kaznivo dejanje in je verjetno, da bo mogoče pri preiskavi obdolženca prijeti ali da se bodo odkrili sledovi kaznivega dejanja ali predmeti, ki so pomembni za kazenski postopek. Osebna preiskava se sme opraviti, če so podani utemeljeni razlogi za sum, da je določena oseba storila kaznivo dejanje in je verjetno, da se bodo pri preiskavi našli sledovi in predmeti, ki so pomembni za kazenski postopek (ZKP, 2021).

Preiskavo odredi sodišče z obrazloženo pisno odredbo. Odredba o preiskavi se izroči pred začetkom preiskave tistemu, pri katerem naj se preiskava opravi ali ki naj se preišče. Pri tem se ga pouči, da ima pravico obvestiti odvetnika, ki je lahko navzoč pri preiskavi. Če tisti, na katerega se nanaša odredba o preiskavi zahteva, da je pri preiskavi navzoč odvetnik, se začetek preiskave odloži do prihoda odvetnika, vendar najdlje za dve uri. Pred začetkom preiskave se od tistega, na katerega se nanaša odredba o preiskavi zahteva, da naj prostovoljno izroči osebo oziroma predmete, ki se iščejo. S preiskavo se lahko začne tudi brez poprejšnje izročitve odredbe in brez poprejšnje zahteve za izročitev osebe ali stvari, če se pričakuje oborožen odpor ali če je potrebno, da se preiskava opravi takoj in nepričakovano, ali če se opravi preiskava v javnih prostorih. Preiskava se praviloma opravlja med 6. in 22. uro. Opravlja se lahko tudi izven tako določenega časa, če se je v njem začela pa se do 22. ure še ni končala ali če so podani razlogi iz 218. člena ZKP ali če preiskovalni sodnik oceni, da bi zaradi odlašanja lahko bili uničeni sledovi kaznivega dejanja oziroma predmeti, pomembni za kazenski postopek in to posebej dovoli. Določbe tega in ostalih členov, ki se nanašajo na hišno in osebno preiskavo, se smiselno uporabljajo tudi za preiskavo skritih prostorov prevoznih sredstev (ZKP, 2021).

V 216. členu ZKP, ki se prav tako nanaša na hišno preiskavo, pa je podrobneje opisan postopek izvedbe hišne preiskave, in sicer pri hišni preiskavi ima pravico biti navzoč tisti, čigar stanovanje ali prostor se preiskuje ali njegov zastopnik. Zaklenjeni prostori, pohištvo ali druge stvari se odprejo s silo samo, če njihov imetnik ni navzoč ali če jih noče

prostovoljno odpreti. Pri odpiranju se je treba ogibati nepotrebnih poškodb. Pri hišni ali osebni preiskavi morata biti kot priči navzoči dve polnoletni osebi. Preiskavo ženske sme opraviti samo ženska; tudi za priče se vzamejo samo ženske. Priče je treba pred začetkom preiskave opozoriti, da pazijo, kako se preiskava opravlja in da imajo pred podpisom zapisnika o preiskavi pravico podati svoje ugovore, če mislijo, da vsebina zapisnika ni pravilna. Če se opravi preiskava v prostorih državnih organov, podjetij ali drugih pravnih oseb, se povabi njihov predstojnik, ki naj bo pri preiskavi navzoč. Če se opravi preiskava v vojaškem objektu, se povabi pristojni vojaški starešina, ki naj bo pri preiskavi navzoč. Hišno in osebno preiskavo je treba opraviti obzirno, da se ne moti hišni mir. O vsaki hišni ali osebni preiskavi se napravi zapisnik, ki ga podpiše tisti, pri katerem se opravi preiskava ali ki se ga preišče, njegov zastopnik, če je bil navzoč pri preiskavi in tisti, katerih navzočnost je obvezna. Pri preiskavi se zasežejo samo tisti predmeti oziroma listine, ki so v zvezi z namenom preiskave v posameznem primeru. V zapisnik se vpišejo in v njem natančno opišejo predmeti oziroma listine, ki se zasežejo. Zapisnik se izda tistemu, pri katerem se opravi preiskava ali ki se ga preišče oziroma njegovemu zastopniku (ZKP, 2021).

Pri hišni preiskavi je zelo pomembno upoštevati določila 217. člena ZKP, kateri govori o tem, da če se pri hišni ali osebni preiskavi najdejo predmeti, ki niso v zvezi s kaznivim dejanjem, zaradi katerega je bila preiskava odrejena, pač pa kažejo na drugo kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti, se tudi ti opišejo v zapisniku in zasežejo. To se takoj sporoči državnemu tožilcu, da začne kazenski pregon. Ti predmeti se takoj vrnejo, če državni tožilec spozna, da ni razloga za kazenski pregon, pa tudi ne kakšnega drugega zakonskega razloga, da bi se morali predmeti vzeti (ZKP, 2021).

Pri hišnih preiskavah preiskovalci velikokrat naletijo prav na takšne predmete, ki niso navedeni v odredbi za hišno preiskavo. V kolikor preiskovalci v preiskavi najdejo predmete, ki jih je potrebno zaseči po Zakonu o prekrških, le-te zapišejo v Zapisnik o hišni preiskavi in jih nato zasežejo na podlagi 123. člena Zakona o prekrških (v nadaljnjem

besedilu ZP-1), ob tem pa izpolnijo tudi Potrdilo o zasegu predmetov, katerega se zraven Zapisnika o opravljeni hišni preiskavi vroči preiskovancu (ZKP, 2021).

Policija pri izvedbi preiskave stanovanja in drugih prostorov po odredbi sodišča, če je to določeno v odredbi, zaseže tudi vse elektronske naprave, med katere spada tudi mobilni telefon, za kar mora po izvedbi preiskave stanovanja in drugih prostorov pridobiti pisno privolitev za preiskavo zaseženih naprav, na katerih se nahajajo morebitni dokazi, s katerim se dokazuje kaznivo dejanje (ZKP, 2021).

2.4 Odvzemi prostosti in odreditev pridržanja

Odvzem prostosti in pridržanje ima policija določeno v več zakonodajah, in sicer v Zakonu o prekrških, ZNPPol-u, Zakonu o pravilih cestnega prometa in Zakonu o nadzoru državne meje. Odvzem prostosti in pridržanje, ki se nanaša na obravnavo in preiskovanje kaznivih dejanj, pa je določeno v 157. členu ZKP.

Prvi odstavek 157. člena ZKP se uporablja za storilce, kateri so izvršili kaznivo dejanje in je policija oziroma njeni preiskovalci o tem kaznivem dejanju že zbrala vsa obvestila, pridobila vse predmete kaznivega dejanja in je storilca potrebno samo še zaslišati oziroma od njega zbrati obvestila po ZKP. Zatem ga policisti s kazensko ovadbo in njegovo izjavo privedejo k preiskovalnemu sodniku. Predhodno se preiskovalci o tem morajo posvetovati z DT, kateri usmerja predkazenski postopek in odloča o tem ali bo priporne razloge, ki so navedeni v nadaljevanju, predlagal sodišču (ZKP, 2021).

Drugi odstavek 157. člena ZKP določa, da smejo policisti izjemoma nekomu vzeti prostost in ga pridržati. To kaže na to, da odvzem prostosti in pridržanje za policiste ni obvezno, se pa mora izvesti, če so podani vsi zakonski pogoji. V tem odstavku je določeno, da morajo biti podani utemeljeni razlogi za sum, da je nekdo storil kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti, če je pridržanje potrebno zaradi ugotovitve istovetnosti, preverjanja alibija, zbiranja obvestil in dokaznih

predmetov o tem kaznivem dejanju. Obvezno se morajo pridržali in priporni razlogi med seboj povezovati. V nadaljevanju tega odstavka so navedeni priporni razlogi, kateri izhajajo iz 1., 2 in 3. točke prvega odstavka 201. člena ZKP in iz 1. in 2. točke prvega odstavka 432. člena ZKP. V primeru iz 2. točke prvega odstavka 201. člena ZKP pa obstajajo priporni razlogi le, če je opravičena bojazen, da bo ta oseba uničila sledove kaznivega dejanja (ZKP, 2021).

Kot navedeno so priporni razlogi navedeni v 201. členu ZKP, kjer je določeno, da se »pripor sme odrediti zoper osebo, če se skriva, če ni mogoče ugotoviti njene istovetnosti ali če so druge okoliščine, ki kažejo na nevarnost, da bi pobegnila, če je upravičena bojazen, da bo uničila sledove kaznivega dejanja, ali če posebne okoliščine kažejo, da bo ovirala potek kazenskega postopka s tem, da bo vplivala na priče, udeležence ali prikrivalce, če teža, način storitve ali okoliščine, v katerih je bilo kaznivo dejanje storjeno in njene osebne lastnosti, prejšnje življenje, okolje in razmere v katerih živi ali kakšne druge posebne okoliščine kažejo na nevarnost, da bo ponovila kaznivo dejanje, dokončala poskušeno kaznivo dejanje ali storila kaznivo dejanje, s katerim grozi«. Določila tega 201. člena se uporabljajo predvsem za kazniva dejanja, ki se preganjajo po uradni dolžnosti, za katere je zagrožena zaporna kazen petih let (ZKP, 2021).

Drugače so določeni priporni razlogi v 432. členu ZKP, saj so tukaj prav opredeljena kazniva dejanja, pri katerih se sme odrediti pripor, in sicer na obrazložen predlog tožilca se pripor sme izjemoma odrediti zoper tistega, za katerega je utemeljen sum, da je storil kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti, če se skriva, če se ne da ugotoviti njegova istovetnost ali če so podane druge okoliščine, ki očitno kažejo na nevarnost, da bo sicer pobegnil, če gre za kaznivo dejanje zoper javni red in mir, zoper spolno nedotakljivost ali za kaznivo dejanje s prvinami nasilja, za katera se sme izreči kazen zapora dveh let ali za druga kazniva dejanja, za katera se lahko izreče kazen zapora treh let, kadar je podan razlog za pripor iz 2. ali 3. točke prvega odstavka 201. člena ZKP (ZKP, 2021).

Pri odvzemu prostosti in pridržanju morajo policisti obvezno upoštevati segmente, ki se med seboj povezujejo, in sicer obstoj pridržanih razlogov (zaradi ugotovitve istovetnosti, preverjanja alibija, zbiranja obvestil in dokaznih predmetov o tem kaznivem dejanju), ki se morajo povezovati s pripornimi razlogi. V nadaljnjih odstavkih 157. člena ZKP so določeni postopki pri odvzemu prostosti in pridržanju, katere morajo policisti pri izvedbi le-teh upoštevati. Ko policija izvaja odvzem prostosti in pridržanje, pri tem storilcem, z namenom dokazovanja kaznivega dejanja, zaseže tudi mobilni telefon (ZKP, 2021).

3 ZAKONSKA UREDITEV ZA PREISKAVO MOBILNIH NAPRAV

Kot navedeno v drugem poglavju tega diplomskega dela, ima policija po Zakonu o kazenskem postopku pooblastilo, da od oseb sprejema ustne kazenske ovadbe, zbira obvestila, zasega predmete, opravlja hišne preiskave po odredbi sodišča in brez njih ter lahko osebi, ki je izvršila kaznivo dejanje, ki se preganja po uradni dolžnosti, odvzame prostost in odredi pridržanje. Pri teh splošnih pooblastilih policija lahko storilcu, ki je izvršil kaznivo dejanje in ostalim osebam, da bi dokazala kaznivo dejanje, katero policija obravnava, odvzame oziroma po zakonu zaseže tudi mobilne naprave, katere lahko na podlagi Zakona o kazenskem postopku tudi preišče in s strani operaterja pridobi podatke o naročniku oziroma lastniku mobilne naprave ter vse ostale podatke (opravljeni klici, bazne postaje, ki so zabeležile lokacijo mobilne naprave, …) (ZKP, 2021).

3.1 Preiskava vsebine elektronskih in mobilnih naprav

Pooblastilo za preiskavo elektronskih in mobilnih naprav je policiji naložena v celotnem 219a. členu ZKP, kjer je v prvem odstavku navedeno, da ko policija zaseže elektronske oziroma mobilne naprave s katerimi bo dokazovala izvršeno kaznivo dejanje, preiskavo elektronskih in z njo povezanih naprav ter nosilcev elektronskih podatkov kot so telefon, telefaks, računalnik, disketa, optični mediji in spominske kartice, zaradi pridobitve podatkov v elektronski obliki lahko opravi, če so podani utemeljeni razlogi za sum, da je bilo storjeno kaznivo dejanje in je podana verjetnost, da elektronska naprava vsebuje elektronske podatke, na podlagi katerih je mogoče osumljenca ali obdolženca identificirati, odkriti, prijeti ali odkriti sledove kaznivega dejanja, ki so pomembni za kazenski postopek, ali ki jih je mogoče uporabiti kot dokaz v kazenskem postopku (ZKP, 2021).

Drugi, tretji, četrti in peti odstavek pravijo, da se preiskava mobilne naprave lahko izrecno opravi na podlagi pisne privolitve imetnika elektronske oziroma mobilne

naprave v primeru, da obstajajo utemeljeni razlogi za sum, da je bilo storjeno kaznivo dejanje. V kolikor pa imetnik elektronske naprave pisno ne privoli v preiskavo, policija na pristojno Okrožno državno tožilstvo poda predlog za izdajo odredbe o preiskavi vsebine zasežene elektronske naprave. Preiskovalni sodnik izda odredbo za preiskavo elektronske naprave na pisno obrazložitev tožilstva. Zelo pomembno določilo tega odstavka je, da če se preiskava opravi na podlagi odredbe sodišča, se izvod te odredbe pred začetkom preiskave izroči imetniku oziroma uporabniku elektronske naprave, ki naj se preišče. Izjemoma, če pisne odredbe ni mogoče pravočasno pridobiti ter če obstaja neposredna in resna nevarnost za varnost ljudi ali premoženja, lahko preiskovalni sodnik na ustni predlog državnega tožilca odredi preiskavo elektronske naprave z ustno odredbo. O predlogu državnega tožilca in odredbi preiskovalni sodnik izdela uradni zaznamek. Pisna odredba mora biti izdana najpozneje v dvanajstih urah po izdaji ustne odredbe, sicer policija, ki je odredbo izvršila, zapisniško uniči ali izbriše shranjene ali kopirane podatke in o tem v osmih dneh obvesti preiskovalnega sodnika, državnega tožilca in imetnika oziroma uporabnika elektronske naprave, če je znan. Če se preiskava elektronske naprave odredi v odredbi za hišno ali osebno preiskavo, za izdajo tega dela odredbe in njeno izvršitev, veljajo pogoji in postopki iz tega člena. V tem primeru tudi predlog za hišno ali osebno preiskavo poda državni tožilec. Predlog in odredba o preiskavi elektronske naprave morata vsebovati podatke, ki omogočajo identifikacijo elektronske naprave, ki se bo preiskala, utemeljitev razlogov za preiskavo, opredelitev vsebine podatkov, ki se iščejo in druge pomembne okoliščine, ki narekujejo uporabo tega preiskovalnega dejanja in določajo način njegove izvršitve (ZKP, 2021).

V šestem odstavku je določeno, da imetnik oziroma uporabnik elektronske naprave mora omogočiti dostop do naprave, predložiti šifrirne ključe oziroma šifrirna gesla in pojasnila o uporabi naprave, ki so potrebna, da se doseže namen preiskave. Če noče tako ravnati, se sme kaznovati oziroma zapreti po določbi drugega odstavka 220. člena ZKP, razen če gre za osumljenca ali obdolženca ali osebo, ki ne sme biti zaslišana kot priča ali se je v skladu s tem zakonom odrekla pričevanju (ZKP, 2021).

Vsi nadaljnji odstavki do vključno desetega odstavka določajo kdo in kako lahko izvede preiskavo mobilne naprave. Preiskava se opravi tako, da se ohrani integriteta izvirnih podatkov in možnost njihove uporabe v nadaljnjem postopku. Preiskava mora biti opravljena na način, s katerim se v najmanjši možni meri posega v pravice oseb, ki niso osumljenci ali obdolženci in varuje tajnost oziroma zaupnost podatkov ter se ne povzroča nesorazmerna škoda. Preiskavo opravi strokovno usposobljena oseba. O preiskavi se napravi zapisnik, ki med drugim obsega identifikacijo elektronske naprave, ki je bila pregledana:

- datum ter uro začetka in konca preiskave oziroma ločeno za več preiskav, če preiskava ni bila opravljena v enem delu;
- morebitne sodelujoče in navzoče osebe pri preiskavi;
- številko odredbe in sodišče, ki jo je izdalo;
- način izvedbe preiskave;
- ugotovitve preiskave in druge pomembne okoliščine.

Če se pri preiskavi najdejo podatki, ki niso v zvezi s kaznivim dejanjem, zaradi katerega je bila preiskava odrejena, temveč kažejo na drugo kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti, se zasežejo tudi ti. To se navede v zapisnik in takoj sporoči državnemu tožilcu, da začne kazenski pregon. Ti podatki pa se takoj uničijo, če državni tožilec spozna, da ni razloga za kazenski pregon in tudi ne kakšnega drugega zakonskega razloga, da bi se morali podatki vzeti. O uničenju se sestavi zapisnik. Če v tem členu ni določeno drugače, se za odreditev in izvršitev odredbe o preiskavi elektronske naprave smiselno uporabljajo določbe tretjega in četrtega odstavka 215. člena ter četrtega, petega in sedmega odstavka 216. člena ZKP (ZKP, 2021).

Zelo pomembno določilo je navedeno v enajstem odstavku in sicer, če je bila preiskava elektronske naprave opravljena brez odredbe sodišča ali v nasprotju z njo ali brez pisne privolitve imetnika oziroma lastnika naprave, sodišče svoje odločbe ne sme opreti na zapisnik o preiskavi in na tako pridobljene podatke (ZKP, 2021).

3.1.1 Zakonska podlaga za praktično izvedbo preiskave elektronskih in mobilnih naprav

V Zakonu o kazenskem postopku je točno določena izvedba preiskave zasežene elektronske naprave, na podlagi česar se pridobijo in zavarujejo vsi podatki, ki nadalje policiji služijo kot dokaz v predkazenskem postopku. V 223.a členu ZKP je določeno, da če se zaseže elektronska naprava zaradi oprave preiskave, se podatki v elektronski obliki zavarujejo tako, da se shranijo na drug ustrezen nosilec podatkov na način, da se ohrani istovetnost in integriteta podatkov ter možnost njihove uporabe v nadaljnjem postopku ali se izdela istovetna kopija celotnega nosilca podatkov, pri čemer se zagotovi integriteta kopije teh podatkov. Če to ni mogoče, se elektronska naprava zapečati, če je mogoče, pa samo tisti del elektronske naprave, ki naj bi vseboval iskane podatke. Nosilci podatkov, na katere se zavarujejo podatki so CD-zgoščenke, DVD-zgoščenke, Blury-zgoščenke, USB ključi in zunanji trdi disk. Mobilne naprave v današnjem času imajo v sami napravi veliko prostora za shranjevanje podatkov, zato se podatki lahko posnamejo v večini na Blury-zgoščenke, USB ključe z večjo prostornino za shranjevanje podatkov in na zunanje trde diske (ZKP, 2021).

Nadalje je v 223.a členu določeno, da če je bila elektronska naprava zasežena brez odredbe sodišča in je bila zaradi zavarovanja podatkov izdelana njihova kopija, vendar sodišče v dvanajstih urah ni izdalo odredbe za preiskavo po petem odstavku 219.a člena ZKP oziroma ni bila dana privolitev po drugem odstavku 219.a člena ZKP, policija zapisniško trajno uniči izdelano kopijo in o tem v osmih dneh pisno obvesti preiskovalnega sodnika, državnega tožilca in imetnika oziroma uporabnika elektronske naprave, če je le ta znan. Imetnik, uporabnik, upravljavec ali skrbnik elektronske naprave oziroma tisti, ki ima do nje dostop, mora na zahtevo organa, ki jo je zasegel, takoj ukreniti, kar je potrebno in je v njegovi moči, da se onemogoči uničenje, spreminjanje ali prikrivanje podatkov. Če noče tako ravnati, se sme kaznovati oziroma zapreti po določbi drugega odstavka 220. člena ZKP, razen če gre za osumljenca, obdolženca ali

osebo, ki ne sme biti zaslišana kot priča ali se je v skladu s tem zakonom odrekla pričevanju (ZKP, 2021).

Lastnika mobilne in ostalih zaseženih naprav policija povabi, da je lahko pri postopku zavarovanja podatkov navzoč sam, njegov zastopnik, odvetnik ali strokovnjak. Če se stranka v postopku vabilu policije ne odzove ali če je odsoten ali če oseba ni znana, se zavarovanje podatkov in izdelava istovetne kopije opravi v njegovi nenavzočnosti. Zavarovanje podatkov opravi ustrezno usposobljena oseba. V kolikor je oseba prisotna pri zavarovanju podatkov »se v zapisnik zapiše tudi kontrolna vrednost, oziroma se na drug ustrezen način v zapisniku zagotovi možnost naknadnega preverjanja istovetnosti in integritete zavarovanih podatkov«. Izvod zapisnika se izroči osebi, ki je bila navzoča pri zavarovanju podatkov (ZKP, 2021).

Strokovni delavec policije, kateri izvaja zavarovanje podatkov iz mobilnih in ostalih elektronskih naprav, mora zaseg in zavarovanje podatkov opraviti na način, s katerim se v najmanjši možni meri posega v pravice oseb, ki niso osumljenci ali obdolženci in varuje tajnost oziroma zaupnost podatkov ter se ne povzroča nesorazmerna škoda zaradi nezmožnosti uporabe elektronske naprave (ZKP, 2021).

Po opravljenem postopku zavarovanja podatkov, ki so na mobilnih in ostalih elektronskih napravah, se medij, na katerega so posneti podatki, v obliki delovne kopije in originala preda preiskovalcu, kateri preiskuje kaznivo dejanje. Preiskovalec nato delovno kopijo zavarovanih podatkov pregleda in iz njih izlušči vse podatke, kateri bodo kasneje služili kot dokaz v predkazenskem postopku. Kopije zaseženih podatkov se hranijo, dokler je to potrebno za postopek. Elektronska naprava se hrani, dokler podatki niso shranjeni na način, ki zagotovi istovetnost in integriteto zaseženih podatkov, vendar ne več kakor tri mesece od dneva pridobitve. Če izdelava takšne kopije podatkov ni mogoča, se elektronska naprava ali del elektronske naprave, ki vsebuje iskane podatke, hrani, dokler je to potrebno za postopek, vendar ne več kakor šest mesecev od dneva pridobitve, razen če je bila zasežena elektronska naprava uporabljena za izvršitev

kaznivega dejanja oziroma je sama elektronska naprava dokaz v kazenskem postopku. Kopije podatkov, pridobljene v skladu z določbami 223.a člena ZKP, ki se ne nanašajo na kazenski pregon in za katere ni kakšnega drugega zakonskega razloga, da bi se smeli hraniti, se izločijo iz spisa, če je to mogoče in se zapisniško uničijo, o čemer se v osmih dneh obvestijo preiskovalni sodnik, državni tožilec in imetnik elektronske naprave (ZKP, 2021).

3.2 Zakonska podlaga za pridobitev podatkov o prometu v elektronskem komunikacijskem omrežju in lokacija

Vsak uporabnik mobilnih naprav, kateri ima v svoji mobilni napravi SIM kartico, lahko z operaterjem javnega omrežja sklene naročniško razmerje ali pa si pridobi predplačniško SIM kartico, katero vstavi v svojo mobilno napravo. S tem, ko oseba z operaterjem sklene naročniško ali predplačniško razmerje, se v tej točki pričnejo obdelovati osebni podatki. Operaterji, ki so nosilci javnih komunikacijskih storitev, »morajo sprejeti ustrezne tehnične in organizacijske ukrepe za zagotovitev zavarovanja svojih storitev«. Če je potrebno, za zagotovitev zavarovanja svojih storitev v delu, ki se nanaša na varnost omrežja, sprejmejo ustrezne tehnične in organizacijske ukrepe skupaj s ponudnikom javnega komunikacijskega omrežja. Ukrepi morajo ob upoštevanju tehnološkega razvoja in stroškov njihove izvedbe zagotoviti takšno raven varnosti in zavarovanja, ki ustreza predvidenemu tveganju. Tveganje predstavlja zlasti vsako dejanje, storitev ali izdelek, ki posega v tajnost, zaupnost in varnost elektronskega komunikacijskega omrežja ali elektronske komunikacijske storitve, s tem ko spremeni dostopnost, vsebino, ceno ali kakovost storitve, in ki ga lahko operater sam ali skupaj z drugimi operaterji učinkovito onemogoči. Ukrepi morajo vsaj zagotoviti, da ima dostop do osebnih podatkov le pooblaščeno osebje za z zakonom dovoljene namene, varovati shranjene ali poslane osebne podatke pred nenamernim ali nezakonitim uničenjem, nenamerno izgubo ali spremembo ter nepooblaščenim ali nezakonitim shranjevanjem, obdelavo, dostopom ali razkritjem in zagotavljati izvajanje varnostne politike pri obdelavi osebnih podatkov.

Nadzor nad izvajanjem delovanja operaterjev in komunikacijskih omrežij opravlja Agencija za komunikacijska omrežja Republike Slovenije (ZEKom-1, 2012).

Če policija želi storilcu, ki je izvršil kaznivo dejanje, ki se preganja po uradni dolžnosti in je pri sebi imel mobilni telefon ali pa je z njim izvršil kaznivo dejanje (komunikacija in ostale storitve), dokazati storjeno kaznivo dejanje, lahko na pristojno Okrožno državno tožilstvo poda predlog za izpis prometa elektronskih komunikacij in izpis lokacij. Izpis prometa je vezan na SIM kartico, izpis lokacij pa na mobilni telefon. V 149b. členu ZKP je določeno, da če so podani razlogi za sum, da je bilo storjeno, da se izvršuje ali da se pripravlja oziroma organizira kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti in je za odkritje tega kaznivega dejanja ali storilca potrebno pridobiti podatke o prometu v elektronskem komunikacijskem omrežju, lahko preiskovalni sodnik na obrazložen predlog državnega tožilca odredi operaterju, da pristojnemu organu sporoči podatke o udeležencih, okoliščinah in dejstvih elektronskega komunikacijskega prometa, kot so: številka ali druga oblika identifikacije uporabnikov elektronskih komunikacijskih storitev, vrsta, datum, čas in trajanje klica oziroma druge elektronske komunikacijske storitve, količina prenešenih podatkov in kraj, iz katerega je bila elektronska komunikacijska storitev opravljena. Predlog in odredba morata biti pisna in morata vsebovati podatke, ki omogočajo identifikacijo komunikacijskega sredstva za elektronski komunikacijski promet, utemeljitev razlogov, časovno obdobje, za katerega se podatki zahtevajo ter ostale pomembne okoliščine, ki narekujejo uporabo ukrepa. Če so podani razlogi za sum, da je bilo storjeno, oziroma da se pripravlja kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti in je za odkritje tega kaznivega dejanja ali storilca potrebno pridobiti podatke o lastniku ali uporabniku določenega komunikacijskega sredstva za elektronski komunikacijski promet, ki niso objavljeni v naročniških imenikih in o času, v katerem je tako sredstvo bilo oziroma je v uporabi, lahko policija od operaterja zahteva, da ji na njeno pisno zahtevo, tudi brez privolitve posameznika, na katerega se ti podatki nanašajo, sporoči te podatke. Operater svoji stranki ali tretji osebi ne sme razkriti, da je ali da bo določene podatke posredoval pristojnemu organu ali policiji (ZKP, 2021).

Policija lahko podatke o naročniku (osebne podatke, podatke o sklenitvi naročnine, nakupu naprave in ostale podatke) zahteva na podlagi zaprosila. Operater mora te podatke nato policiji tudi nuditi, vendar se lahko operater pri tem tudi odloči, da zahtevane podatke pošlje v presojo pristojnemu sodišču, katero preveri zakonitost zahtevanih podatkov. Operater se zavezuje, da naročniku ne bo izdal, da je podatke o naročniku posredoval policiji ali sodišču največ 24 mesecev, sodnik pristojnega sodišča pa to lahko podaljša še za 12 mesecev. V tem primeru operater ne sme posredovati podatkov o prometu ali lokaciji, saj to lahko stori le na podlagi pridobljene odredbe pristojnega sodišča (ZKP, 2021).

Policija ali pristojno Okrožno državno tožilstvo lahko od operaterja zahteva, da ohrani podatke o prometu in lokaciji njihovega naročnika do izdaje odredbe pristojnega sodišča, vendar ne dlje kot 30 dni od izročitve zahteve, kar se lahko podaljša še za dodatnih 30 dni. V takem primeru obstaja bojazen, da se bodo podatki, katere hrani operater izbrisali, saj lahko operater podatke hrani le določen čas (ZKP, 2012, čl. 149e). V drugem odstavku 149.e člena ZKP je določeno, da je ohranitev podatkov o prometu oziroma podatkov o vsebini komunikacij pri operaterju mogoče zahtevati le zaradi odkritja, preprečitve ali dokazovanja kaznivega dejanja iz četrtega odstavka 149.a člena ali iz drugega odstavka 150. člena ZKP oziroma zaradi odkritja storilca takšnega kaznivega dejanja (tajno opazovanje in sledenje komunikacij in ostalega) (ZKP, 2021).

4 TAKTIKA IN METODE PRISKOVANJA KAZNIVIH DEJANJ

Policija pri obravnavanju in preiskovanju kaznivih dejanj izvaja določena opravila oziroma ukrepe za raziskavo in dokazovanje kaznivega dejanja storilcu kaznivega dejanja. Ta opravila oziroma ukrepe mora policija izvajati v skladu z zakonom. Zaseg in preiskava mobilnega telefona spada med ta opravila, v nadaljevanju pa bomo opisali postopek odvzema in preiskave mobilnega telefona, pri čemer bomo opisali postopanje policije v primeru izvršitve uradno pregonljivega kaznivega dejanja in dokazovanje tega kaznivega dejanja na podlagi zaseženega mobilnega telefona osumljencu tega kaznivega dejanja.

4.1 Zaseg mobilnega telefona po izvršitvi kaznivega dejanja

Kot navedeno v empiričnem delu diplomskega dela, policija lahko osumljencu kaznivega dejanja, katerega je po izvršitvi kaznivega dejanja prijela in z njim izvedla postopek ali mu odvzela prostost in odredila pridržanje, na podlagi Zakona o kazenskem postopku zaseže mobilni telefon, če se smatra, da bodo mobilni telefon oziroma podatki na njem služili kot dokaz v predkazenskem in kasneje tudi v kazenskem postopku. Zaseg policija opravi na podlagi 220. člena ZKP in mobilni telefon zaseže z Zapisnikom o zasegu predmetov, en izvod Zapisnika pa izroči osebi, ki ji je bila naprava zasežena. Sam zasežen mobilni telefon, v katerem je vstavljena tudi SIM kartica izbranega operaterja, se pred osumljencem spravi v oblazinjeno kuverto in se zapečati, pečat pa morata podpisati osumljenec in policist, ki je pečatenje opravil. S tem se zavaruje osumljenca in njegov mobilni telefon, da osebe, ki nimajo upravičenega stika z mobilnim telefonom, z njim ne poskušajo upravljati. Policija nato osumljencu predoči pisno privolitev za preiskavo elektronske naprave, kjer se osumljenec opredeli o tem, ali soglaša s preiskavo naprave ali ne, ali bo pri preiskavi navzoč, ali bo pri preiskavi navzoč njegov odvetnik in ali bo pri preiskavi navzoča oseba, ki jo bo osumljenec pooblastil in je strokovnjak na področju računalništva. V kolikor se osumljenec strinja s preiskavo mobilnega telefona in SIM kartice, se naprava pošlje v preiskavo strokovnjakom na Oddelku za računalniško

preiskovanje Sektorja kriminalistične policije pristojne policijske uprave. V kolikor se osumljenec ne strinja s preiskavo mobilnega telefona, mora policija na pristojno Okrožno državno tožilstvo podati pobudo za preiskavo na podlagi 219.a člena ZKP. Pobuda za preiskavo elektronske naprave mora vsebovati podatke, ki omogočajo identifikacijo elektronske naprave, ki se bo preiskala, utemeljitev razlogov za preiskavo, opredelitev vsebine podatkov, ki se iščejo, druge pomembne okoliščine, ki narekujejo uporabo tega preiskovalnega dejanja in določajo način njegove izvršitve. V kolikor sodišče izda odredbo za preiskavo elektronske naprave, se izvod odredbe izroči imetniku te naprave oziroma osebi, ki ji je bila zasežena, nato pa se elektronska naprava oziroma v našem primeru mobilni telefon pošlje v preiskavo. Policist ali kriminalist, kateri vodi preiskavo kaznivega dejanja, zaseženega mobilnega telefona pred izdajo odredbe za preiskavo elektronske naprave ne pošilja na Oddelek za računalniško preiskovanje. Osumljenec, kateremu je bil zasežen mobilni telefon, je po izdani odredbi lahko sam navzoč pri preiskavi, ali njegov odvetnik ali oseba, ki jo pooblasti (ZKP, 2021).

V kolikor se mobilni telefon zaseže pri preiskavi stanovanja in drugih prostorov na podlagi izdane odredbe za to preiskavo s strani sodišča, se postopa na enak način kot je opisano pri zasegu na podlagi 220. člena ZKP s to razliko, da mora biti zaseg mobilnega telefona z vstavljeno SIM kartico, odrejen v odredbi za preiskavo stanovanja in drugih prostorov. V kolikor se osumljenec, kateremu je bil mobilni telefon zasežen pri preiskavi stanovanja in drugih prostorov, ne strinja z preiskavo mobilnega telefon s SIM kartico, mora policija na pristojno Okrožno državno tožilstvo ponovno podati pobudo za preiskavo elektronske naprave na podlagi 219.a člena ZKP, sodišče pa na predlog tožilca izda ali ne izda odredbe za preiskavo (ZKP, 2021).

4.2 Zavarovanje podatkov in forenzična preiskava podatkov na zaseženem mobilnem telefonu

Ko so izpolnjeni vsi pogoji, da lahko policija opravi zavarovanje podatkov, ki so na zaseženem mobilnem telefonu in SIM kartici, to opravilo kot navedeno opravijo

strokovno usposobljene osebe - kriminalisti, ki so zaposleni na Oddelku za računalniško preiskovanje, Sektorja kriminalistične policije, pristojne policijske uprave. Osumljenec, kateremu je bil zasežen mobilni telefon, je dolžan policiji posredovati vsa gesla in ključe za vstop v podatke mobilnega telefona in SIM kartice, da kriminalisti, ki zavarujejo podatke mobilnega telefona, lahko do tega dostopajo. Težava se pojavi, ko osumljenec teh gesel ne poda, saj so se z željo po tajnosti informacij začeli razvijati enkripcijski programi, ki posamezniku omogočajo zaščito njegovih podatkov – ti postanejo nedostopni in nedosegljivi nepooblaščenim osebam. S tega vidika je enkripcija podatkov družbi potrebna in dobrodošla. Temna plat enkripcije pa se pokaže v kazenskih oziroma predkazenskih postopkih, ko ta organom pregona prepreči dostop do digitalnih podatkov, do katerih so upravičeni na podlagi sodne odredbe ali privolitve za preiskavo mobilnega telefona. Z razvojem komuniciranja je človek začel razvijati tudi metode, kako komunikacijo zaščititi pred osebami, katerim vsebine niso bile namenjene. Digitalna enkripcija pa se lahko izkaže za izredno problematično pri preiskovanju kaznivih dejanj, ko storilec kaznivega dejanja zakodira digitalne dokaze z enkripcijsko metodo, zaradi česar so tako zavarovani digitalni dokazi neuporabni in nedosegljivi računalniškim forenzikom in preiskovalcem kaznivih dejanj. V zadnjem času se pojavljajo velike pravne dileme, kako pridobiti digitalne podatke iz informacijskih sistemov, ki so zaščiteni z enkripcijskim programom. Teh je na tržišču več vrst, nivo njihove zaščite pa je odvisen od enkripcijskega ključa, ki ga vsebujejo (Markelj, Bernik, 2013, stran 85, 86 in 87, ZKP, 2021).

4.2.1 Programska oprema za forenzično zavarovanje podatkov

Pri zavarovanju podatkov iz mobilne naprave oziroma pri mobilni forenziki obstaja ogromno opreme oziroma orodij, med katera uvrščamo samostojne programske rešitve, forenzične in ne forenzične. Te je mogoče namestiti na forenzične delovne postaje v okviru različnih operacijskih sistemov (Windows, Linux, Mac OS X), kot tudi celovite forenzične rešitve – vse v enem, ki jih sestavlja programska ter pripadajoča strojna oprema in tudi nekatere strogo namenske strojne naprave. Programska oprema za digitalno-forenzične postopke mobilnih naprav je lahko plačljiva oziroma brezplačna in

je lahko tudi brez kod. Med programsko opremo se štejejo tudi ne forenzična programska orodja, med katera se uvrščajo orodja, ki niso bila posebej razvita za izvajanje forenzičnih preiskav. Tu gre za različna orodja proizvajalcev naprav ali proizvajalcev mobilnih operacijskih sistemov, ki so namenjena upravljanju z napravo v smislu sinhronizacije podatkov z računalnikom, testiranju in diagnostiki, kot tudi razvoju aplikacij za mobilne naprave. Bistvena značilnost forenzične opreme je, da na forenzično sprejemljiv način prekopira podatke iz predmetne naprave in pri tem za zavarovane podatke samodejno izračuna zgoščeno vrednost, ki zagotavlja integriteto teh podatkov (Ayers, Brothers & Jansen, 2014). Pri postopku ustvari tudi dnevniško datoteko, iz katere so razvidne vse tehnične lastnosti in podrobnosti postopka. Na drugi strani ne forenzična oprema opisanega ne zagotavlja, zato morajo preiskovalci v primeru uporabe takšne opreme v skladu s forenzičnimi načeli zagotoviti, da so upoštevane vse bistvene prvine. Preiskovalci lahko pri izvajanju postopkov v okviru mobilne forenzike uporabijo tudi takšno orodje, če z njegovo uporabo dosežejo namen preiskave in tega drugače niso mogli izvesti (Sotošek, 2016, stran 11).

Kot pravi Sotošek v svojem diplomskem delu, »forenzična samostojna programska oprema kot tudi forenzične celovite rešitve omogočajo izvajanje vseh procesov, od pridobitve oziroma zavarovanja podatkov do njihove analize in izdelave ustreznih elektronskih poročil v okviru procesa preiskave elektronske naprave«. S takšno opremo se izvajajo postopki na t. i. ne invaziven način, kar pomeni, da mobilne naprave pri postopku ni treba razstavljati ali v njo kakor koli v fizičnem smislu posegati. Kot forenzična strojna oprema so mišljeni različni priključki, kabli, vmesniki in drugi dodatki ter same naprave, kot so npr. namizni računalniki z zasloni, prenosniki in druge prenosne naprave v obliki večjih dlančnikov z zasloni na dotik, ki so namenjene predvsem uporabi na terenu. Poleg navedenega obstajajo še strogo namenske strojne naprave za pridobivanje podatkov na t. i. invazivni način, kjer je treba fizično poseči v napravo, tako da se jo popolnoma razstavi ali celo odstrani podatkovni nosilec (čip). Gre za metode Chip-off, JTAG in Micro Read, ki jih podrobneje opišemo v naslednjem poglavju« (Sotošek, 2016, stran 11 in 12).

Kot v nadaljevanju opisuje Sotošek »Slovenski policiji in njihovim preiskovalcem so na voljo le komercialna forenzična orodja, in sicer Cellebrite UFED in MSAB Xry, ki vključujeta tudi pripadajoči komplet z različnimi priključki, kabli, adapterji ter čitalniki spominskih in SIM-kartic. Preiskovalci imajo na voljo še samostojni forenzični programski opremi Oxygen Forensics in Lantern Katana Forensics, ki pa nista na takšnem nivoju kot prej navedeni, v smislu števila naprav, ki so podprte s strani števila različnih forenzičnih profilov ali načinov pridobivanja podatkov, ki jih je moč uporabiti. Forenzična oprema, ki jo uporabljajo v policiji slovenski preiskovalci, je vezana na časovno veljavne licence, katerih redno posodabljanje omogoča podporo novih modelov mobilnih naprav, nove priključke za povezavo ter nove načine za komunikacijo med mobilno napravo in delovno postajo, predvsem pa so najpomembnejši novi načini oziroma metode in tehnike pridobivanja podatkov iz naprav. V zvezi tega je potrebno upoštevati, da se preiskovalci v slovenski policiji soočajo s težavami, ki so povezane s podprtostjo mobilnih naprav s strani forenzične opreme, saj zaradi pomanjkanja financ v policiji ne omogočajo rednega posodabljanja opreme, povezane pa so tudi s sistemom dodatnih izobraževanj, kar je v trenutni situaciji zelo pomembno z vidika uporabe različnih pristopov oziroma alternativnih metod in tehnik pridobivanja podatkov, ki bi lahko omogočile doseganje namena forenzične preiskave« (Sotošek, 2016, stran 12).

4.2.2 Način zavarovanja podatkov iz mobilnih naprav

Sotošek v svojem diplomskem delu pravi, da »način pridobivanja podatkov, ki ga preiskovalec izbere, je vsekakor odvisen od vrste podatkov, ki se iščejo. Ti pa so odvisni od narave primera oziroma storitve kaznivega dejanja, zaradi katerega je bila v (pred)kazenskem postopku naprava zasežena in jo je treba preiskati. Prav tako na izbiro načina vpliva tudi mobilna naprava sama, v smislu podprtosti v okviru forenzične opreme ter tudi ostale okoliščine, kot so npr. posedovanje potrebnih šifrirnih ključev oziroma gesel; čas, ki je preiskovalcem na voljo – v primeru priporne zadeve, kadar je osumljencu odrejen pripor in je nadaljnji postopek odvisen od izsledkov preiskave, itn. Preiskovalci

praviloma začnejo postopek z načini, ki čim manj posegajo tako v napravo kot tudi v spreminjanje podatkov na napravi. Najpomembneje pa je, da preiskovalec izbere način, s katerim bo učinkovito in uspešno pridobil podatke« (Sotošek, 2016, stran 12).

Obstajajo trije načini pridobivanja podatkov iz mobilnih naprav in sicer ročni, logični in fizični način (Barmpatsalou, Damopoulos, Kambourakis & Katos, 2013, str. 5).

- **ROČNI NAČIN,** kjer z uporabo tipkovnice, drugih tipk ali prek zaslona na dotik, upravlja z menijem naprave. Pri tem preiskovalec pregleduje podatke, ki so vidni na zaslonu mobilne naprave. Podatke zavaruje s slikanjem ali snemanjem s kamero ali tudi s programom, ki omogoča video zajem zaslona na delovni postaji (npr. liteCam Android). Tak način preiskovalec izbere, ko mobilna naprava ni podprta s strani forenzične opreme oziroma je podprta le delno. Tak način se uporablja tudi, če obstaja prevelika nevarnost za izgubo podatkov ali poškodovanje naprave. Slaba lastnost ročnega načina pridobivanja podatkov je v količini podatkov na napravi, zaradi česar bi preiskovalec izgubil ogromno časa za njihovo pridobivanje in zavarovanje, prav tako pa je tu tudi človeški faktor, kjer lahko prihaja do napak, kot so nenamerno brisanje ali spreminjanje podatkov (Ayers, Brothers & Jansen, 2014, str. 17).
- **LOGIČNI NAČIN** pridobivanja podatkov, kjer preiskovalci pridobijo aktivne podatke, ki se nahajajo na podatkovnem nosilcu mobilne naprave in so kot taki vidni in dostopni uporabniku naprave. Tu gre za dodeljene podatke, ki niso izbrisani, do njih pa se dostopa na nivoju datotečnega sistema (Hoog, 2011). Posebnost pri tem načinu je, da lahko baze vsebujejo tudi nekatere zapise oziroma podatke, ki jih je uporabnik zbrisal, na nivoju datotečnega sistema pa to pomeni, da je mesto v bazi, kjer se takšen zapis oziroma podatek nahaja, le označeno kot prosto za prepis z novimi podatki. Z uporabo logičnega načina se lahko pridobijo tudi nekateri podatki, ki jih je uporabnik izbrisal (Hoog, 2011). Osnovni in bistveni pogoj, ki mora biti izpolnjen, da lahko preiskovalec uporabi logični način pridobivanja podatkov, je vzpostavitev komunikacije med napravo

in forenzično delovno postajo oziroma forenzičnim orodjem. Uporaba tega načina pridobivanja podatkov je podprt pri veliki večini mobilnih naprav in je najbolj razširjena v okviru komercialne forenzične opreme. Prednost tega načina je, da izvedba postopka ni zahtevna in ne zahteva dodatnih izobraževanj. Ta način zavarovanja podatkov je za preiskovalce v večini primerov zadosten, saj z njim zavarujejo željene podatke in ni več potrebe po dodatnih načinih zavarovanja (Sotošek, 2016, stran 15).

- **FIZIČNI NAČIN**, pri katerem ni potrebno poseči v mobilno napravo s postopki razstavljanja naprave in odstranjevanja modulov (SWGDE, 2013). Programske metode fizičnega pridobivanja podatkov vključujejo uporabo različnih tehnik, med najpogostejše pa spada uporaba prirejenih zagonskih nalagalnikov ali drugih prirejenih programskih kod, ki se v večini primerov začasno naložijo v delovni pomnilnik – RAM, nekatere pa je treba polno namestiti na podatkovni nosilec mobilne naprave (Ayers, Brothers & Jansen, 2014). Nekatere tehnike za pridobitev podatkov potrebujejo vklopljeno napravo, nekatere pa postopek pridobivanja podatkov izvajajo v fazi, ko je naprava sicer vklopljena, vendar se operacijski sistem še ni naložil. Slednje je z vidika forenzične sprejemljivosti zaželeno, saj se pri tem ne spreminja originalnih podatkov. Slovenski preiskovalci za fizični način pridobivanja podatkov uporabljajo le komercialno forenzično opremo, ki avtomatizirano ustvarja nekatere potrebne pogoje in okoliščine ter preiskovalca pravilno vodi skozi postopek s pomočjo navodil, ki se med postopkom izpisujejo na zaslonu komercialne forenzične opreme (Sotošek, 2016, stran 15 in 16).

Težava pri dostopu do pomnilnika mobilnega telefona pri mobilni forenziki predstavlja informacijska varnost in je danes dostopnost do pomnilnika za razliko od računalnikov oziroma trdih diskov, skoraj nemogoča. Sodobni mobilni telefoni imajo podatke šifrirane, zato komercialna orodja za mobilno forenziko iščejo neko šibkost v strojni in programski opremi, da se omogoči dostop do pomnilnika mobilnega telefona. Proizvajalci mobilnih telefonov to šibkost v šifriranju strojne in programske opreme

redno posodabljajo in hitro proizvajajo nove mobilne telefone, ki imajo novo strojno opremo, do katere je potrebno najti ranljivost (Petek, 2022, starn 29). Iz tega izhaja, da se v največ primerih opravlja logično zavarovanje podatkov iz pomnilnika mobilnega telefona. Zaradi napake pri izbiri pravilnega orodja za zavarovanje podatkov iz mobilnega telefona lahko privede do nepopolnega in neustreznega zavarovanja podatkov in s tem zmanjša integriteto podatkov, kar lahko privede do kompromitacije digitalnih dokazov (Saleem idr., 2016).

Drugo težavo pri analizi in zavarovanju podatkov iz mobilnih telefonov predstavlja način, kako so podatki shranjeni. Namreč aplikacije za komunikacijo podatke shranjujejo v baze, medtem ko so slike, posnetki in ostali dokumenti shranjeni v klasičnih datotekah (Lin idr., 2018). Najrazsežnejša baza podatkov za shranjevanje podatkov je SQLite, pri čemer je potrebna preiskava vsake baze posebej, saj so baze tako zasnovane s strani proizvajalca. Komercialna forenzična orodja sicer omogočajo analizo teh podatkov, ki pripadajo različnim aplikacijam, vendar lahko tukaj pride do nezanesljivosti teh orodij kot tudi preverjanja dokazov, kar je ena od osnovnih načel digitalne forenzike, da so lahko pridobljeni digitalni dokazi sprejemljivi na sodišču in lahko služijo kot dokaz (Nemetz idr., 2018).

4.3 Preiskava elektronske komunikacije in baznih postaj

Ko policija oziroma preiskovalci zasežejo mobilni telefon s SIM kartico, lahko na podlagi 149b. člena ZKP na pristojno Okrožno državno tožilstvo podajo pobudo, da preiskovalni sodnik izda odredbo za preiskavo podatkov za mobilno telefonsko številko, ki je v obliki SIM kartice vstavljena v mobilni telefon. Ko preiskovalni sodnik izda odredbo za preiskavo podatkov mobilne številke, katero je uporabljal osumljenec, je operater dolžan posredovati vse podatke, ki so povezani s telefonsko številko osumljenca in IMEI številko mobilnih naprav, v katere je bila SIM kartica oziroma telefonska številka vstavljena. Operater, kot smo navedli v empiričnem delu, hrani navedene podatke samo določen čas. V kolikor so preiskovalci oziroma sodnik, ki je izdal odredbo, presegli rok, ki

dovoljuje hrambo podatkov operaterju, se lahko zgodi, da podatkov, ki so lahko ključni dokaz v predkazenskem in kasneje tudi v kazenskem postopku, operater ne sme posredovati. V kolikor se podatki od operaterja zahtevajo v roku, ki operaterju dovoljuje posredovanje podatkov, ta na podlagi prepisa odredbe preiskovalnega sodnika pristojnega Okrožnega sodišča policiji posreduje izpis podatkov od operaterja. Operater policiji posreduje izpis podatkov, na katerem so razvidni podatki, kot so ura in datum komunikacije, podatki o telefonskih številkah in naročnikih, s katerimi je osumljenec komuniciral in IMEI številke mobilnih telefonov, v katere je bila vstavljena SIM kartica (Ipavec, 2016).

Ko policija oziroma preiskovalec, ki vodi preiskavo zoper osumljenca, ki mu je bil zasežen mobilni telefon s SIM kartico, prejme izpis podatkov operaterja na podlagi odredbe sodišča, se opravi preiskava in analiza. Kot navedeno, se iz podatkov, ki se nanašajo na SIM kartico, ki je vstavljena v mobilni telefon, vidijo podatki kot so ura in datum komunikacije, podatki o telefonskih številkah in naročnikih, s katerimi je osumljenec komuniciral in IMEI številke mobilnih telefonov, v katere je bila vstavljena SIM kartica. Na podlagi teh podatkov se lahko dokazuje izvršitev očitanega kaznivega dejanja. Predvsem se lahko na podlagi IMEI številke dokazuje približna lokacija, kje se je osumljenec v času kaznivega dejanja nahajal. V kolikor ima osumljenec na svojem mobilnem telefonu vključeno lokacijo ali mobilne podatke, se naprava poveže z bazno postajo (Ipavec, 2016).

Načelo sorazmernosti pomeni, da mora omejitev ustavnih pravic oziroma poseg vanje izpolnjevati tri pogoje, in sicer: poseg mora biti nujen, poseg mora biti primeren (in s tem učinkovit) za dosego zaželenega, ustavno dopustnega cilja in upoštevati je treba tudi t. i. sorazmernost v ožjem smislu, ki je v tem, da je pri ocenjevanju nujnosti posega treba tehtati tudi pomembnost s posegom prizadete pravice v primerjavi s pravico, ki se s tem posegom želi zavarovati in odmeriti nujnost posega sorazmerno s težo prizadetih posledic. Namreč informacijski pooblaščenec ugotavlja, da je običajno k uvajanju novih pooblastil vodila dostopnost neke določene nove tehnologije na trgu (npr. brezpilotni

letalniki, IMSI lovilci) oziroma zmanjšanje učinkovitosti organov pregona zaradi uporabe novih tehnologij na strani osumljencev oz. preiskovancev (npr. večja uporaba šifriranih komunikacij s strani storilcev kaznivih dejanj, uporaba predplačniških SIM kartic ipd.). Temu je običajno sledila takojšnja priprava pravnih podlag, ki naj bi z novimi pooblastili policiji nevtralizirale navidezno prednost potencialnih storilcev kaznivih dejanj pri rabi informacijskih tehnologij. Predhodne analize nujnosti, primernosti in učinkovitosti ter sorazmernosti takih pooblastil praviloma niso bile izvedene, naknadne analize pa ne predvidene. Obrazložitve so bile skope, pogosto oprte na neprepričljive argumente in včasih celo zavajajoče (Informacijski pooblaščenec, 2014, stran 6 in 7).

Dejstvo pa je, da so podatki o prometu in lokaciji storilcev kaznivih dejanj, kateri izvršijo hujša kazniva dejanja ali kazniva dejanja s področja organizirane kriminalitete, nujno potrebni za dokazovanje izvršitve kaznivega dejanja. Ker se pri izvršitvi tovrstnih kaznivih dejanj uporabljajo mobilni telefoni, so ti podatki zelo pomembni, zlasti pri analizi podatkov o prometu v predkazenskem postopku je mogoče ugotoviti območje, na katerem je bil mobilni telefon uporabljen, s kom je uporabnik telefoniral. S temi podatki pa lahko pridobimo okviren čas kaznivega dejanja in lokacijo, kjer se je storilec nahajal. Navedeni dokazi so nepogrešljivi v predkazenskem postopku in kasneje tudi v kazenskem postopku za dokazovanje izvršenega kaznivega dejanja (Ipavec, 2016, stran 36).

Zanimiv je podatek, da je Slovenska policija v letu 2022 pridobila 381 podatkov o prometu v elektronskem komunikacijskem omrežju, kar je za 1 podatek manj kot leta 2021 in kar za 102 podatka manj kot v letu 2020 in predhodnih letih, kjer se število pridobljenih podatkov o prometu v elektronskem komunikacijskem omrežju giblje okrog 500. Število oseb, zoper katere je bila odrejena pridobitev podatkov o prometu v elektronskem omrežju, znaša 120, kar je za 17 oseb manj kot leta 2021 in kar 86 oseb manj kot leta 2020 (Policija, 2023).

5 ANALIZA JAVNO DOSTOPNIH PRIMEROV

Analizirali bomo dva javno dostopna primera, kjer je mobilni telefon tako v predkazenskem postopku in v sodnem postopku služil kot eden od ključnih dokazov. Prva analiza primera bo osredotočena na zavarovanje in pregled podatkov na mobilnem telefonu, kateri je opravljen na podlagi 219a. člena ZKP. Druga analiza primera bo osredotočena na izvedbo ukrepa pridobitve podatkov o prometu v elektronskem komunikacijskem omrežju in lokacija na podlagi 149b. člena ZKP. Oba primera sta iz javno dostopne sodne prakse.

5.1 Primer zavarovanja in pregleda podatkov na mobilnem telefonu

Primer izhaja iz javno dostopne sodbe Višjega sodišča v Mariboru, sodba številka VSM Sodba III Kp 1101/2020, z 2. 9. 2020. V tem primeru je storilec izvršil kaznivo dejanje poskus prepovedanega prehajanja meje ali ozemlja države po tretjem odstavku 308. člena Kazenskega zakonika (KZ-1) v zvezi z drugim odstavkom 20. člena, kar pomeni, da je dejanje izvršil v sostorilstvu in ponarejanja listin po tretjem odstavku 251. člena KZ-1. Primer je osredotočen na enega storilca, sam postopek in podatki drugih storilcev niso znani. Eden od storilcev, na katerega se primer nanaša, je bil za izvršeni kaznivi dejanji obsojen na enotno kazen enega leta zapora in na 300,00 EUR denarne kazni. Storilec se je na sodbo pritožil na Višje sodišče v Mariboru, in sicer se ni strinjal z varnostnim ukrepom sodišča, odvzem predmetov oziroma odvzema dveh mobilnih telefonov, kateri so mu bili odvzeti. Vsaj en mobilni telefon storilec s to pritožbo želi prejeti nazaj.

Kot je možno razbrati iz javno dostopne sodbe, so storilci tuji državljani in so bili prijeti pri izvršitvi kaznivega dejanja. Iz tega je možno sklepati, da so policisti storilcu ob prijetju, na katerega se nanaša ta javno dostopna sodba, odvzeli prostost in odredili pridržanje na podlagi II. odstavka 157. člena ZKP, saj je izvršil kaznivo dejanje, ki se preganja po uradni dolžnosti. Zagrožena kazen, vsaj za sprovajanje, pa je od treh do desetih let zapora in denarna kazen. V tem primeru so nedvomno obstajali pridržalni razlogi, med katerimi je za izpostaviti zbiranje dokaznih predmetov, med katere spada tudi mobilni

telefon. Pri tem so obstajali tudi priporni razlogi za odvzem prostosti in sicer je bil storilec tujec, zato so okoliščine kazale na to, da bo oseba pobegnila in se ognila sojenju na območju Slovenije. Prav tako je obstajala bojazen, da bo storilec uničil dokaze, kot so podatki na mobilnih telefonih ali celo same mobilne telefone, s katerimi se bo kaznivo dejanje lahko dokazalo. Pridržanje, katero odredi policija ob zgoraj navedenih pogojih, lahko traja največ 48 ur, v tem času pa policija izvede vse pridržalne ukrepe. V roku 48 ur mora policija, kot navedeno zbrati vsa obvestila ter dokaze in storilca s kazensko ovadbo privesti k preiskovalnemu sodniku pristojnega sodišča. V kolikor policija to ne stori, mora storilca izpustiti. V tem primeru so policisti storilca privedli k preiskovalnemu sodniku, kateri je odredil pripor.

Iz sodbe ni točno razvidno kako so policisti mobilna telefona storilcu odvzeli, vendar obstajata le dve opciji, prva je zaseg predmeta na podlagi 220. člena ZKP, ko se predmeti zasežejo neposredno storilcu na kraju ali med postopkom in on te predmete izroči ali na podlagi 214. člena ZKP, ko pristojno sodišče na upravičeno obrazložitev tožilstva izda odredbo za preiskavo stanovanja in drugih prostorov, med katere spada tudi preiskava vozil.

Policisti so nato od storilca morali pridobiti pisno privolitev za zavarovanje in preiskavo elektronske naprave na podlagi 219.a. člena ZKP, v kolikor storilec pisne prijave ni podal, so morali policisti pridobiti odredbo s strani pristojnega sodišča. Na podlagi vsega navedenega je bilo nato tudi s strani strokovnega delavca policije opravljeno zavarovanje in preiskava podatkov na zaseženih mobilnih telefonih po metodah, katere so opisane v četrtem poglavju. O samem zavarovanju in preiskavi je bil sestavljen zapisnik, sami podatki pa so bili posneti na zaključen medij, kot je DVD alu Blu-Ray, tako da v ta zaključen medij več nihče ne more posegati. Iz sodbe je razvidno, da je storilec, s pomočjo zaseženih mobilnih telefonov pred izvršitvijo kaznivega dejanja in tudi na dan izvršitve, imel komunikacijo preko aplikacije Whats Up. Vsebino komunikacije iz zaseženih mobilnih telefonov pa so preiskovalci uporabili kot dokaz v predkazenskem postopku in je kot ključen dokaz, kot je razvidno iz sodbe, služil tudi v kazenskem

postopku in izreku sodbe. Sodišče je nato v izreku sankcije zaporne kazni izreklo tudi varnostni ukrep odvzema obeh zaseženih mobilnih telefonov, saj sta bila telefona uporabljena kot sredstvo pri izvršitvi kaznivega dejanja, ker je storilec preko teh telefonov komuniciral z ostalimi osebami in se je na ta način lahko pripravil na izvršitev kaznivega dejanja. Višje sodišče je zavrnilo pritožbo storilca, da bi se mu zasežena mobilna telefona vrnila, saj sta služila kot predmet za izvršitev kaznivega dejanja.

V tem primeru je mobilni telefon oziroma podatki na njem služil kot dokaz tako v predkazenskem kot tudi v kazenskem postopku. Tako policija kot tudi pravosodni organi so v tem primeru od začetka postopka do konca postopali po ZKP, pri tem pa je bilo ključnega pomena dokazati izvršeno kaznivo dejanje storilcu, kar je na koncu tudi odlično uspelo, saj je bil storilec pravnomočno obsojen. Sodelovanje med navedenimi organi in zbiranje ključnih dokazov pa je vedno ključnega pomena.

5.2 Primer pridobitve podatkov o prometu v elektronskem komunikacijskem omrežju in lokacija

Ta primer izhaja iz javno dostopne sodbe Vrhovnega sodišča Republike Slovenije, sodba številka VSRS Sodba I Ips 56957/2018, z 29. 4. 2021. Okrožno sodišče v Celju je obsojenega s sodbo III K 56957/2018 dne 11. 11. 2019 spoznalo krivega štirih kaznivih dejanj ropa po prvem in drugem odstavku 206. člena KZ-1. Za vsako dejanje mu je določilo kazen 5 let zapora in izreklo enotno kazen 17 let in 6 mesecev zapora; v izrečeno kazen je vštelo čas pripora. Obsojenec pa je v tem primeru dolžan plačati stroške, ki jih je povzročil po svoji krivdi in izdatke oškodovancev ter izdatke in nagrado njihovih pooblaščencev. S sodbo je sodišče izreklo tudi varnostni ukrep odvzema predmetov, odločilo o premoženjskopravnem zahtevku in obsojencu odvzelo premoženjskopravno korist. Obsojenec se je po pooblaščencu pritožil na drugostopenjsko Višje sodišče v Celju, katero pa je pritožbo zavrnilo kot neutemeljeno in potrdilo sodbo sodišča prve stopnje. Obsojenec se je nato pritožil še na Vrhovno sodišče, katero je njegovo pritožbo v celoti zavrnilo. Glavni pritožbeni razlog pa je izdana odredba preiskovalne sodnice Okrožnega

sodišča v Celju, številka I Kpd 56240/2017 z dne 13. 12. 2017, katera je izdala odredbo za izvedbo ukrepa po 149.b členu ZKP, s pomočjo katerega se je dokazovala komunikacijska povezava obsojenca in je na podlagi tega dokaza prvostopenjsko sodišče oprlo svojo sodbo.

Obsojenec je v njegovi pritožbi zatrjeval, da je odredba le prepis pisnega predloga tožilca, da odredba ne vsebuje sodne kontrole dokazov, ki jih je ponudilo tožilstvo, da odredba ni konkretizirana in določna do te mere, da bi se lahko preizkusila sodnikova lastna presoja o pogojih za poseg v pravico do zasebnosti, da odredba ni obrazložena glede zahtevanega dokaznega standarda (razlogov za sum), da v odredbi ni konkretiziranih razlogov, da bi bila telefonska številka sostorilca v uporabi, da v odredbi ni 4/8 konkretiziranih razlogov oziroma manjka obrazložitev razlogov o obstoju utemeljenega razloga za sum, da je bila ta telefonska številka uporabljena pri storitvi kaznivega dejanja na škodo oškodovancev in da v odredbi ni obrazloženih razlogov za sum, da bi obsojeni storil očitano dejanje.

V tem primeru je policija na Okrožno državno tožilstvo v Celju podalo pobudo za izdajo odredbe, za izvedbo ukrepa po 149.b členu ZKP, čemur je tožilstvo sledilo in je na okrožno sodišče v Celju podalo predlog za izdajo te odredbe. Preiskovalna sodnica v Celju je izdala odredbo za izvedbo tega ukrepa. Obsojenec je nato v pritožbi na Vrhovno sodišče preiskovalni sodnici, katera je izdala odredbo, očital, da je vsebinsko presojo namesto preiskovalne sodnice opravil predlagatelj, državni tožilec. Preiskovalna sodnica mora in je v tem primeru tudi morala opraviti samostojno presojo predpostavk ukrepa po takrat veljavnem prvem in drugem odstavku 149.b člena ZKP. Vendar pa iz načina ubeseditve odredbe ni mogoče sklepati, da je preiskovalna sodnica takšno samostojno presojo opustila. Iz odredbe izhaja sodničina lastna presoja pravne podlage za odreditev ukrepa, določno zatrjevanje podlage za presojo predpostavk ukrepa, lastna ocena razlogov za sum udeležbe pri izvršitvi kaznivega dejanja ropa po prvem in drugem odstavku 206. člena ZKP ter lastna presoja primernosti in (vsebinske ter časovne) nujnosti oziroma omejenosti ukrepa.

Nato obsojenec zatrjuje, da v odredbi ni obrazložen dokazni standard "razlogov za sum", ki ga je tudi po ureditvi, veljavni na dan izdaje odredbe, zahtevala ureditev po prvem in drugem odstavku 149.b člena ZKP. Prvi odstavek 149.b. člena ZKP je kot stopnjo verjetnosti izvršitve kaznivega dejanja določal, da morajo biti podani »razlogi za sum, da je bilo storjeno, da se izvršuje ali da se pripravlja oziroma organizira kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti«. Vsebino dokaznega standarda je treba razumeti v povezavi z namenom ukrepa, med katerim je tudi odkritje storilca. Zato po zakonski ureditvi zadošča, da je na ravni razlogov za sum izkazana le izvršitev kaznivega dejanja (ne pa tudi že individualiziran domnevni storilec dejanja). Na podlagi gradiva, ki je bilo preiskovalni sodnici predloženo, so bile okoliščine kaznivega dejanja ropa v odredbi jasno navedene in tudi preverljive. Obrazložitev odredbe glede zahtevanega dokaznega standarda je zato v celoti zadostovalo zakonskim merilom. Preiskovalna sodnica je nato v odredbi sprejela določnejše stališče in sicer, da so podani razlogi za sum, da je obsojenčev brat udeležen v dejanju na škodo oškodovancev. Ta korak je bil sestavni del individualizacije komunikacijskih sredstev, to je telefonov z navedenimi IMEI številkami in naročniških kartic, ki so se v teh telefonih uporabljali. ZKP, še posebej v luči ustavnih zahtev po obrazložitvi sodne odločbe zahteva, da sodišče svojo presojo tudi v tem delu obrazloži tako, da jo je mogoče vsaj preveriti, kot je primer sodbe Vrhovnega sodišča RS I Ips 24015/2010-1055 z dne 11. 9. 2014, smiselno tudi Ustavno sodišče RS v odločbi Up-709/15-29, Up-710/15-34 z dne 9. 10. 2019 v 50. točki obrazložitve. Sodišče se je torej v tem primeru izdaje odredbe moralo opreti na izrazljiva in preverljiva dejstva, ki razumnega človeka prepričajo v udeležbo imenovanega osumljenca in s tem posledično v primernost odreditve ukrepa v zvezi z določenimi komunikacijskimi sredstvi.

V odredbi za izvedbo ukrepa po 149.b členu ZKP so bili pri tej presoji ključni naslednji koraki: storilci so dobro poznali osebne okoliščine oškodovancev in okolico kraja dejanja, v krog oseb s tem znanjem ne sodijo stranke ali poslovni partnerji oškodovanca, z relevantnimi podatki je zunaj družinskega ali poslovnega kroga razpolagal brat

obsojenca in pritožnika. To je dejanska podlaga, na kateri temelji sklep, da so podani razlogi za sum udeležbe obsojenčevega brata pri kaznivem dejanju. Takšna dejanska podlaga je nedvomno preverljiva in na ravni razlogov za sum tudi ni nerazumna. Več pa zakonodajalec z uzakonitvijo tega dokaznega standarda ne zahteva.

Obsojencu je sporno tudi osredotočenje na določena komunikacijska sredstva. ZKP je zahteval, da odredba vsebuje »podatke, ki omogočajo identifikacijo komunikacijskega sredstva za elektronski komunikacijski promet«. Ukrep bo primeren le, če bo ugotovljena izrazljiva, preverljiva dejanska povezava med dejanjem (in v tem primeru tudi osumljencem) ter komunikacijskim sredstvom. Tudi to presojo je preiskovalna sodnica v izdaji odredbe za izvedbo ukrepa ustrezno opravila, in sicer v treh korakih: ugotovila je, da obsojenčev brat uporablja določeno telefonsko številko, da s to telefonsko številko (SIM kartico) uporablja več mobilnih telefonov, in da se v teh telefonih uporablja več telefonskih številk (SIM kartic). Ob takšnih korakih je povsem razumno sklepanje, da obsojenčev brat uporablja ne le enega, ampak več mobilnih telefonov in ne le eno, ampak več SIM kartic. Tudi ta sklep je razumen, preverljiv in nikakor ne arbitraren. S tem je v odredbi tudi (skladno s takratno zakonsko ureditvijo) vzpostavljena povezava med kaznivim dejanjem, osumljencem in uporabljenimi komunikacijskimi sredstvi. Obsojenec je v tem primeru napačno pričakoval, da besedilo takrat veljavnega 149.b člena ZKP zahteva obstoj "utemeljenih razlogov za sum", da je bilo določeno komunikacijsko sredstvo uporabljeno za točno določeno kaznivo dejanje. Izhaja iz razumne predpostavke, da storilci pri izvršitvi kaznivega dejanja uporabljajo svoja komunikacijska sredstva. S tem, ko je v odredbi vzpostavljena razumna in preverljiva povezava med osumljencem in individualiziranimi komunikacijskimi sredstvi, je zadoščeno tako zahtevi po primernosti odrejenega ukrepa kot vsebini sodne kontrole ukrepa.

Obsojenec je še zatrjeval, da v odredbi za izvedbo ukrepa po 149.b členu ZKP ni obrazloženih razlogov za sum, da bi obsojeni storil očitano dejanje. Za presojo zakonitosti odredbe v tem primeru ni pomembno, da so šele s pomočjo analize zbranih

podatkov identificirali obsojenega kot osumljenca, kot je to obrazloženo v sodbi sodišča prve stopnje. Pomembno je, da je bila telefonska številka, na kateri takšna analiza temelji, pridobljena s predhodnim, zakonitim in preverljivim obdelovanjem zbranih osebnih podatkov brata obsojenca, temu pa obsojenec niti ne nasprotuje.

Vrhovno sodišče je pritožbo obsojenca v vseh točkah in v celoti zavrnilo, kot je pa iz te sodbe moč razbrati, je bila izdaja odredbe za izvedbo ukrepa po 149b. členu ZKP ključna, da so lahko tako preiskovalci kot kasneje tožilstvo v sodnem postopku obsojencu dokazali izvršena kazniva dejanja. Da je policija sploh lahko podala pobudo na tožilstvo za izvedbo navedenega ukrepa, je predhodno morala zbrati dokaze, da je obstajal dokazni standard razlog za sum, da se izvršuje ali da se pripravlja oziroma organizira kaznivo dejanje, kar se v tem primeru nedvomno je. Iz primera je razvidno, da je telefon predstavljal ključen dokaz, s katerim so storilci pripravljali in organizirali izvršitev kaznivih dejanj. Na ta dokaz je tudi oprta sodba sodišča prve in druge stopnje ter Vrhovnega sodišča Republike Slovenije.

Kot v prvem primeru, je bilo ključno zbiranje dokazov s strani preiskovalcev, kateri so to odlično opravili, saj so pridobili odredbo za elektronski komunikacijski promet, za SIM kartico in mobilni telefon, katerega je uporabljal obsojenec. Brez tega ključnega dokaza ne bi bilo mogoče pridobiti ostalih dokazov zoper obsojenca in ostale sostorilce. Sodelovanje med policijo in pravosodnimi organi ter zbiranje ključnih dokazov pa je bilo kot v prvem primeru ključnega pomena.

6 ZAKLJUČEK

Mobilni telefoni oziroma bolj v zadnjem času pametni telefoni, so dandanes nepogrešljiva sredstva, ki jih človek uporablja pri vsakdanjih opravilih. Na teh telefonih, ki služijo kot mini računalniki, se shranjuje veliko podatkov, ki so osebne narave, da bi pa ti podatki bili zlorabljeni, pa si nihče ne želi, saj to lahko ima hude posledice za uporabnika mobilnega telefona. Pomembno varovalo, da ne more prihajati do zlorab podatkov, ki so hranjeni na mobilnih telefonih, je v prvi vrsti zakonodaja, ki ščiti uporabnika mobilnega telefona in njegove podatke, ki so hranjeni na mobilnem telefonu. Nadalje bi uporabnika morala ščititi programska in varnostna oprema mobilnega oziroma pametnega telefona. Pa vendar prihaja do zlorab teh podatkov in vdora v sam sistem telefona s strani hekerjev, kateri si na podlagi teh podatkov pridobivajo protipravno premoženjsko korist in za to nikdar ne odgovarjajo, saj za vdor v sistem mobilnih telefonov uporabljajo najboljšo opremo ali prihajajo iz držav, kjer je na tem področju zakonodaja zelo slaba ali je sploh ni. S tem je organom pregona zelo otežena preiskava teh kaznivih dejanj.

Edini legalen način, da se pridobijo podatki iz mobilnega telefona in podatki o komunikaciji je, ko nekdo na območju RS izvrši kaznivo dejanje in se podatki lahko pridobijo na podlagi pisne privolitve imetnika oziroma lastnika mobilnega telefona in na podlagi odredbe sodišče. Podatki, ki so hranjeni na mobilnem telefonu, lahko služijo kot dokaz v predkazenskem in kasneje tudi v kazenskem postopku. Podatki, ki so hranjeni na mobilnem telefonu se pridobijo na podlagi 219.a člena ZKP, kjer lahko imetnik poda privolitev za preiskavo, v kolikor je ne, pa se preiskava opravi na podlagi odredbe sodišča. Težava se tukaj pojavi, ko imetnik mobilnega telefona preiskovalcu ne izda vstopnih kod v sam sistem telefona. Takrat se morajo preiskovalci posluževati komercialnih programskih oprem, če pa nimajo dostopa do teh, pa morajo mobilne telefone poslati na preiskavo v tujino, kjer takšno programsko opremo imajo. Največja težava so mobilni telefoni proizvajalca Apple, s katerega v Sloveniji skoraj ni mogoče zavarovati podatkov, ki so hranjeni na mobilnem telefonu, če imetnik naprave ne poda gesel za vstop. Takrat

slovenski preiskovalci zaprosijo tuje varnostne organe, da to za njih opravijo, je pa to seveda povezano tudi s stroški. Storilci kaznivih dejanj imajo na svojih telefonih hranjenih veliko podatkov, ki služijo kot dokaz in so ti podatki nepogrešljivi za preiskovalce v postopku. Kot smo navedli v obeh analiziranih primerih, se sodbe sodišč, katere izrečejo sankcijo zoper storilce kaznivih dejanj, oprejo na podatke, ki so hranjeni v mobilnem telefonu in povežejo storilca kaznivega dejanja s samim kaznivim dejanjem. Za zavarovanje podatkov in s tem dokazov iz mobilnega telefona, ki je bil zasežen osumljencu kaznivega dejanja je, kot smo že navedli, dovolj osumljenčeva pisna privolitev za to. V kolikor privolitve ne da, preiskovalci na pristojno tožilstvo podajo pobudo za izdajo odredbe, tožilstvo pa na pristojno sodišče poda predlog za izdajo odredbe.

Za podatke o prometu elektronskih komunikacij pa mora policija takoj podati odredbo na način, da na pristojno tožilstvo poda pobudo za izdajo odredbe, tožilstvo pa poda predlog na pristojno sodišče za izdajo odredbe. Podlaga za navedeno je bil 149.b člen ZKP, katerega je ustavno sodišče v času pisanja diplomskega dela, 6. 7. 2023, razveljavilo. Podatki o prometu elektronskih komunikacij so preiskovalcem v preteklosti velikokrat pomagali pri preiskavanju kaznivih dejanj, saj je bilo mogoče ugotoviti lokacijo, kje se storilec nahaja, s kom je ter kdaj in s kom je komuniciral. Ti podatki so kasneje, kot smo navedli v primeru, služili tudi kot dokaz v samem kazenskem postopku in se je sodišče pri izreku sodbe oprlo na te dokaze. Teh podatkov policija po odločitvi Ustavnega sodišča v prihodnje več ne bi morala pridobiti, kljub temu, da je v preteklosti policija bila na podlagi odredbe upravičena do teh podatkov, saj je s tem dokazovala samo kaznivo dejanje. Policija je organ, ki bi moral biti upravičen do teh podatkov, v kolikor oseba izvrši kaznivo dejanje ali se na njega pripravlja. S tem policija, ki je zaupanja vreden organ in ne sme izdajati podatkov, ne bi kršila zasebnosti in pravic državljanov Slovenije, pač pa bi na točno določen način, ki ga veleva zakon, prišla do podatkov, s katerimi bi se kaznivo dejanje dokazovalo. Policiji je v 148. členu ZKP naloženo, da je dolžna odkriti in zavarovati sledove kaznivega dejanja in predmete, ki utegnejo biti dokaz v kazenskem

postopku. S tem, ko policija ne more tega zavarovati, je lahko ogrožen sam kazenski postopek in dokazovanje le-tega.

6.1 Odgovori na raziskovalna vprašanja

Na raziskovalno vprašanje, kako so lahko podatki na mobilnem telefonu ključni za uspešno raziskovanje v kriminalističnih postopkih, lahko iz vidika preiskave podatkov, ki so hranjeni na mobilnem telefonu, odgovorimo, da mobilni telefon oziroma podatki na njem, nedvomno služi in bo, v kolikor ne bo zakonodaja spremenjena, v predkazenskem postopku še naprej služil kot dokaz. Prav tako vedno obstaja povezava med podatki na telefonu in ostalimi dokazi, ki se zavarujejo pri preiskavi kaznivega dejanja v predkazenskem postopku. Storilci kaznivih dejanj velikokrat snemajo ali slikajo svoja dejanja ter odtujene predmete. Prav tako storilci komunicirajo s sostorilci ali z ostalimi udeleženci in se s tem dokazuje povezava med njimi.

Odgovor na raziskovalno vprašanje, kako so lahko podatki baznih postaj pomemben vir za informacije za ugotavljanje storilca na kraju izvršenega kaznivega dejanja, pa je bil člen, kateri je bil podlaga za pridobitev teh podatkov, ampak je bil s strani ustavnega sodišča razveljavljen in se ga preiskovalci v bodoče ne bodo več mogli posluževati in tako ne bodo mogli pridobiti tega dokaza. Kot smo navedli v drugem primeru je bil storilec obsojen, ker so preiskovalci in kasneje tožilstvo lahko dokazali, da je storilec za samo pripravo na kaznivo dejanje uporabljal mobilni telefon in komuniciral s sostorilci in so bili ti podatki ključni za obsodbo. Sodna praksa bo v prihodnosti pokazala, kako bodo policija, tožilstvo in sodišče lahko brez ključnih dokazov, kot je promet elektronskih komunikacij, lahko uspešno dokazovali in sodili storilcem kaznivih dejanj. Nedvomno pa bo njihovo delo s tem oteženo. Razumljivo je, da je vsak poseg v zasebnost človeka zelo občutljiv, pa vendar bi moral zakonodajalec policiji, tožilstvu in sodiščem, pod točno določenimi pogoji, omogočiti vpogled v promet elektronske komunikacije, saj te institucije ne smejo zlorabljati teh podatkov, ki lahko služijo le kot dokaz v postopkih. V kolikor pa bi do zlorab prišlo, bi bilo potrebno določiti hude sankcije. Ker je ustavno sodišče 149.b člen ZKP razveljavilo, lahko potrdimo, da pa v tem primeru v prihodnje

mobilni telefon oziroma promet elektronskih komunikacij več ne more služiti kot dokaz v predkazenskem postopku, dokler seveda zakonodaja ne bo drugače napisana.

Povezanost med podatki, ki so hranjeni na mobilnem telefonu in samimi podatki iz baznih postaj, kakor tudi med ostalimi dokazi, ki so bili ugotovljeni pri preiskavi kaznivega dejanja, nedvomno obstaja, in sicer se vsi ti dokazi med seboj prepletajo, na koncu pa kot skupek služijo kot dokaz. V kolikor enega od teh dokazov ne moremo ali pa ne smemo uporabiti, lahko pride do tega, da so tudi ostali dokazi neuporabni, saj so se lahko med seboj povezovali, kot je to razvidno v drugem primeru, in sicer brez pridobitve podatkov o komunikacijskem prometu ne bi bilo mogoče izslediti ostalih storilcev kaznivega dejanja in ostalih dokazov.

VIRI IN LITERATURA

Agencija za komunikacijska omrežja in storitve Republike Slovenije. *Mobilna omrežja.* https://www.akos-rs.si/radijski-spekter/raziscite/mobilna-omrezja

Ayers, R., Brothers, S., Jansen, W. (2014). *Guidelines of Mobile Device Forensics*. http://dx.doi.org/10.6028/NIST.SP.800-101r1

Barmpatsalou, K., Damopoulos, D., Kambourakis, G., Katos, V. (2013). *A critical review of 7 years of Mobile Device Forensics*. https://www.researchgate.net/profile/Dimitrios_Damopoulos/publication/258273700_Acritical_review_of_7_years_of_Mobile_Device_Forensics/links/00b49527a80aa132930 00000.pdf

Cerar, M., (2009). *Zakon*. https://www.iusinfo.si/medijsko-sredisce/kolumne/10976

Delo. (2010). *Pametni mobilni telefoni prevzemajo prevlado.* Pridobljeno 24.10.2023 iz https://old.delo.si/novice/znanoteh/pametni-mobilni-telefoni-prevzemajo-prevlado.html

European Justice. (2019). *Pravni viri, Vrste pravnih aktov - opis*. https://e-justice.europa.eu/content_member_state_law-6-si-maximizeMS-sl.do?member=1

Hoog, A. (2011). *Android Forensics. Investigation, Analysis, and Mobile Security for Google Android. Waltham: Elsevier*.

Informacijski pooblaščenec (2014). *Presoje vplivov na zasebnost pri uvajanju novih policijskih pooblastil. Smernice informacijskega pooblaščenca.* https://www.iprs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost_pri_uvajanju_novih_policijskih_pooblastil_Smernice_IP.pdf

Ipavec, S. (2018). *Pomen podatkov o elektronskih komunikacijah za kriminalistično preiskavo.* Univerza v Mariboru, Fakulteta za varnostne vede.

Kazenski zakonik (2023). *Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16, 27/17, 23/20, 91/20, 95/21, 186/21, 105/22 – ZZNŠPP in 16/23.*

Lin, X., Chen, T., Zhu, T., Yang, T. in Wei, F (2018). *Automated forensic analysis of mobile applications on Android devices. Digital investigation, 18(26), 59-66.* https://doi.org/10.1016/j.diin.2018.04.012

Litchfield S. (2010). *Defining the Smartphone – part 1.* AAS: http://www.allaboutsymbian.com/features/item/Defining_the_Smartphone.php

Litchfield S. (2010). *Defining the Smartphone – part 2 (testing the definition, head to head.*http://www.allaboutsymbian.com/features/item/Spy_versus_Spy_No_Smartphone_versus_Smartphone.php

Markelj, B., Bernik, I., (2013). *Sodobni aspekti informacijske varnosti.* Fakulteta za varnostne vede.

Ministrstvo za notranje zadeve, Policija, Služba generalnega direktorja policije (2023). *Letno poročilo o delu policije 2022.* https://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2022.pdf

Nemetz, S., Schmitt, S. in Freling, F. (2018). *A standardized corups for SQLite database forensics. Digital investigation, 18(24), 121-130.* Https://doi.org/10.1016/j.diin.2018.01.015

Petek, A. (2022). *Omejitve pri pridobivanju digitalnih dokazov.* Univerza v Mariboru, Fakulteta za varnostne vede.

Saleem, S, Popov, O. in Baggili, I. (2016). *A method and a case study for the selection of the best availible tool for mobile divice forensics using decision analysis.* Digital investigation, *16(6), 55-64.* https://doi.org/10.1016/j.diin.2016.01.008

Sodstvo Republike Slovenije (2018). *Na sodišču.* https://nasodiscu.si/ustava-republike-slovenije

Sotošek, S. (2016). *Vpliv zaščitnih mehanizmov na uspešno pridobivanje podatkov pri forenzični preiskavi mobilnih naprav na platformi android.* Univerza v Ljubljani, Fakulteta za upravo.

Statistični urad RS. (2023). *Svetovni dnevi brez mobilnih telefonov.* https://www.stat.si/StatWeb/news/Index/9355

Ustava Republike Slovenije (2021). *Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99, 75/16 – UZ70a in 92/21 – UZ62a.*

Višje sodišče v Mariboru. (2020). S*odba številka VSM Sodba III Kp 1101/2020, z 2. 9. 2020.*https://www.sodnapraksa.si/?q=*:*&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&id=2015081111440841

Vrhovno sodišče Republike Slovenije. (2021). S*odba številka VSRS Sodba I Ips 56957/2018, z 29. 4. 2021.* https://www.sodnapraksa.si/?q=id:2015081111447769&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&page=0&id=2015081111447769

Zakon o elektronskih komunikacijah (2017). *(Uradni list RS, št. 40/17)*.

Zakon o kazenskem postopku (2021). Uradni list RS, št. 176/21 – uradno prečiščeno besedilo, 96/22 – odl. US, 2/23 – odl. US in 89/23 – odl. US.

Zakon o nalogah in pooblastilih policije (2021). *Uradni list RS, št. 15/13, 23/15 – popr., 10/17, 46/19 – odl. US, 47/19 in 153/21 – odl. US.*

Univerza v Mariboru

Fakulteta za varnostne vede

IZJAVA O AVTORSTVU IN ISTOVETNOSTI TISKANE IN ELEKTRONSKE OBLIKE ZAKLJUČNEGA DELA

Ime in priimek študent-a/-ke: Marko Furlan

Študijski program:

Varnost in policijsko delo

Naslov zaključnega dela:

Mobilni telefon kot dokaz v predkazenskem postopku

Mentor: prof. dr. Bojan Dobovšek

Somentor: /

Podpisan-i/-a študent/-ka Marko Furlan

- izjavljam, da je zaključno delo rezultat mojega samostojnega dela, ki sem ga izdelal/-a ob pomoči mentor-ja/-ice oz. somentor-ja/-ice;
- izjavljam, da sem pridobil/-a vsa potrebna soglasja za uporabo podatkov in avtorskih del v zaključnem delu in jih v zaključnem delu jasno in ustrezno označil/-a;
- na Univerzo v Mariboru neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve avtorskega dela v elektronski obliki, pravico reproduciranja ter pravico ponuditi zaključno delo javnosti na svetovnem spletu preko DKUM; sem seznanjen/-a, da bodo dela deponirana/objavljena v DKUM dostopna široki javnosti pod pogoji licence Creative Commons BY-NC-ND, kar vključuje tudi avtomatizirano indeksiranje preko spleta in obdelavo besedil za potrebe tekstovnega in podatkovnega rudarjenja in ekstrakcije znanja iz vsebin; uporabnikom se dovoli reproduciranje brez predelave avtorskega dela, distribuiranje, dajanje v najem in priobčitev javnosti samega izvirnega avtorskega dela, in sicer pod pogojem, da navedejo avtorja in da ne gre za komercialno uporabo;
- dovoljujem objavo svojih osebnih podatkov, ki so navedeni v zaključnem delu in tej izjavi, skupaj z objavo zaključnega dela;
- izjavljam, da je tiskana oblika zaključnega dela istovetna elektronski obliki zaključnega dela, ki sem jo oddal/-a za objavo v DKUM.

Uveljavljam permisivnejšo obliko licence Creative Commons: CC BY-NC 4.0 (navedite obliko)

Kraj in datum: Maribor, 22. 11. 2023

Podpis študent-a/-ke: