UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Bojan Skokić

Prikriti preiskovalni ukrepi v Sloveniji in trendi razvoja tehnologije na področju specialne operativne tehnike

Diplomsko delo

Ljubljana, 2016

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Bojan Skokić

Mentor: izr. prof. dr. Uroš Svete

Prikriti preiskovalni ukrepi v Sloveniji in trendi razvoja tehnologije na področju specialne operativne tehnike

Diplomsko delo

Ljubljana, 2016

Prikriti preiskovalni ukrepi v Sloveniji in trendi razvoja tehnologije na področju specialne operativne tehnike

Policija ima na voljo prikrite preiskovalne ukrepe za odkrivanje težjih oblik kriminala, predvsem organiziranega, v vseh svojih pojavnih oblikah. Te ukrepe policija izvaja takrat, ko s klasičnimi kriminalističnimi metodami ne more pridobiti dokazov za pregon. Predhodno mora policija za uporabo prikritih preiskovalnih ukrepov pridobiti dovoljenja in odredbe pristojnih sodišč ter državnega tožilstva, saj navedeni ukrepi grobo posegajo v človekove pravice. Policija mora izvajati vse postopke zakonito, operativno neodvisno in v skladu s kriminalistično stroko ter veljavnimi zakoni. Ti ukrepi so glavno »orožje« policije proti katerikoli obliki kriminalne dejavnosti, zato organi pregona vlagajo veliko truda v zbiranje kakovostnih dokazov. V diplomski nalogi želim predstaviti trende, ki bodo v prihodnosti spremenili posege v zasebnost, česar pa trenutno veljavna zakonodaja ne pokriva ter pušča sivo cono za različne zlorabe, tako s strani posameznikov kot drugih akterjev. Razvoj tehnologije, ki je danes dostopna tako posameznikom, širšim množicam, podjetjem in mednarodnim korporacijam, omogoča da lahko vsi nadzorujemo in spremljamo vsakogar, če le posedujemo primerno tehniko in znanje. Svetovni trg ponuja različno specialno tehniko državam, podjetjem, posameznikom in kriminalnim združbam. Po eni strani z zakoni reguliramo in nadzorujemo delovanje organov pregona, po drugi pa je država nemočna pri zagotavljanju temeljnih pravic in svoboščin posamezniku, ko ga drugi nadzira.

Ključne besede: prikriti preiskovalni ukrepi, specialna operativna tehnika, policija.

Covert investigational measures in Slovenia and trends in the development of technology in the field of special operational techniques

The police are using covert investigational measures for detection of serious crime, particularly organized, in all its manifestations. These measures are used when standard criminal investigation methods cannot obtain evidence for the prosecution. In order to obtain covert investigation measures, the police must gain permissions and orders from competent courts and public prosecutor's office, because those measures seriously infringe human rights. The police must carry out all the procedures legally, operationally independent, in accordance with the criminal profession and as well as applicable laws. These measures represent main "weapon" of the police against any form of criminal activity, therefore law enforcement authorities invest a lot of effort in gathering quality evidence. In the diploma thesis I would like to present the trends that would change the encroachments on privacy in the future and this is not covered by the current legislation and leaves the grey area for various abuses, both by individuals and other actors. The development of technology that is available today for individuals, masses, businesses and international corporations, allows everyone to control and monitor everyone, if only possess appropriate technology and knowledge. Global market offers different special technique to countries, companies, individuals and criminal organizations. On one hand the laws regulate and supervise the operation of law enforcement authorities, but on the other hand the state is powerless to guarantee fundamental rights and freedoms of the individual, when it is monitored by others.

Key words: covert investigational measures, special technique, police.

KAZALO

KAZALO SLIK

1 UVOD

Velikokrat je kriminalna dejanja težko dokazati, potencialno pa lahko predstavljajo nevarnost tako za organe pregone, kot tudi za državljane. Policija je od nekdaj iskala rešitve oziroma metode, s katerimi bi lahko učinkovito in z minimalnimi stroški dokazala kriminalna dejanja. Razvoj prikritih preiskovalnih ukrepov[1] (PPU) je šel v smer z razvojem tehnologije, kar pa na žalost dan današnji predstavlja bolj problem kot rešitev za odkrivanje kriminala, predvsem organiziranega.

Policija izvaja PPU z namenom pridobivanja dokazov, ko slednje z običajno preiskovalno tehniko ni mogoče. PPU so policiji in organom pregona na voljo predvsem za odkrivanje težjih oblik organiziranega kriminala. Glavni problem PPU je poseganje v osnovne človekove pravice, saj so v primeru uporabe PPU te lahko kršene. Po drugi strani pa je pridobivanje zakonitih dokazov proti organiziranemu kriminalu lahko oteženo. Izredno težko je najti pravo mejo, ki bi bila primerna tako za eno kot za drugo stran. Zato mora biti delo policije izvedeno v skladu z zakoni in na podlagi ustrezno izdanih dovoljenj in odredb s strani pristojnih sodišč.

Diplomsko nalogo sem pripravili z namenom opisa in predstavitve PPU, novejših tehnik zbiranja dokazov in nadzorovanja posameznikov v boju proti kriminalnim dejanjem. Glavni namen diplomskega dela je predstavitev trendov, ki bodo v prihodnosti spremenili posege v zasebnost, česar pa trenutno veljavna zakonodaja ne pokriva ter pušča sivo cono za različne zlorabe, tako s strani posameznikov kot drugih akterjev. V diplomski nalogi bom opisal tudi nadzor nad uporabo tehničnih sredstev za zbiranje, prenos in obdelavo osebnih podatkov, ki je lahko z razvojem tehnologije otežen. V današnjem času je namreč vse več pripomočkov lahko in enostavno dostopnih tako posameznikom, kot tudi širšim množicam ali pa raznim podjetjem, kar pa omogoča nadzor nad vsakim posameznikom, v kolikor imamo na voljo ustrezno znanje. S tem je seveda lahko kršena osnovna človekova pravica nad zasebnostjo, kar bo prav tako predmet naše diplomske naloge. Varovanje zasebnosti je tako pomembno področje, da je zapisana tudi v ustavi Republike Slovenije, ki v 35. členu pravi, da mora biti vsakemu posamezniku zagotovljena pravica do zasebnosti in osebnostnih pravic, hkrati pa mora biti zagotovljena nedotakljivost človekove telesne in duševne celovitosti.

[1] PPU – prikriti preiskovalni ukrepi

V medijih se velikokrat omenja »neustrezno« delo policije, predvsem, ko gre za pridobivanje dokazov zoper težja kriminalna dejanja. Ničkolikokrat so bile obsodbe razveljavljenje zaradi neustrezno pridobljenih dokazov zoper obtožene.

1.1 Predmet in cilj diplomske naloge

Predmet diplomske naloge je opredelitev in opis PPU, novejših tehnik nadzorovanja posameznikov ter ovrednotenje dela policije, ko gre za prekrite preiskovalne ukrepe. Cilj in pomen diplomske naloge je predstavitev PPU po veljavni zakonodaji, opisi vseh ukrepov ter predstavitev specialne operativne tehnike ter trendov razvoja v prihodnosti. Zanima me tudi problem razvoja novih tehnologij s področja specialne operativne tehnike, ki neformalnim akterjem in slehernemu posamezniku ali skupinam omogoča zlorabo dosežkov razvoja tehnologije za lastne potrebe in interese.

1.2 Raziskovalne metode

V diplomskem delu bom uporabil predvsem metodo zbiranja primarnih in sekundarnih pravnih in drugih virov s področja, ki ga zajema diplomsko delo. Nato bom pridobljene podatke analiziral ter uporabil analitično sintetično metodo primarnih (pravnih) virov.

1.3 Hipoteza

V diplomskem delu si bom zastavil hipotezo, ki pravi, ***da bo tehnološki razvoj na področju specialne operativne tehnike otežil nadzor nad uporabo tehničnih sredstev za zbiranje, prenos in obdelavo osebnih podatkov***. Na koncu bom postavljeno hipotezo preveril.

1.4 Struktura

Diplomsko delo je v osnovi sestavljeno iz devetih delov. V *prvem* delu bom opredelil predmet in cilje diplomske naloge, raziskovalne metode, hipotezo in strukturo diplomske naloge, tu so tudi opredeljeni temeljni pojmi, ki bodo v nadaljevanju predstavljali osnovno izhodišče za celotno diplomsko delo (organiziran kriminal, organ pregona). V *drugem* delu so našteti in opisani prikriti preiskovalni ukrepi slovenske policije po veljavni zakonodaji. V *tretjem* delu je opisana specialna operativna tehnika, klasična in nove oblike tehnologije na tem področju.

V *četrtem* delu bom opisal nadzor nad uporabo prikritih preiskovalni ukrepov policije. V *petem* delu je opisana pravica do zasebnosti, v *šestem* delu pa Zakon o varstvu osebnih podatkov. V s*edmem* delu je zajet predlog ureditve uporabe specialne operativne tehnike, *osmi* del predstavlja analiza komercialno dostopnih tehnologij v odnosu do kršenja posameznikove zasebnosti. V zadnjem, *devetem* delu pa bom podal sklep diplomske naloge, v katerem bom postavljeno hipotezo potrdil oziroma zavrnil.

1.5 Opredelitev temeljnih teoretičnih pojmov

1.5.1 Organizirani kriminal

Do sedaj še ne obstaja definicija organiziranega kriminala, ki bi bila mednarodno sprejeta. Zato strokovnjaki iz tega področja poizkušajo sestaviti enotno definicijo, ki bi nato služila kot glavna in mednarodno sprejeta teoretična podlaga za oblikovanje različnih politik, praks, ukrepov in mehanizmov za boj proti organiziranemu kriminalu. Na podlagi sprejete definicije bi učinkoviteje uredili pravni sistem in poenotili mednarodna prizadevanja za zatiranje organiziranega kriminala (Dobovšek 2009).

Največ poskusov definiranja izhaja iz ZDA[2], kjer je organiziran kriminal opredeljen kot združenje dveh ali več oseb, namenjeno vzpostavitvi monopola na določenem zemljepisnem prostoru, v takšni kriminalni dejavnosti, ki prinaša dobiček ali kontinuiran finančni dohodek. To dosega s terorjem ali nasiljem proti tistim, ki se upirajo ali nasprotujejo njegovemu

[2] Definicija povzeta po FBI (angl. *Federal Bureau of Investigation*)

razvoju, razrašča pa se s podkupovanjem javnih delavcev, katerih sodelovanje je nujno potrebno za obstoj in nadaljnji razvoj ilegalnega delovanja (Dobovšek 2009).

1.5.2 Organ pregona

Pojem organi pregona zajema policijo in državno tožilstvo, ki po veljavni zakonodaji usmerja aktivnosti policije. Delo državnega tožilstva, policije in drugih pristojnih državnih organov, ki sodelujejo pri pregonu storilcev kaznivih dejanj ureja Uredba o sodelovanju državnega tožilstva, policije in drugih pristojnih državnih organov in institucij pri odkrivanju in pregonu storilcev kaznivih dejanj ter delovanju specializiranih in skupnih preiskovalnih skupin (Nacionalni sistem integritete 2016).

2 PRIKRITI PREISKOVALNI UKREPI

Osnovno načelo policije je, da prikrite preiskovalne ukrepe predlaga v primerih, ko s klasičnimi preiskovalnimi metodami ni mogoče doseči želenih ciljev oz. rezultatov ali pa bi izvedba klasičnih preiskovalnih ukrepov razkrila dejavnosti policije.

Po Zakonu o kazenskem postopku (ZKP)[3] lahko policija uporablja PPU, če obstajajo utemeljeni razlogi za sum, da je določena oseba izvršila, še izvršuje ali organizira izvršitev katerega izmed kaznivih dejanj, pri čemer je mogoče utemeljeno sklepati, da policisti z drugimi ukrepi tega dejanja ne morejo odkriti, preprečiti ali dokazati oziroma bi bilo to povezano z nesorazmernimi težavami (ZKP, 149.a člen).

PPU izvajajo policisti ali drugi zakonsko določeni državni uslužbenci pod posebno določenimi pogoji in se razlikujejo od običajnih ukrepov uradnih pooblaščenih oseb. Najpomembnejši značilnosti PPU sta tajnost izvajanja in močan poseg v človekove pravice in svoboščine. Zaradi tega jih organi pregona uporabljajo pri najnevarnejših kaznivih dejanjih, ki so navedeni v ZKP (Žaberl 2006).

Med PPU spadajo:

- tajno opazovanje,
- pridobitev podatkov o udeležencih, okoliščinah in dejstvih elektronskega komunikacijskega prometa,
- nadzor elektronskih komunikacij s prisluškovanjem in snemanjem ter kontrola in zavarovanje dokazov o vseh oblikah komuniciranja, ki se prenašajo v elektronskem komunikacijskem omrežju
- kontrola pisem in drugih pošiljk
- kontrola računalniškega sistema banke ali druge pravne osebe, ki opravlja finančno ali drugo gospodarsko dejavnost
- prisluškovanje in snemanje pogovorov s privolitvijo vsaj ene osebe udeležene v pogovoru

[3] *Zakon o kazenskem postopku* (uradno prečiščeno besedilo) (ZKP-UPB8). Ur. L. RS 32/2012 (4. Maj 2012)

- prisluškovanje in opazovanje v tujem stanovanju ali drugih prostorih z uporabo tehničnih sredstev za dokumentiranje
- navidezen odkup, navidezno sprejemanje oziroma dajanje daril ali navidezno jemanje oziroma dajanje podkupnine
- tajno delovanje
- sporočanje zaupnih podatkov in pošiljanje dokumentacije o vlogah, depozitih, stanju in prometu na računih ali drugih poslih osumljenca, obdolženca in drugih oseb (Dežman in Erbežnik 2003).

Po zaključku uporabe PPU, mora policija vse posnetke (tako digitalni zapis vseh prestreženih posnetkov, kot tudi prepise), sporočila in predmete, ki so bili pridobljeni z uporabo teh ukrepov, skupaj s poročilom, ki obsega povzetek zbranih dokazov, predati državnemu tožilcu (ZKP, 153. člen).

PPU predstavljajo posebna policijska pooblastila, ki so od ostalih oz. splošnih policijskih pooblastil razlikujejo v jakosti posega v človekove pravice ter po dejstvu, da so izvajani prikrito in ne javno. Razlikujejo se tudi med seboj, vendar imajo nekatere skupne izvedbene in zakonske značilnosti. Te značilnosti so slednje:

- Za pridobitev odredb mora obstajati utemeljeni razlog za sum (oz. visoka stopnja verjetnosti), da je bilo neko kaznivo dejanje storjeno, pri čemer ni mogoče dokazov pridobiti drugače kot s PPU oz. bi na drugačen način ogrožali življenja in zdravje ljudi.
- Vsi ukrepi so izvajani v predkazenskem postopku, ko je bilo kaznivo dejanje že izvršeno oz. je v fazi izvrševanja. Lahko pa se ukrepe izvaja tudi v fazi, ko do kaznivega dejanja še ni prišlo, vendar pod posebnimi pogoji.
- V kolikor so bili PPU izvajani zakonito imajo nato v kazenskem postopku dokazno vrednost in sodba lahko temelji na podlagi zbranih dokazov.
- PPU so izvajani v tajnosti (prikrito), tako da oseba, proti kateri je se izvajajo tega ne ve. Prikritost oz. tajnost je bistvena značilnost teh ukrepov, saj policija nebi prišla do relevantnih dokazov, če bi osumljenec vedel, da ga preiskujejo (Žaberl 2006, 310 – 311).

2.1 Pravna podlaga za prikrite preiskovalne ukrepe

PPU so določeni in definirani v ZKP od člena 149.a do člena 156, medtem ko mednarodno sodelovanje urejajo mednarodne pogodbe in sporazumi. V navedenih členih so opisani posamezni PPU, dokazni standardi, vsebina odredb za posamezna kazniva dejanja, za katera se sme odredba izdati, kdo lahko odredbo izda ter način in čas izvajanja PPU. ZKP so določeni tudi pogoji za uvedbo PPU ter način ravnanja s pridobljenimi izsledki.

Dokazni standardi, ki so potrebni za uvedbo PPU so: razlogi za sum, utemeljeni razlogi za sum in utemeljen sum. Ti standardi predstavljajo procesna jamstva, ki so namenjena temu, da se zaščitijo človekove pravice in temeljne svoboščine vpletenih v kazenskem postopku, pred posegi državnega represivnega aparata. Za policijo je zadosten razlog za sum, da je bilo neko kaznivo dejanje storjeno, na sodišču pa velja utemeljen sum, kjer pa je potrebna sodna preiskava, da bi ta sum potrdila. ZKP ne opredeljuje pojma razlogi za sum in utemeljen sum, ker zakon določa, da so zadosti dejstva, ki kažejo na elemente in storilca kaznivega dejanja. V postopku policija najprej ugotavlja z manjšo verjetnostjo in nato z večjo, ki na koncu privede do dokaza, ki je potreben za obsodilno sodbo. Razlogi za sum temeljijo na praksi dela policije pri pregonu in na sodbah sodišč. Utemeljeni razlogi za sum so podlaga za globok poseg v človekove pravice in se lahko izvajajo v predkazenskem postopku, ko vpletena oseba še ne ve, da je pod preiskavo kot domnevni storilec (Mozetič 2007).

PPU lahko odreja policija sama, vendar le za ukrepe kadar gre za pridobitev informacije o lastniku ali uporabniku določenega komunikacijskega sredstva; državni tožilec za ukrepe, ko se milejše posega v pravice posameznika in preiskovalni sodnik za ukrepe, ki pomenijo najhujši poseg v pravice in svoboščine (ZKP, 149.a – 156. člen).

Skupne značilnosti PPU so naslednje:

- Subsidiarnost uporabe PPU, kar pomeni, da policija s klasičnimi policijskimi pooblastili ni mogla zbrati ustreznih dokazov;
- vsi PPU so časovno omejeni;
- vsi PPU se izvajajo v tajnosti, torej na način, da oseba proti kateri se izvajajo, tega ne ve ter

- vsi PPU imajo dokazno vrednost, saj predstavljajo dokaz v nadaljnjem kazenskem postopku, v kolikor so bili ukrepi odrejeni in izvajani zakonito (ZKP, 149.a – 156. člen).

2.2 Pogoji za uporabo prikritih preiskovalnih ukrepov

PPU se lahko uporabljajo v primeru, da obstajajo utemeljeni razlogi za sum, da je oseba izvršila, še vedno izvršuje ali pa pripravlja izvršitev katerega izmed kaznivih dejanj, pri čemer je mogoče utemeljeno sklepati, da policisti z drugimi ukrepi ne morejo dokazati tega dejanja ali pa bi to povzročilo nesorazmerne težave. PPU se uporabljajo še v primeru, da je mogoče utemeljeno sklepati, da bi opazovanje druge osebe, ki ni osumljenec privedlo do identifikacije osumljenca, kjer osebni podatki niso znani, prav tako ne njegovo prebivališče ali lokacija, kjer se nahaja. Ko gre za kazniva dejanja, ki imajo v zakonu predpisano kazen zapora petih let ali več, je policija prav tako upravičena do uporabe PPU (ZKP, 149.a člen).

Če gre za kazniva dejanja, ko je ogrožena varnost Republike Slovenije (RS) in njena ustavna ureditev ter v primeru kaznivih dejanj kjer je ogrožena človečnost in mednarodno pravo, za katera je v zakonu predpisana kazen zapora petih ali več let, je uporaba PPU prav tako upravičena. PPU se lahko uporablja tudi v primeru drugih kaznivih dejanj, za katera je v zakonu predpisana kazen zapora osmih let ali več (ZKP, 150. člen).

Predlog in odredba za uporabo PPU morata vsebovati sledeče:

- Podatke za določitev osebe, proti kateri se predlaga oziroma odreja ukrep;
- utemeljitev razlogov za sum, da gre za izvrševanje, pripravo ali organizacijo določenih kaznivih dejanj;
- kateri ukrep se predlaga oziroma odreja, način izvajanja ukrepa, njegov obseg in trajanje, točno določitev prostora in/ali kraja izvajanja ukrepa, elektronsko – komunikacijsko sredstvo in ostale pomembne okoliščine, ki narekujejo uporabo posameznega ukrepa;
- utemeljitev oziroma ugotovitev, da je posamezen ukrep potrebno uporabiti, ko ni mogoče zbiranje dokazov na drug način in je uporaba ostalih milejših ukrepov onemogočena ter

- ustno odredbo, ki narekuje utemeljitev razloga za predčasno izvrševanje (ZKP, 149.a člen).

3 SPECIALNA OPERATIVNA TEHNIKA

3.1 Definicija

Uporaba tehničnih sredstev sega v začetke zbiranja tajnih podatkov. Dejavnost zbiranja podatkov je lahko nevarna, saj lahko pride do kompromitacije subjekta in dejavnosti. Da bi zmanjšali nevarnost najdbe obremenilnega materiala in zagotovili tajnost dejavnosti, so si zbiralci tajnih podatkov zamislili najrazličnejše zapise zbranih podatkov (Pipan 2009, 28).

3.2 Klasična specialna operativna tehnika

Med klasično specialno operativno tehniko spadajo:

- Naprave, ki prestrezajo elektronske komunikacije v vseh oblikah komuniciranja, ki se prenaša v elektronskem komunikacijskem omrežju;
- naprave, ki spremljajo gibanje in določajo položaj preiskovane osebe;
- prikrite naprave za snemanje zvoka in slike;
- posebne optične naprave, kot npr. očala za nočno gledanje, naprave, ki zaznavajo toploto telesa, specializirane kamere in fotoaparati;
- naprave, ki omogočajo tajen vstop v stanovanja in druge prostore in
- motilci signalov, detektorji signalov in neznanih virov napajanja (Uredba o oborožitvi, vojaški opremi, specialni operativni tehniki in naročilih zaupne narave, 4. člen).

3.3 Nove oblike in tehnologije na področju specialne operativne tehnike

Na tem področju se tehnologija hitro spreminja, še preden pride v splošno uporabo, jo že uporabljajo zasebniki, velikokrat pa vlada ne more narediti veliko, da bi lahko preprečila uporabo specialne operativne tehnike na zasebnem nivoju.

1. Tehnologije, ki podpirajo operativno delovanje na terenu in jih izvajajo tajni operativci:

- tajno opazovanje in sledenje
- tajno delovanje
- navidezni odkup, navidezno sprejemanje oziroma dajanje daril ali navidezno jemanje ali dajanje podkupnine
- tajno fotografiranje in video snemanje
- tajno prisluškovanje in snemanje pogovorov

2. Tehnologije za tehnično zbiranje podatkov:

- prisluškovanje pogovorom oziroma kakršnim koli komunikacijam
- obvezna hramba podatkov v prometu elektronskih komunikacij
- naprave za dekodiranje šifriranih komunikacij
- odkrivanje, prepoznavanje in določanje lokacije ter zasledovanje komunikacijskih sredstev in naprav
- motilci signalov
- avtomatsko (biometrijsko) prepoznavanje ljudi, obrazov in sledenje
- inteligentni videonadzor
- računalniški virusi
- avtomatska prepoznava registrskih tablic (Pipan 2009).

3. Novosti na področju tehnologije:

- *Software Defined Radio*[4]: skupaj z Open Source programsko opremo omogoča prestrezanje SMS sporočil in snemanje pogovorov v GSM (večinoma zgolj 2G, ne pa tudi 3G) omrežju. Dosegljivo bolj ali manj vsem, za zelo malo denarja.
- Naprave za zaznavanje elektromagnetnega "podpisa" elektronskih naprav: večina elektronskih naprav oddaja različno elektromagnetno valovanje, glede na specifiko spektra sevanja, se da določiti tip elektronske naprave na daljavo.
- Miniaturizacija računalniških sistemov omogoča vgradnjo "bug[5]" komponent v obstoječe računalniške naprave (med tipkovnico in računalnik, na omrežni kabel ipd.).

[4] SDR

Celoten PC z oddajnikom, ni večji od USB ključka. Enaka oprema se lahko uporablja tudi za simulacijo naprav, RFID[6] kartic ipd.

- Radar za pregledovanje tal visoke ločljivosti[7]: gre za napravo, ki dovolj majhna, da se lahko namesti na ultralahko letalo, omogoča pa snemanje površja do oddaljenosti 40 km z ločljivostjo okoli 1 m ali manj. Primerna je za sledenje vozil, plovil na morju, detekcijo razlitij na vodni površini ipd. (Zaugg, Hudson in Long 2006).
- Vedno manjše in cenejše termalne in nočne kamere, ki jih je mogoče namestiti celo na pametni telefon (Flir 2016).
- RFID podkožni vsadki za označevanje oseb (Technovelgy 2016).
- Radar, ki penetrira skozi zid[8]: radar, ki omogoča zaznavanje skozi zidove. Zaenkrat ima še slabo ločljivost, zaznava pa obliko prostora ter omogoča informacije o obliki in materialu tarče v njem. Možno je celo zaznavanje dihanja človeka skozi 23 cm debel zid (Engin, Çiftçioğlu, Özcan in Tekin 2007).
- *Data mining* pomeni združevanje velike količine podatkov in je na voljo v družabnih omrežjih. Se dela že sedaj ročno, moderna programska oprema pa omogoča hitrejše delo in profiliranje (Chen in drugi 2004).
- Brezpilotni letalniki, ki so vse manjši in vedno bolj zmogljivi ter vzdržljivi, saj omogočajo več ur lebdenja na določeni točki, oddaljeno pristajanje, vsebujejo kamere za nočno snemanje ipd. (BSB International 2015).

3.3.1 Brezpilotni letalniki

Brezpilotni letalniki se uvrščajo v posebno vejo letalstva, in sicer k letalnikom brez pilota oz. posadke. Brezpilotni letalniki so bili razviti predvsem z namenom nadziranja, izvidovanja in obveščanja. Razvoj takih letal so podpirali različni vojaški centri in obveščevalne agencije, saj so hitro spoznali prednosti, ki jih taka letala prinašajo. Na začetku so jih uporabljali za nadzor, izvidovanje in obveščanje na kriznih območjih, kjer je bilo preletavanje s helikopterji ali letali nevarno. Tu so bili prvi Izraelci, ki tudi veljajo za začetnike na tem področju, seveda pa

[5] Bug komponenta predstavlja prestreznik, ki prestreza kakršnokoli delo na računalniku (uporaba tipkovnice, vnos gesel ipd.).
[6] angl. *Radio Frequency IDentification* oz. Radiofrekvenčna identifikacija
[7] angl. *High resolution ground scanning radar*
[8] angl. *Wall penetrating radar*

Američani niso zaostajali. Razvili so veliko različnih letalnikov, ki opravljajo različne naloge, v grobem pa jih lahko razdelimo v štiri različne skupine:

- Strateška brezpilotna letala: delujejo na velikih višinah, zunaj vidnega območja, avtonomna so več kot 24 ur.
- Taktična brezpilotna letala: delujejo na srednjih višinah, izven vidnega območja, avtonomna so 12 ur.
- Mini UAV[9]: letijo na vidnem območju in so avtonomna 2 uri.
- Bojni brezpilotni letalniki UCAV[10]: ti letalniki so razviti v dve smeri, in sicer v ofenzivne namene, saj so opremljeni z raketami in/ali bombami ter v defenzivne namene, saj so opremljeni z elektronskimi motilniki signalov in napravami za motenje delovanja elektronskih naprav (Podgoršek 2008).

Brezpilotni letalniki se vse bolj uporabljajo za tržne namene, zato je potrebno zakonsko in pravno urediti uporabo ter določiti pravo razmerje med uporabnostjo in varnostjo ter preprečiti, da bi ravno instrument za zagotavljanje varnosti postal vir njenega ogrožanja. Čeprav brezpilotni letalniki sestavljajo in proizvajajo tudi v Sloveniji, pa posledice njihove uporabe na področju zagotavljanja varnosti še niso preučene, prav tako je področje komercialne uporabe na pravnem področju precej neurejeno (Svete in drugi 2015, 350).

Brezpilotna letala so sposobna samostojnega letenja, ki jih nadzirajo računalniki ali pa jih iz razdalje krmarijo človeški operaterji. Na splošno je letalnik zgolj plovilo oz. nosilec, uporaben postane šele, če ima vgrajen podsistem za opravljanje nalog. Sistemov za opravljanje nalog je več vrst, in sicer jih lahko razdelimo v tri večje skupine; sistemi za transport, sistemi za nadzor in zajem podatkov ter oborožitveni sistemi (Svete in drugi 2015, 351 – 352).

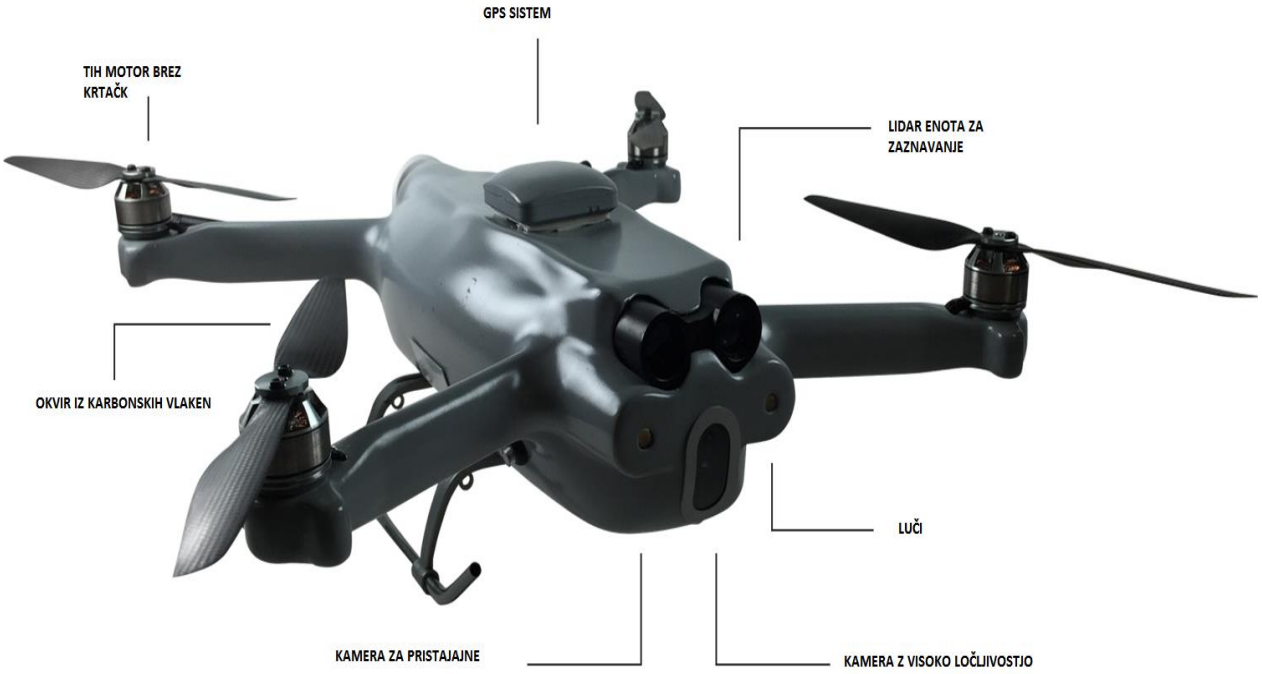
3.3.1.1 Brezpilotni letalnik SQ – 4

Brezpilotna letala so lahko opremljena z zmogljivimi objektivi, ki omogočajo nadzor od daleč ali IMSI lovilci za prestrezanje mobilnih komunikacij, radarskimi tehnologijami za spremljanje lokacije ciljev in spremljanje njihovega gibanja in biometričnimi tehnologijami za prepoznavanje in profiliranje prebivalstva. Brezpilotna letala multiplicirajo zmogljivosti

[9] angl. *Unmanned Aerial Vehicles*
[10] angl. *Unmanned Combat Aerial Vehicle*

tehnologij nadzora zaradi svoje fleksibilnosti gibanja, prikritega načina delovanja in nizkimi stroški nakupa ter vzdrževanja (BCB International 2015).

Slika 3. 1: Prikaz brezpilotnega letalnika SQ – 4 UAS



Vir: BCB International (2015)

SQ – 4 tehta (glej Sliko 3.1) samo okoli 1000 gramov (skupaj z baterijo), saj je izdelan iz lahkih karbonskih vlaken in ponuja brezpilotni mini letalnik s funkcijo navpičnega vzleta in pristanka VTOL[11]. Odvisno od zahtev, RECON[12] sistem SQ – 4, lahko leti na relaciji do 3 kilometre, s trajanjem letenja do 60 minut. SQ – 4 RECON je mogoče upravljati z daljinskim upravljalnikom ali pa lahko leti avtonomno s pomočjo GPS – točkovnega načina navigacije. Njegova vertikalna hitrost je 6,5 m/s, horizontalna pa več od 8 m/s. Velika prednost mini letalnika je tudi območje delovne temperature, ki sega od -20 do 50 °C, prav tako pa je letalnik vodoodporen, kar mu omogoča letenje tudi v dežju (BCB International 2015).

Mini letalnik je sposoben širokega spektra nalog in je zelo enostaven za letenje in upravljanje z minimalnim usposabljanjem. Zaradi svoje majhnosti je zelo primeren za prikrito opazovanje ljudi, vozil, lokacij, zemljišč, stavb itd. Ima funkcijo avtopilota, ki ima združene komunikacijske module za nadzor, video in telemetrijo. Multiprocesor ima vgrajen rezervni

[11] VTOL – Vertical Take Off and Landing – funkcija navpičnega pristajanja in vzletanja
[12] RECON – angl. Reconnaisance – opazovalni, npr. opazovalno letalo

sistem za obnovitev med letom ter samostojno napajanje. Avtopilotne lastnosti se lahko uporabljajo za avtomatsko vzletanje in pristajanje, brezpilotni letalnik lahko stoji na trenutnem položaju na konstantni višini, lahko se vrne v začetni položaj, prav tako vsebuje dve kameri visoke ločljivosti, ki omogočata snemanje pod kotom (med 90° in 130°), snemanje ponoči ipd. Letalnik lahko leti tudi v prostoru, saj ima vgrajen senzor LIDAR. Navzdol obrnjene kamere omogočajo pristanek SQ – 4 na daljavo. Motorje se lahko ugasne in tako lahko letalnik nadzoruje območje tudi do 4 ure (BCB International 2015).

3.3.2 Biometrična tehnologija za prepoznavo obrazov in nadzorovanje gibanja Verilook Surveillance SDK

Produkt je namenjen razvoju specializirane programske opreme, ki opravlja biometrično obrazno identifikacijo in beleži gibanje pešcev in/ali predmetov s pomočjo videa ali slik iz visoko ločljivih digitalnih nadzornih kamer. SDK[13] se uporablja za pasivno identifikacijo tudi, ko mimoidoči pešci ne želijo biti prepoznani, torej zakrivajo obraz. Seznam možnih uporabnikov zajema organe pregona, varnostne službe, lokale in restavracije, trgovske centre, aplikacije za štetje obiskovalcev, nadzorne centre prometa in druge poslovne uporabnike. Aplikacija Verilook Surveillance deluje v okolju Windows in Linux (Neurotechnology 2015).

Glavne značilnosti biometrične tehnologije Verilook Surveillance SDK so:

- zaznavanje obrazov v realnem času, primerjava obstoječih datotek obrazov z novimi vnosi in posledično s tem odkrivanje tistih, ki se jih spremlja ali išče
- dva algoritma za nadzorne sisteme: biometrični za prepoznavo obrazov in algoritem za zaznavanje premikanja ter sledenje osebam dokler ne izginejo nadzornim kameram; aplikacija je sposobna ugotoviti tudi ali je oseba vstopila v objekt, se zadržuje ali zapušča določeno območje
- hkratno sledenje večjemu številu obrazov ali predmetov preko video prenosa v živo
- napredno prepoznavanje in sledenje pešcem in objektom z naprednimi programskimi opcijami
- klasifikacija po spolu, nasmešku, odprtih ustih, zaprtih očeh, zatemnjenih očalih itd.

[13] SDK – Software Development Kit – programsko orodje

- avtomatsko beleženje dnevnikov dogodkov in poročil, prepoznavanje novih obrazov iz video nadzora in primerjava z že obstoječimi
- mrežno povezovanje večjega števila kamer in računalnikov z namenom izvajanja masovnega nadzora (Neurotechnology 2015).

3.3.3 Aplikacija za nadzor komunikacij, ki se izvajajo preko mobilnega telefona – Surveillance station 7.0 DS CAM

Mobilna aplikacija za nadzor omogočajo uporabniku, da na mobilnemu telefonu spremlja video v živo ali pa dostopa v bazo shranjenih videoposnetkov iz katere koli lokacije v okviru svojega sistema nadzora. Integrirana časovnica lahko sproti obvešča o dogodkih in omogoča uporabniku, da nemudoma sprejme različne odločitve in ukrepe. Posamezne slike in video posnetke lahko uporabnik shrani na mobilni telefon ali jih deli z drugimi napravami v mreži. Aplikacija je primerna za telefone z iOS in Android operacijskim sistemom (glej Sliko 3.2).

Slika 3. 2: Prikaz sistema Synology Surveillance Station

Vir: Neurotehnology (2015)

Produkt ima številne prednosti, med drugim omogoča hkratno spremljanje do 6 kamer in sprotno zajemanje slik, upravljanje položaja kamer na daljav in upravljanje baze posnetkov in sproten pregled posnetkov. Nadzorna postaja zagotavlja konstantni sistem obveščanja in skrbi, da je uporabnik seznanjen z vsem, kar se dogaja na IP kameri preko sporočil SMS, e – pošte, in potisnih obvestil v aplikaciji DS cam za iOS in Android naprave. Prav tako si lahko uporabnik ustvari razpored obveščanja in se odloči, če želi prejemati sporočila (Neurotehnology 2015).

3.3.4 Osebni navigacijski sistem – *Personal eye system*

PES[14] oziroma osebni navigacijski sistem je aplikacija namenjena navigaciji, sledenju in deljenju taktičnih podatkov znotraj skupine uporabnikov. PES je namenjen profesionalnim uporabnikom kot so vojaki, policisti, zasebni detektivi, varnostne službe, gasilci, pripadniki civilne zaščite, gorske reševalne službe. Skratka vsem, ki potrebujejo topografsko navigacijo. Namen PES – a je, da združi GPS sprejemnik, mobilni telefon in topografsko karto v eno priročno napravo.

Prednosti uporabe PES – a:

- Učinkovitejše načrtovanje poti;
- hitrejše zbiranje in deljenje informacij;
- skoraj realno časovno sledenje lastnim enotam ter
- digitalni zemljevid, ki omogoča poleg navigacije tudi snemanje poti.

Prikaz lastne pozicije

Lastna pozicija je vedno vidna v zgornjem delu zaslona, v izbranem koordinatnem sistemu (DMS, UTM ali MGRS) skupaj z nadmorsko višino, hitrostjo in natančnostjo. Poleg tega je prikazan tudi vir lokacijske informacije (GPS sprejemnik ali GSM omrežje).

[14] angl. *Personal Eye System*

Uporaba GPS omrežja

PES uporablja vgrajen GPS sprejemnik za določanje lastnega položaja. Hitrost določanja in natančnost, pa sta odvisna od kvalitete signala in GPS sprejemnika. V primeru ko sateliti niso vidni, pa PES poizkuša svoj položaj uganiti iz podatkov ki so na voljo v GSM omrežju.

Sledenje

PES sproti beleži opravljeno pot in sled prikaže na zemljevidu. PES lahko shrani več poti in jih hkrati prikazuje, medtem ko eno pot beleži. Poleg beleženja poti, omogoča tudi beleženje različnih dogodkov na tej poti, dodajanje slik in opisov, ter izvoz poti v PDF poročilo.

Navigacija

PES lahko uporabnika vodi po v naprej določeni poti. Uporabniki si lahko pot medsebojno delijo, funkcionalnost pa je enostavno dostopna v uporabniškem vmesniku, spravljena pod tipko »NAV«.

Pretvorba koordinat

PES vsebuje tudi zelo priročen pretvornik med koordinatnimi sistemi. Uporabnik lahko hitro pretvori koordinate iz enega od najbolj razširjenih koordinatnih sistemov kot so DMS (Latitude/Longitude), UTM (Universal Traverse Mercator) in MGRS (Military Grid Reference System) v ostale. Poleg tega pa podpira tudi Polarni koordinatni sistem, kjer uporabnik z azimutom in razdaljo določa točko relativno na lastno pozicijo.

PES Strežnik

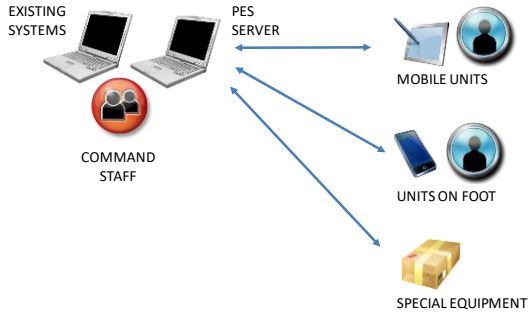
Skupna taktična slika

PES ne more skriti svojih vojaških korenin. Geografske informacije kot so POI[15] točke oziroma točke zanimanja, vojaške enote, oznake tarč, ki jih uporabnik doda na zemljevid, lahko PES deli s celotno skupino uporabnikov, ali pa jih pošlje le enemu točno določenemu preko SMS/MMS ali e – mail sporočila. Deljenju skupne taktične slike je namenjen PES strežnik (pes.milsistemika.com), funkcionalnost pa je na voljo v okviru gumba COP na uporabniškem vmesniku.

[15] angl. *Point of Interest*

PES Strežnik je lahko nameščen na prenosnem računalniku. To pomeni, da je celoten PES sistem (Strežnik in klienti) prenosljiv ter ga je moč v roku nekaj 10 minut postaviti kjerkoli kjer je na voljo mobilno 3G ali WiFi omrežje (glej Sliko 3.3).

Slika 3. 3: Shema PES sistema



Vir: Mil Sistemika (2016)

Poleg hranjenja in prikaza skupne taktične slike PES strežnik omogoča še:

- Uporabo PES – a in prikaz situacije preko spletnega vmesnika;
- hranjenje vseh podatkov, ki jih je strežnik prejel;
- upravljanje z bazo PES uporabnikov;
- delitev taktičnih podatkov na ločene operacije;
- delitev uporabnikov v taktične skupine;
- uporabo namenske sledilne opreme (GPS sledilcev) in
- povezavo z ostalimi informacijskimi sistemi (Mil Sistemika 2016).

3.4 Pravna podlaga obstoječe opreme policije

Pravna podlaga za sisteme, ki jih policija že uporablja in zajemajo ter obdelujejo podatke:

- Uporaba naprav za fotografiranja ter avdio in video snemanje, pri spremljanju javnih zbiranj pod pogoji iz 2. odstavka 114. člena Zakona o nalogah in pooblastilih policije;
- uporaba sistemov za video nadzor in fotografiranje pri izvajanju nalog nadzora državne meje pod pogoji iz Zakona o nadzoru državne meje in

- tajno opazovanje s pomočjo sistemov za ugotavljanje položaja in gibanja ter tehničnih naprav za prenos in snemanje glasu, fotografiranje in video snemanje, pod pogoji iz 1. odstavka 149.a člena Zakona o kazenskem postopku (ZKP, 149.a člen).

4 NADZOR NAD DELOM POLICIJE V RS

Nadzor nad policijo mora biti v prvi vrsti naloga policije same. V RS ima policija lasten notranji nadzor, seveda pa policijo nadzirajo tudi različne druge institucije ter celo državljani. V okviru Ministrstva za notranje zadeve opravlja nadzor nad policijo, na vseh področjih policijskega dela Direktorat za policijo in druge varnostne naloge. Nadzor nad delom policije je temeljnega pomena za uspešno in učinkovito uporabo policijskih pooblastil ter izvajanje policijskih nalog. Direktorat za policijo in druge varnostne vede izvaja redne, izredne in ponovne nadzore. Uvedba nadzora je naročena s strani ministra, ki jo odredi pisno. Ministrstvo za notranje zadeve ima izda načrtovani lenti program rednih nadzorov. Namen rednih nadzorov je celovita ocena zakonitosti in dejanskega stanja na posameznem področju policijske dejavnosti ter ocena varstva človekovih pravic. Izredni nadzori se izvajajo v primerih ocene zakonitosti in varstva človekovih pravic, kadar jih z načrtovanjem rednih in ponovnih nadzorov ni mogoče predvideti v naprej. Ponovni nadzori pa so namenjeni preverjanju odprave nepravilnosti, ki so bile ugotovljene na rednih oz. izrednih nadzorih (MNZ 2016).

V demokratičnih državah se nadzor nad policijo in izvajanjem dela pojavlja v različnih oblikah, in sicer:

- Politični oz. parlamentarni nadzor,
- sodni nadzor, ki je izvajan s strani sodišč,
- državljanski nadzor, ki ga izvajajo državljani, mediji in drugi,
- nadzor državnega tožilca ter
- notranji nadzor, ki ga izvaja policija sama in MNZ (MNZ 2016).

V Sloveniji delimo nadzor nad delom policije na notranji in zunanji nadzor. Notranji nadzor zajema torej nadzor policije same in MNZ, zunanji pa se deli na parlamentarni nadzor, nadzor Ustavnega sodišča RS, nadzor vlade, sodni nadzor in nadzor državnega tožilstva, nadzor nevladnih organizacij, nadzor varuha človekovih pravic, nadzor javnosti in medijev, nadzor Evropskega sodišča za človekove pravice ter Evropskega odbora za mučenje (Čas 2012, 134).

4.1 Zunanji nadzor

4.1.1 Parlamentarni nadzor in nadzor vlade RS

Politični oz. parlamentarni nadzor je nadzor nad izvajanjem policijskega dela in policijskih pooblastil, ki je izvajan preko parlamenta oz. Državnega zbora RS. Državni zbor izvaja nadzor preko Vlade RS, saj mora Vlada poročati parlamentu o rezultatih dela, pod njeno okrilje pa sodi tudi MNZ in policija. Oblike parlamentarnega nadzora so sledeče:

- Nezaupnica vladi,
- interpelacija ministra za notranje zadeve,
- poslanska vprašanja, ki so postavljena ministru za notranje zadeve,
- spremljanje vlade preko delovnih teles državnega zbora ter
- posebne parlamentarne preiskovale skupine (Čas 2012, 135).

V vsaki parlamentarni demokratični državi, je nujen člen v zagotavljanju demokratične odgovornosti izvršilne oblasti parlament. V primeru nadzora nad delom policije je MNZ odgovorno državnemu zboru, ta pa na volitvah odgovarja ljudstvu. Nadzor nad policijo v demokratičnih državah mora biti zagotovljen s sredstvi, s katerimi policija odgovarja tako državnim organom, kot tudi javnosti (Amnesty International Slovenije 2004).

4.1.2 Nadzor ustavnega sodišča RS

Ustavno sodišče RS ime v pristojnosti odločanje o zakonitosti in ustavnosti pravnih aktov, med drugim pa odloča tudi o kršenju človekovih pravic in svoboščin. V 160. členu Ustave RS je zapisano, da ustavno sodišče odloča o pritožbi le, v primeru, da je bilo izčrpano pravno varstvo. Ustavno sodišče je najvišji organ ustavnega varstva človekovih pravic in svoboščin v RS, zato ima pomembno vlogo tudi pri pri nadzoru izvajanja policijskih pooblastil (Čas 2012, 135).

4.1.3 Sodni nadzor in nadzor državnega tožilca

Določen vpogled nad delom policije imata v RS tudi sodišče in državno tožilstvo, predvsem v (pred)kazenskem postopku. Državno tožilstvo ima možnost usmerjanja predkazenskega postopka ter ob prejemanju poročil policije o ukrepih in ugotovitvah iz predkazenskega postopka. Določeno obliko nadzora predstavlja tudi dolžnost sodišča, da preverja in izdaja odredbe za različne posege policije na nivoju človekovih pravic. Taka oblika nadzora je omejena zgolj na kazenski postopek, če pa gre za zadeve, ki ne rezultirajo v ovadbah ali zbranih dokazih pa je izrazito omejena ali pa sploh ne obstaja.

7. odstavek 148. člena ZKP določa, da ima vsak posameznik, ki je bil vpleten pri uporabi kateregakoli ukrepa policije pravico, da v treh dneh vloži pritožbo pri pristojnem državnem tožilcu. Vendar ti postopki niso pravno regulirani, saj državni tožilec nima roka za obravnavo teh pritožb, ni ustaljenega postopka za preverjanje in reševanje postopkov, ni postopkov in sankcij, v kolikor so ugotovljene nepravilnosti, statistični podatki niso nikjer zabeleženi ipd. O nadzoru tožilstva in sodišča govorimo tudi o pravnih postopkih, ki se lahko sprožijo proti policistom, ki naj bi ravnali protizakonito. Ko gre za uvedbo oz. izvedbo kazenskih postopkov, pa je moč naleteti na številne ovire, saj v tem primeru policija preiskuje samo sebe. Za ustrezen nadzor nad policijo je ključnega pomena nadzor sodišča in delna vpletenost tožilstva, za zakonito izvedbo predkazenskega/kazenskega postopka ter spoštovanje pravic obtoženca in drugih oseb. Celoten pravosodni sistem je tudi odgovoren za zagotavljanje odgovornosti policistov za kršitve (Žaberl 2006, 49; Čas 2012, 135 – 136).

4.1.4 Varuh človekovih pravic RS

V RS so se razvili nekateri demokratični mehanizmi, ki zagotavljajo odgovornost države in njenih uslužbencev, njihova glavna naloga pa je tako nadzor nad učinkovitostjo pravnih mehanizmov ter po drugi strani pa naj bi sami zagotavljali nadzor nad delovanjem državnih organov. Eden izmed takšnih mehanizmov je Varuh človekovih pravic RS, čigar naloga je reševanje pobud državljanov, po tem, ko so že izčrpali druga pravna sredstva ter za obravnavo vprašanj, ki so pomembna za z vidika človekovih pravic in pravne varnosti (Čas 2012, 136).

Varuh človekovih pravic RS je pravzaprav nadzornik oblasti, saj s svojim delom omejuje samovoljo poseganje oblasti v temeljne človekove pravice in svoboščine posameznika. Varuh lahko deluje v primeru kršitve človekovih pravic in svoboščin, ki so navedeni v ustavi ter tudi v primeru kršenja katerekoli posameznikove pravice s strani oblasti in njenih nosilcev. Varuh človekovih pravic je samostojen in neodvisen organ, svojo organiziranost in delo pa ureja skladno z zakonom in drugimi splošnimi akti (Varuh človekovih pravic 2016).

Varuh človekovih pravic ima v Sloveniji močno vlogo, saj je imenovan s strani državnega zbora in je ustavna kategorija. Sicer nima neposrednih pristojnosti in deluje neformalno, vendar je uvrščen med državne nadzore nad policijo in ima zaradi pravne podlage visoko stopnjo neodvisnosti) (Čas 2012, 136).

4.1.5 Nadzor nevladnih organizacij

V RS poteka nadzor nevladnih organizacij nad delom policije, te organizacije pa skrbijo za človekove pravice in temeljne svoboščine. V svetu se take organizacije povezujejo med seboj, pri čemer pridobivajo na ugledu in dobivajo vedno večji vpliv. Ena izmed takih nevladnih organizacij v RS je Amnesty International Slovenije[16], ki vsako leto poda poročilo v katerem obravnava kršenje osnovnih človekovih pravic. Ta poročila niso zavezujoča, vendar imajo vseeno veliko težo tako v strokovni, kot tudi v laični javnosti. Poleg AIS deluje v RS še Helsinški monitor, ki daje izjave o različnih dogodkih, pri katerih so kršene človekove pravice in temeljne svoboščine ljudi, v teh izjavah pa javnosti, državam oz. mednarodnim organizacijam pojasnjuje svoje mnenje, poglede in ugotovitve (Amnesty International Slovenije 2004; Čas 2012, 136 – 137).

4.1.6 Nadzor Evropskega sodišča za človekove pravice

V Evropi je za kršenje človekovih pravic in temeljnih svoboščin ter za odločanje o individualnih pritožbah o kršenju človekovih pravic pristojno Evropsko sodišče za človekove pravice. Zelo veliko je primerov kršenja človekovih pravic, ki se posredno ali neposredno nanašajo na policijske postopke. Vsak posameznik., ki je mnenja, da so mu bile kršene

[16] AIS

osnovne človekove pravice, ki so zapisane v evropskem kodeksu o človekovih pravicah in ki je že izčrpal vsa pravna sredstva v lastni državi, lahko poda pritožbo na Evropsko sodišče za človekove pravice, ki ima sedež v Strasbourgu. Ko gre za izvajanje policijskih pooblastil gre po navadi za kršenje pravice do življenja, do svobode in varnosti, poštenega sojenja, pravice do spoštovanja zasebnega in družinskega življenja ter pravice do prepovedi mučenja (Klemenčič, Kečanovič in Žaberl 2002, 28).

4.2 Notranji nadzor

Notranji nadzor lahko delimo na nadzor MNZ ter na notranji nadzor, ki ga izvaja policija sama. Notranji nadzor nad policisti izvajajo predvsem njihovi nadrejeni, v kolikor pa je izdan sklep o nadzoru s strani direktorja policijske uprave ali generalnega direktorja policije pa to delo opravljajo tudi delavci policijske uprave in generalne policijske uprave. Policija prav tako opravlja nadzor (splošni, ponovni, strokovni) nad delom organizacijskih enot policije. Policija zagotavlja notranjo disciplino z rednim izvajanjem in vodenjem notranjega nadzora, kršitve pa se obravnava v disciplinskih postopkih. Tudi policisti so dolžni sporočiti kršitve drugih policistov, predvsem s področja kršitve človekovih pravic. Za nadzor nad delom policije pa je odgovorno MNZ, ki ima vsa nadzorna in usmerjevalna pooblastila (Žaberl 2006, 51 – 52). Ta razmerja so zajeta v Zakonu o policiji ter v Pravilniku o usmerjanju in nadzoru policije (Ur. l. RS, št. 97/2004). V okvir ministrstva sodijo tudi pritožbe, ki jih proti policistom vložijo državljani (Čas 2012, 138).

5 PRAVICA DO ZASEBNOSTI

5.1 Pojem zasebnosti

Pojem zasebnost pomeni sposobnosti oz. možnosti posameznika ali skupine ljudi, da ločijo podatke o sebi od drugih in jih po potrebi selektivno prikazujejo. Kje je meja in vsebina kar se šteje, da gre za zasebnost, je prav tako odvisno od vsakega posameznika, njegove kulture in časa v katerem živi. Zasebnost je večkrat povezana z anonimnostjo, ki pa pomeni željo biti in ostati neznan (nepoznan) ali neopažen v javnem življenju. Posameznik sam pri sebi razčisti kaj je zasebno. V osnovi zasebnost pomeni intimen, svojstven, prirojen in občutljiv notranji svet. Stopnje, do katere se zasebnost razkriva se razlikujejo tako geografsko, časovno in kulturno, kot tudi individualno (Lampe 2004).

5.2 Ustava RS

V 35. členu Ustave RS je opredeljena pravica do zasebnosti in osebnostne pravice. Z Ustavo RS v členih od 34. do 38. so opredeljene tudi sledeče pravice:

- Varstvo osebnih podatkov;
- varstvo pisem in drugih medijev;
- svoboda izražanja govora, misli in javnega nastopanja;
- osebna varnost in dostojanstvo;
- nedotakljivost stanovanja ter
- nedotakljivost človekove zasebnosti ter telesne in duševne celovitosti.

Pravica do zasebnosti je elementarna človekova pravica – tako mednarodna kot ustavna pravica javnopravnega značaja ter osebnostna pravica civilnopravnega značaja, kot ena izmed nepogrešljivih elementov človekove eksistence, ki varuje človeka pred državno oblastjo, javnostjo in drugimi posamezniki, je pravica biti sam z minimumom posegov v odločitveno, duševno, prostorsko in informacijsko zasebnost (Železnikar 2011, 19 – 20).

5.3 Vrste zasebnosti

Zaradi problematike, ki jo obravnavamo v diplomski nalogi bomo v nadaljevanju predstavil tri vrste zasebnosti, in sicer informacijsko zasebnost, zasebnost v prostoru in komunikacijsko zasebnost.

5.3.1 Informacijska in komunikacijska zasebnost

Informacijska zasebnost se osredotoča na osebne podatke posameznika, hkrati pa vključuje tudi vse komunikacije posameznika. Ključno je zbiranje in upravljanje z osebnimi podatki in varovanje le – teh. Pomen varstva osebnih podatkov ni zgolj v varovanju podatkov, ampak gre tu tudi za varovanje posameznika, na katerega se ti podatki nanašajo (Kaučič in Grad 2003). Informacijska zasebnost posameznika je ogrožena že z zbiranjem in objavljanjem osebnih podatkov, brez vedenja posameznika, lahko pa tudi s prisluškovanjem in opazovanjem oz. s poskusom katerega izmed teh dejanj (Kovačič 2006).

Ljudje dandanes živijo vsak po svoje in različno pojmujejo informacijsko zasebnost. Prav tako zbiranje različnih vrst osebnih podatkov posega v polje zasebnosti in varnosti. Vsak posameznik različno varuje svojo zasebnost, kar pa v današnji dobi ni enostavno, sploh s prihodom raznih socialnih omrežij (npr. Facebook, Instagram ipd.), kjer pa je informacijska zasebnost lahko zelo hitro kršena. Varovanje osebnih podatkov je zlasti pomembno predvsem zaradi preprečevanja kraje identitete. Razkritje podatkov o finančnih transakcijah in poslovanju lahko privede do tega, da je posameznikovo življenje lahko resno ogroženo. Zakon o varstvu osebnih podatkov ureja načela, postopke, pravice in ukrepe s katerimi je mogoče preprečiti nezakonite in prekomerne posege v integriteto človekove osebnosti (Kaučič in Grad 2003).

Komunikacijska zasebnost v osnovi zagotavlja zasebnost vseh oblik sporazumevanja. Sem spada tudi zasebnost telefonskih pogovorov, pošte, vse oblike elektronskega komuniciranja, kot npr. prenosi vsebin iz spleta, elektronska pošta, dokumenti v digitalni obliki, socialna omrežja, v glavnem ves pretok informacij, ki jih ustvari elektronsko komunikacijsko sredstvo (Kaučič in Grad 2003).

Informacije so se v preteklosti prenašale zgolj ustno, skozi pogovore, z napredkom tehnike pa je informacije mogoče prenašati tudi elektronsko. Ravno tehnološki napredek je omogočil, da je posameznikova zasebnost in s tem tudi zasebna komunikacija postala predmet interesa drugih posameznikov ali javnosti. Prisluškovanje pogovorom za zaprtimi vrati je zamenjala tehnologija tehničnega prisluškovanja pogovorom v prostorih, kjer se nahaja posameznik in prisluškovanja s tehniko snemanja na daljavo (Lampe 2004).

5.3.2 Zasebnost v prostoru

Zasebnost v prostoru ščiti posameznika do te mere, da je lahko sam in se nanaša predvsem na omejevanje poseganja v zasebnost na delovnem mestu ali doma. Tako zasebnost je mogoče doseči z gradnjo ograj ali zidov, namestitvijo zatemnjenih stekel, postavitvijo predelnih sten itd. Prostorska zasebnost je ključna, pri varovanju posameznika na določenih javnih mestih kot so trgovski centri z oblačili, javna stranišča, polja zasebnosti v bolnišnicah, bankah ipd. (Kaučič in Grad 2003).

6 ZAKON O VARSTVU OSEBNIH PODATKOV

6.1 Splošna opredelitev

8. člen Zakona o varstvu osebnih podatkov[17] (ZVOP) pravi, da se osebni podatki lahko obdelujejo le, če osebne podatke in njihovo obdelavo določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev.

Namen obdelave osebnih podatkov mora biti določen z zakonom, v primeru obdelave na podlagi osebne privolitve posameznika pa mora biti predhodno pisno ali na drug način podano obvestilo, ki prikazuje namen obdelave osebnih podatkov (ZVOP, 8 člen).

6.2 Pravne podlage v javnem sektorju

Osebni podatki v javnem sektorju se lahko obdelujejo, če so osebni podatki in njihova obdelava določeni z zakonom. Z zakonom se lahko določi, da se določeni osebni podatki obdelujejo le z osebno (pisno) privolitvijo posameznika.

Nosilci javnih pooblastil lahko obdelujejo osebne podatke tudi na podlagi osebne privolitve posameznika brez podlage v zakonu, v primeru, da ne gre za izvrševanje nalog kot nosilcev javnih pooblastil. Zbirke osebnih podatkov, ki nastanejo na tej podlagi, morajo biti ločene od zbirk osebnih podatkov iz drugih virov.

V javnemu sektorju se lahko izjemoma obdelujejo osebni podatki, ki so nujni za izvrševanje zakonskih pristojnosti, obveznosti ali javnega sektorja, če se s to obdelavo ne posega v upravičen interes posameznika, na katerega se osebni podatki nanašajo (ZVOP, 9. člen).

[17] Zakon o varstvu osebnih podatkov (uradno prečiščeno besedilo) (ZVOP-1-UPB1) z dne 16.10.2007

6.3 Pravne podlage v zasebnem sektorju

Osebni podatki v zasebnem sektorju se lahko obdelujejo, če so osebni podatki in njihova obdelava določeni z zakonom ali če gre za obdelavo določenih osebnih podatkov, za katere je bila podana osebna privolitev posameznika.

V zasebnem sektorju se lahko obdelujejo osebni podatki posameznikov, ki so z zasebnim sektorjem sklenili pogodbo, v kolikor je obdelava osebnih podatkov primerna in potrebna za izvedbo pogajanj za sklenitev pogodbe oz. za njeno izpolnjevanje.

V zasebnem sektorju se lahko obdelujejo osebni podatki, če je to nujno zaradi uresničevanja interesov zasebnega sektorja, ki so v skladu z zakonom in ti interesi prevladujejo nad interesi posameznika, na katerega se osebni podatki nanašajo (ZVOP, 10. člen).

Zavarovanje osebnih podatkov

Zavarovanje osebnih podatkov vključuje tako organizacijske, kot tudi tehnične in logično – tehnične postopke ter ukrepe, s katerimi se osebni podatki varujejo. Z istimi ukrepi in postopki se prav tako preprečuje slučajno ali namerno (nepooblaščeno) uničevanje podatkov, sprememba ali izguba podatkov ter nepooblaščena obdelava teh podatkov:

- Z varovanjem prostorov, opreme in sistemske programske opreme, kar vključuje vhodno – izhodne enote;
- z varovanjem aplikativne programske opreme, ki služi za obdelavo osebnih podatkov;
- s preprečevanjem nepooblaščenih dostopov do osebnih podatkov pri prenosu, kar vključuje prenos po telekomunikacijskih sredstvih in omrežjih;
- z zagotavljanjem učinkovitega načina blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov ter
- z omogočanjem poznejšega ugotavljanja, kdaj so bili posamezni osebni podatki vnešeni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

Postopki in ukrepi za zavarovanje osebnih podatkov morajo biti ustrezni glede na tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo. Zaposleni,

funkcionarji in drugi posamezniki, ki opravljajo dela oz. naloge pri osebah, ki obdelujejo osebne podatke, so dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju njihovih nalog, del oz. funkcij. Tudi v primeru prenehanja funkcije, zaposlitve, opravljanja del ali nalog, so obvezani varovanja tajnosti osebnih podatkov (ZVOP, 24. člen).

7 PREDLOG UREDITVE UPORABE SPECIALNE OPERATIVNE TEHNIKE ZARADI NOVIH TEHNOLOGIJ V ODNOSU DO PRAVICE O ZASEBNOSTI

7.1 Za organe pregona

Zaradi dostopnosti novih tehnologij na trgu (brezpilotni letalniki, IMSI[18] lovilci ipd.), organi pregona težijo k uvajanju novih pooblastil. Ravno zaradi bliskovitega tehnološkega razvoja v zadnjih desetih letih se je zmanjšala učinkovitost organov pregona na strani osumljencev oz. preiskovancev (povečala se je uporaba šifriranih komunikacij, uporaba predplačniških SIM kartic v telefonih ipd.).

Izvrševanje policijskih pooblastil predstavlja posege v pravico do zasebnosti posameznika in pravico do varstva osebnih podatkov. Nekatera pooblastila pomenijo tudi posege v pravico do svobode združevanja, in s tem posegajo v pravico do osebnega izražanja. Posegi v človekove pravice in temeljne svoboščine pa so možni samo le v skladu z načelom sorazmernosti. Načelo sorazmernosti mora vsebovati tri pogoje, ko gre za omejitev z ustavo določenih pravic. Prvi pogoje je, da gre za nujen poseg, drugi pogoj se navezuje na primernost oz. učinkovitost posega za dosego želenega cilja, ki je dopusten z ustavo. Tretji pogoj pa se navezuje na načelo sorazmernosti v ožjem smislu, kar pomeni, da je potrebno pretehtati pomembnost s posegom prizadete pravice v primerjavi s pravico, ki jo želimo zavarovati. Potrebno je pravo sorazmerje med nujnostjo posega in težo poledic, ki bi bile s tem povzročene.

Organi pregona morajo torej sami pretehtati katero pooblastilo uporabiti in na kakšen način, da bi prišlo do pravega (so)razmerja med dvema različnima stranema, na primer med zagotavljanjem javne varnosti prebivalstva in človekovo pravico do zasebnosti. Če rezultat tehtanja na podlagi izkušenj ni jasen oz. ni mogoče priti do pravega razmerja, potem mora biti to razvidno iz gradiva oziroma obrazložitve določb zakaj je pridobivanje podatkov iz komunikacijske opreme nujno oz. zakaj je pridobivanje podatkov o posamičnem mobilnem telefonu ne zadošča več. Hkrati bi moralo biti razvidno kako je tak ukrep sorazmeren v ožjem

[18] angl. *International Mobile Subscriber Identity*

pomenu. Pri tem se poraja vprašanje o sorazmernosti posega v zasebnost uporabnikov, ki se nahajajo v danem trenutku na določeni lokaciji bazne postaje, zato, da se lahko ugotovi ali se je na določenem območju nahajal mobilni telefon, ki je predmet preiskave. V obrazložitvi bi moralo biti razvidno, zakaj je predlagani poseg nujen in ali bo tak poseg resnično učinkovit in primeren. V takih primerih je potrebno upoštevati, da pripadniki organiziranih kriminalnih združb zamenjajo več deset SIM kartic na teden oz. sprotno po vsaki komunikaciji. Prav tako se poslužujejo uporabe raznih komunikacijskih sredstev, ki so dostopna na spletu, kot recimo Skypa, Facebooka, Google Hangouts in drugih, podobnih komunikacijskih programov. V takih primerih je smiselno vprašanje o učinkovitosti takšnih policijskih pooblastil, saj bi v praksi najverjetneje pridobivali podatke o povsem nedolžnih osebah. Pred organi pregona je težka naloga, kako zagovarjati primernost kakršnegakoli posega v zasebnost. Policija si tudi želi uporabe visokotehnoloških sredstev za identifikacijo oseb, predmetov in vozil. Pri sredstvih za identifikacijo je poseg v zasebnost bistveno večji kot v primeru izvajanja klasičnih policijskih pooblastil (Informacijski pooblaščenec 2014).

7.1.1 Smernice na temo uvajanja oziroma spreminjanja novih pooblastil organov pregona

Nova pooblastila so potrebna v povezavi z novimi tehnologijami na področju specialne operativne tehnike, katerih uporaba bo predstavljala obsežne posege v pravico do zasebnosti ter ukrepi, ki pomenijo množično zbiranje osebnih podatkov. Spremembe pooblastil bodo potrebne ker bo prišlo do pomembnih učinkov na človekove pravice (dostopanje do osebnih podatkov, lokacijskih, prometnih ipd.). Namen smernic je, da opozorijo na pravilen metodološki pristop k uvajanju invazivnih tehnologij in s tem novih pooblastil, ki bi temeljile na pravočasni in celovitejši identifikaciji potreb, analizi nujnosti, primernosti in učinkovitosti ter sorazmernosti s posegi v zasebnost. Cilj je učinkovitost in zakonitost delovanja policije ter verodostojnost in uporabnost zbiranja podatkov v kazenskih postopkih. To bi pomenilo večjo preiskanost kaznivih dejanj. Uvedlo bi se ustrezno tehtanje med pregonom storilcev kaznivih dejanj in upoštevanjem njihovih temeljnih človekovih pravic. Pazili bi na pravice tistih oseb, ki bi se po naključju znašli v preiskavah (US Depratment of Homeland security 2010) .

Te smernice predstavljajo ukrepi, ki omogočajo množično zbiranje podatkov v povezavi z najmodernejšimi informacijsko – komunikacijskimi tehnologijami. Mednje sodijo že

uporabljana sredstva v policiji (IMSI lovilec) in sredstva, ki bodo prišla v operativno uporabo v prihodnjih letih (Informacijski pooblaščenec 2014).

7.1.2 Presoja vplivov na zasebnost

Presoja vplivov na zasebnost je orodje za identifikacijo, analizo in zmanjševanje tveganj glede nezakonitih ravnanj z osebnimi podatki oziroma prekomernimi posegi v pravico do zasebnosti vsakega posameznika.

Temeljna načela presoje vplivov na zasebnost so sledeča:

- Zakonitost (splošna pravila obdelave osebnih podatkov po ZVOP);
- poštenost in transparentnost;
- sorazmernost;
- točnost in ažurnost;
- rok hrambe;
- zavarovanje osebnih podatkov ter
- upoštevanje pravic posameznika (ZVOP).

7.1.3 Izvedba presoje vplivov na zasebnost

Ko gre za izvedbo presoje vplivov na zasebnost so ključni naslednji elementi:

- Ocena stanja na področju urejanja,
- analiza tveganj,
- upravljanje tveganj in
- test sorazmernosti (nujnost, primernost in učinkovitost, sorazmernost).

Ocena stanja na področju urejanja

Ko gre za oceno stanja na področju urejanja se porajata dve vprašanji:

- Zakaj je potrebno uvajati nova pooblastila oziroma spreminjati obstoječa? in

- katere probleme bi nova pooblastila pravzaprav rešila, kako bi nova tehnološka sredstva probleme reševala na ustreznejši način (npr. uvedba brezpilotnih letal v delo policije).

Ko gre za uvajanje novih tehnoloških sredstev je potrebno natančno opredeliti za kakšna sredstva gre, kaj taka sredstva omogočajo ter kakšne so značilnosti njihovega delovanja pri obdelavi osebnih podatkov. Navesti je potrebno tudi kakšne podatke o osebah bi tehnološko sredstvo zbiralo, za kakšen namen in koliko časa se bodo obdelovali.

Analiza tveganj

- Tveganja v povezavi z nujnostjo pooblastil (ali je novo tehnično sredstvo ali pooblastilo resnično nujno potrebno);
- ali je mogoče z drugimi (obstoječimi ali milejšimi sredstvi) doseči isti cilj? Če ne, s čim se to dokazuje (in ne samo domneva);
- tveganja v povezavi z izvajanjem pooblastil (tveganja povezana z zbiranjem podatkov), če na primer tehnična sredstva ne bodo učinkovita za dosego cilja;
- tveganja povezana z zavarovanjem zbranih podatkov (vprašanje pooblaščenega dostopa, zlorabe s strani pooblaščenih oseb, izguba, možnost ne odkritja zlorab);
- tveganja povezana z uporabo podatkov (verodostojnost podatkov) in
- tveganja povezana z uničenjem podatkov (predvideni roki hrambe).

Upravljanje tveganj – varovalke

Z varovalkami se poskrbi za minimizacijo posegov v človekove pravice in prepreči najhujše zlorabe ter zagotovi uporabnost zbranih podatkov. Seznam varovalk :

- Omejitve glede odobritve in uporabe;
- takojšnje zavrženje nepotrebnih podatkov;
- kratki, utemeljeni roki hrambe;
- ukrepi za zavarovanje pridobljenih podatkov;
- ukrepi za nadzor nad rabo pridobljenih podatkov;
- vodenje statistik ter redno letno poročanje o rabi ukrepa;
- notranji in zunanji nadzor;
- obveščanje posameznika, ki je bil tarča oz. slučajna tarča ukrepa in

- možnost tretjega obdelovalca, ki na zahtevo policije le tej posreduje podatke o posamezniku, da posameznika seznani z zahtevkom.

Test sorazmernosti

Po oceni stanja na področju urejanja analiz tveganj in upravljanju tveganj sledi test sorazmernosti.

- Test nujnosti – ali je uporaba določenega tehničnega sredstva ali pooblastila nujna za dosego cilja, ki ga dopušča ustava. Tukaj gre za konkretne podatke, dokazila, argumente, ki dokazujejo, da cilja ni mogoče doseči z nobenim drugim ukrepom oz. blažjim posegom v človekove pravice.
- Test primernosti in učinkovitosti – ali je z ukrepom dejansko mogoče doseči cilje. Vprašanje je ali so predlagani ukrepi primerni in učinkoviti za dosego cilja, ki je ustavno dopusten.
- Test sorazmernosti v ožjem smislu – ali je poseg v zasebnost sorazmeren v primerjavi s pravico, ki jo želimo s posegom zavarovati (Informacijski pooblaščenec 2014).

7.2 Zakon o spremembah in dopolnitvah zakona o kazenskem postopku

Odkrivanje in preiskovanje zahtevnih in hujših oblik kaznivih dejanj ter hiter tehnološki razvoj sta razloga, zaradi katerih morajo imeti pristojni organi za odkrivanje in pregon storilcev kaznivih dejanj na voljo učinkovite preiskovalne ukrepe. Pristojni organi v zadnjih letih zaznavajo, da gre v primeru organiziranih kriminalnih združb za dogovarjanje in izvrševanje kaznivih dejanj v ozkem in zaprtem krogu oseb, z natančno določenimi vlogami in visoko stopnjo previdnosti pri izvrševanju kriminalne dejavnosti. Svoje delovanje organizirajo tako, da posamezniki, ki izvršujejo kazniva dejanja, uporabljajo le njim medsebojno znane telefonske aparate in številke ter v kratkih časovnih presledkih ob osebnem stiku menjajo tako številke kot aparate. To pa pomeni, da organi pregona s klasičnimi metodami preiskovanja (148. člen ZKP) ne more pridobiti telefonskih številk, s katerimi se komunicira in hkrati tudi ne prestrezati teh komunikacij z uveljavljenimi PPU.

Ker je, kot rečeno razvoj novih tehnologij bliskovit, je potrebno organom pregona zagotoviti uporabo ustreznih tehničnih sredstev za ugotavljanje podatkov, ki omogočajo odkrivanjem,

preiskovanje in pregon storilcev kaznivih dejanj. Ko gre za prej omenjene telefonske številke je v Predlogu ZKP – M z dvema novima členoma, in sicer 150.a in 150.b ZKP predlagana pravna podlaga za odreditev in uporabo t.i. IMSI lovilca. Pri tem je potrebno upoštevati načelo sorazmernosti, ki temelji na podlagi testa sorazmernosti, ker gre za resen poseg v človekove pravice.

Ena izmed slabih posledic (pre)hitrega razvoja tehnologij na področju specialnih operativnih tehnik je tudi šifriranje podatkov, predvsem, ko gre za komunikacijo preko različnih elektronskih omrežij (npr. Skype, elektronska pošta ipd.). S tem je uporaba »klasičnega« PPU (150. člen ZKP) skoraj onemogočena. Zato je nujno potrebno policiji omogočiti prestrezanje komunikacije že pri samem viru, preden se podatki šifrirajo, če gre za izpolnitev zakonskih pogojev za odreditev ukrepa iz 150. člena ZKP (ožji nabor hujših in zapletenejših kaznivih dejanj s hujšo predpisano kaznijo, obstoj utemeljenih razlogov za sum, nemožnost pridobitve dokazov z drugimi – manj invazivnimi – ukrepi, odredba preiskovalnega sodnika) (Predlog ZKP – M).

8 ANALIZA KOMERCIALNO DOSTOPNIIH TEHNOLOGIJ IN VPLIV NA ZASEBNOST

V tem poglavju bom ovrednotil komercialno dostopne tehnologije in njihov vpliv na zasebnost ter kako te tehnologije posegajo v nekatere osnovne človekove pravice in svoboščine. Analizo bom izvedel primerjalno, kjer bom tehnologijo, ki je komercialno dostopna vsakemu posamezniku primerjali z trenutno veljavno zakonodajo na področju zasebnosti in človekovih pravic in ovrednotil pravno in zakonsko pokritost tega področja v RS. Za analizo sem izbral nove tehnologije s področja specialne operativne tehnike, ki sem jih opisal pod poglavjem 3.3 (natančneje pod točko 3. Novosti na področju tehnologije).

8.1 SDR

SDR prestreza pogovore in SMS sporočila v kateremkoli telekomunikacijskem omrežju, večinoma sicer v 2G omrežju, pri čemer je v prvi vrsti kršen ZVOP, kjer je v 9. in 10. členu opisano, da je mogoče osebne podatke obdelovati le z podano osebno privolitvijo posameznika. Ker lahko v telefonskem pogovoru oz. SMS sporočilu posameznik nehote izdaja svoje osebne podatke, gre za kršitev pravice do informacijske in komunikacijske zasebnosti ter drugih z ustavo varovanih pravic. Te pravice so opisane v Ustavi RS, in sicer so to splošna pravica do zasebnosti (35. člen), pravica do komunikacijske zasebnosti (37. člen), pravica do informacijske zasebnosti (38. člen) ter pravica do svobode izražanja (39. člen). V primeru SDR tehnologije so kršene vse zgoraj naštete pravice.

8.2 Zaznavanje elektromagnetnega podpisa

V primeru zaznavanja elektromagnetnega podpisa gre zgolj za zaznavanje tipa elektronske naprave, kar je možno izvajati na daljavo. V tem primeru ne gre za kršenje posameznikovih ustavnih pravic, kot tudi ne za kršenje osnovnih pravic in svoboščin. Tudi na področje zasebnosti naprave za zaznavanje elektromagnetnega podpisa ne posegajo.

8.3 »Bug« komponente

V primeru uporabe t.i. bug komponent, ki predstavljajo prestreznik kakršnega koli dela na računalniku (npr. vnašanje gesel, pisanje dokumentov, e – mail pošte, splošna uporaba tipkovnice ipd.) je ponovno kršen ZVOP (9. in 10. člen). Gre za miniaturizirane računalniške enote, ki po navadi niso večje od manjšega USB ključa. Z uporabo bug komponent so kršene tudi številne ustavne pravice. Tudi v tem primeru so kršene pravice do komunikacijske in informacijske zasebnosti (37. in 38. Člen Ustave RS), splošna pravica do zasebnosti (35. člen Ustave RS) in pravica do svobode izražanja, ki je opisana v 39. členu Ustave RS. Ker gre za napravo, ki jo je potrebno na računalnik tudi fizično vgraditi, običajno pa se računalnik nahaja pri osebi doma, gre tu za poseg v pravico do nedotakljivosti stanovanja, ki je opisana v 36. členu Ustave RS.

8.4 Radar za pregledovanje tal visoke ločljivosti

V primeru radarja za pregledovanje tal visoke ločljivosti gre za napravo, ki jo je mogoče namestiti na ultralahko letalo in omogoča pregledovanje tal iz oddaljenosti do 40 km, zaradi visoke ločljivosti pa omogoča natančnost tudi do enega metra. V tem primeru gre za kršenje ZVOP, 9. in 10. člen, saj osebni podatek pomeni tudi spolna usmerjenost, ki je lahko s snemanjem razkrita. Prav tako je lahko kršena osnovna človekova pravica do svobode gibanja (32. člen Ustave RS) in splošna pravica do zasebnosti (35. Člen Ustave RS). Ker ja radar primeren za sledenje plovil, vozil ipd., je v primeru njegove uporabe kršena pravica do zbiranja in združevanja (42. člen Ustave RS), saj ima vsak pravico da se svobodno združuje z drugimi.

8.5 Termalne in nočne kamere

Termalne in nočne kamere so naprave, ki zaznavajo toploto npr. človeškega telesa oz. omogočajo vid ponoči. Tehnologija na tem področju je zelo napredovala, saj so omenjene naprave vse manjše, njihova ločljivost pa je vse višja. Podobno kot v primeru radarja za

pregledovanje tal visoke ločljivosti je tudi tukaj kršen ZVOP (9. in 10. člen). Na področju kršenja ustavnih človekovih pravic gre za kršenje splošne pravice o zasebnosti (35. člen Ustave RS), pravice do komunikacijske in informacijske zasebnosti (37. in 38. člen), pravica do zbiranja in združevanja (42. člen Ustave RS).

8.6 RFID

RFID uporablja elektromagnetno polje, da samodejno prepoznava in spremlja oznako, ki je na tarči. Oznaka vsebuje elektronsko shranjene podatke. Ker je potrebno oznako fizično namestiti na tarčo, ki je lahko denar, obleka, lastnina ali pa jo je mogoče vsaditi v živali ali ljudi, se porajajo resna vprašanja glede kršitve osnovnih človekovih pravic in svoboščin ter zasebnosti. V RS gre za kršenje ZVOP, ponovno 9. in 10 člena, saj ima naprava možnost prejemanja in branja osebnih podatkov. V primeru zasebnosti gre za kršenje pravice zasebnosti v prostoru (problematika namestitve oznak). Glede kršenja ustavnih pravic pa so tu kršene splošna pravica do zasebnosti (35. člen Ustave RS ter pravica do osebnega dostojanstva in varnosti (34. člen Ustave RS).

8.7 Radar, ki penetrira skozi zid

Radar, ki penetrira skozi zid predstavlja učinkovito sredstvo za nadzor oseb doma oz. v zaprtih prostorih. Na tem področju se tehnologija hitro razvija, saj je sedaj mogoče zaznati celo dihanje skozi nekaj 10 cm debel zid. Tehnologija ima sicer še slabšo ločljivost, vendar lahko zaznava obliko prostora ter omogoča informacije o obliki in materialu tarče, ki je v njem, hkrati pa lahko zaznava gibanje v prostoru in oddaljenost tarče od radarja. V tem primeru gre zgolj za kršitev zasebnosti v prostoru, prav tako pa je kršena pravica do splošne zasebnosti (35. člen Ustave RS).

8.8 »Data minig«

Data mining pravzaprav pomeni zbiranje večjih količin podatkov, ki so na voljo predvsem na družabnih omrežjih. Z združevanjem podatkov je mogoče nato dostopati do točno določenih,

tudi osebnih podatkov. Zaradi tega je kršen ZVOP, 9. in 10. člen. Tehnologija omogoča globoko kršitev informacijske in komunikacijske zasebnosti. Glede ustavnih pravic pa je kršen 35. člen ustave RS, ki zagotavlja splošno pravico do zasebnosti. Nadalje je lahko kršen 37. člen Ustave RS, ki zagotavlja komunikacijsko zasebnost ter 38. člen Ustave RS, ki varuje informacijsko zasebnost. Ravno tako posega na področje 39. člena Ustave RS, ki zagotavlja pravico do svobodnega izražanja v kontekstu, da nekdo izraža svoje mnenje na socialnih omrežjih in tehnologija omogoča pregled in vodenje zbirke o uporabniku, ki je tarča nadzora.

8.9 Brezpilotni letalnik

Ko gre za uporabo brezpilotnih letalnikov, ki so sestavljeni iz različnih podsistemov (sam letalnik ter sistema za delovanje, upravljanje in opravljanje nalog), lahko vpliv na zasebnost posameznikov razdelimo glede na sam podsistem. Ko govorimo o letalniku kot nosilcu sistemov za delovanje in upravljanje ter za opravljene nalog, sam letalnik ni sporen z vidika poseganja v človekove pravice in njegovo zasebnost. Ko pa govorim o tehnologijah, ki jih lahko brezpilotni letalnik nosi na sebi pa le – te omogočajo poseg v temeljne človekove pravice in svoboščine. Tukaj predvsem govorimo o posegu v pravico do splošne zasebnosti (35. člen Ustave RS), pravico do informacijske zasebnosti (38. člen Ustave RS) in pravice do komunikacijske zasebnosti, ki je opisana v 37. členu Ustave RS. Prav tako je tu kršena pravica do združevanja in zbiranja – 42. člen Ustave RS in pravica do svobode izražanja (39. člen Ustave RS).

Pri pregledu veljavne zakonodaje na področju specialne operativne tehnike, smo ugotovili, da je področje specialne operativne tehnike sicer zakonsko že predpisano, vendar to ne velja za novejše oblike tehnologij na tem področju. Tu se zato poraja vprašanje, ali se sme novejše naprave uporabljati z namenom nadzora in pridobivanja dokazov v boju proti kaznivim dejanjem, saj so lahko najnovejše tehnologije skupek že obstoječih naprav (npr. radar, ki penetrira skozi zid, ki bo morda v prihodnosti združen z napravo za video in audio nadzor). S tem namenom bo potrebno zakonodajo hitreje posodabljati, saj trenutno veljavna zakonodaja ne dohaja napredka v tehnologiji. Predvsem pa bo potrebno tej tehnologiji slediti in jo v zakonih natančno opredeliti.

9 SKLEP

Kriminalna dejanja različnih razsežnosti je velikokrat težko dokazati, predvsem zaradi tehnologije, ki jo uporabljajo tudi izvajalci kriminalnih dejanj. Dandanes je tehnologija na voljo vsakomur, ki si jo lahko privošči, zato je odkrivanje in predvsem dokazovanje kaznivih dejanj še toliko težje. Največji problem predstavlja ravno napredek in uporaba najnovejše tehnologije, ki pa ni dostopna le državnim agencijam, policiji, obveščevalnim službam ipd., temveč slehernemu posamezniku, ki jo zna uporabljati. V Mehiki denimo mamilarski karteli z droni nadzorujejo mejo z ZDA, trenutno pa še ni ničesar kar lahko ameriška vlada stori, da bi se uporaba teh naprav preprečila (Balido 2016). Zaradi uporabe omenjene tehnologije je velikokrat poseženo v osnovno človekovo pravico, pravico do zasebnosti, saj uporabniki tehnologije za nadzor, torej zasebniki, podjetja, posamezniki, posegajo v življenjski prostor drugih »na skrivaj« in seveda nezakonito. Nadzora nad uporabo tehnologije s strani zasebnih uporabnikov je trenutno še nemogoč oz. ga je mogoče kazensko preganjati šele, ko se uporaba odkrije in dokaže s strani policije.

Prihodnost vsekakor prinaša negotovost. Trendi razvoja tehnologije nakazujejo, da je nadzor nad uporabo le – te težko izvedljiv, saj se trg hitro širi in seveda tudi ponudba, saj je povpraševanja zelo veliko. Zaradi nenehnega razvoja in napredka je nadzor praktično nemogoče izvesti, saj kot rečeno tehnologija tako hitro napreduje, da preden oblasti lahko karkoli storijo, je že nova na tržišču. Nadzor nad uporabo take tehnologije bi morali mednarodno uzakoniti, vendar bo za to potreben še čas. Omenjena tehnologija že omogoča, da lahko vsakdo spremlja vsakogar, zbira informacije in s tem vdira v zasebnost posameznika. Podatki, ki so na ta način zbrani so lahko občutljive poslovne informacije in tajnosti, v primeru, da gre za trgovsko oziroma ekonomsko dejavnost, v kolikor pa to spremljanje ni odkrito in dokazano pa ni mogoče storiti skoraj nič.

Ko gre za PPU je seveda zgodba drugačna, saj je uporaba takih ukrepov zakonsko regulirana, dovoljenje za uporabo pa mora policija v veliki večini primerov pridobiti s strani preiskovalnega sodnika oziroma pristojnega tožilca. Policija je podvržena tudi različnim stopnjam nadzora, tako notranjega, sodnega in nadzora s strani varuha človekovih pravic in hkrati parlamentarnega nadzora, prav tako pa lahko nadzor vršijo tudi državljani sami, seveda s pomočjo ustreznih mehanizmov.

V diplomskem delu smo si zastavili sledečo hipotezo:

Tehnološki razvoj na področju specialne operativne tehnike bo otežil nadzor nad uporabo tehničnih sredstev za zbiranje, prenos in obdelavo osebnih podatkov.

Z analizo, ki smo jo v diplomskem delu opravili z naslova novih tehnologij na področju specialne operativne tehnike, ki so komercialno dostopna vsakomur, smo samo še podkrepili trditev iz postavljene hipoteze, da je novejše naprave, ki so majhne, mobilne in prikrite izrazito težko nadzorovati. Hipotezo lahko glede na zapisno potrdimo. Tehnološki razvoj ne otežuje le nadzora nad uporabo tehnologije v zasebni sferi, temveč tudi v primeru uporabe tehnoloških sredstev s strani policije. Velikokrat imajo policisti izredno težko nalogo, saj je potrebne dokaze za storjeno kriminalno dejanje težko pridobiti brez uporabe PPU.

10 LITERATURA

1. Amnesty International Slovenije. 2004. *Nadzor nad policijo in reševanje pritožb zoper njeno delo.* Ljubljana: Državljanski nadzor nad policijo – priporočila za Slovenijo.
2. Balido, Nelson. 2016. *Mexican cartels patrol border with drones – and U.S. has no response*. Fox News Latino. Dostopno prek: http://latino.foxnews.com/latino/opinion/2016/02/19/nelson-balido-mexican-cartels-patrol-border-with-drones-and-us-has-no-response/ (25. februar 2016).
3. BCB International. 2015. *UAV SQ-4.* Dostopno prek: http://uas.wales/sq-4/#features (28. februar 2015).
4. Chen, Hscinchun in drugi. 2004. *Crime data minig: a general framework and some examples.* Dostopno prek: http://hub.hku.hk/bitstream/10722/45461/1/91939.pdf?accept=1 (23. Avgust 2016).
5. Čas, Tomaž. 2012. *Policijsko pravo – izbrane vsebine za študente Evropske pravne fakultete.* Ljubljana: Evropska pravna fakulteta.
6. Dežman, Zlatan, in Anže Erbežnik. 2003. *Kazensko procesno pravo Republike Slovenije*. Ljubljana: GV založba.
7. Dobovšek, Bojan. 2009. *Transnacionalna kriminaliteta*. Ljubljana: Fakulteta za varnostne vede.
8. Engin, Erman, Berkehan Çiftçioğlu, Meriç Özcan in İbrahim Tekin. 2007. *High resolution ultrawideband wall penetrating radar*. Istanbul: Faculty for engineering and natural science, Sabancy university.
9. *Flir*. Dostopno prek: http://www.flir.com/home/ (22. Avgust 2016).
10. Gadget Review. 2015. *Spy Surveillance Equipment Reviews for 2015.* Dostopno prek: http://www.gadgetreview.com/reviews/spy-equipment-reviews (26. oktober 2015).
11. Informacijski pooblaščenec. 2014. *Presoje vplivov na zasebnost pri uvajanju novih policijskih pooblastil, smernice informacijskega pooblaščenca*. Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost_pri_uvajanju_novih_policijskih_pooblastil_Smernice_IP.pdf (03. marec 2015).

12. - - - 2015. *Uporaba brezpilotnih letalnikov pri opravljanju policijskih nalog, št. 0712-1/2015/435*. Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf /porocila/Brezpilotni_letalniki_-_porocilo_IP.pdf (5. marec 2015).
13. Kaučič, Igor in Franc Grad. 2003. *Ustavna ureditev Slovenije*. Ljubljana: GV založba.
14. *Kazenski zakonik* (uradno prečiščeno besedilo) (KZ-1-UPB2). Ur. L. RS 50/2012. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?url urid=20082296 (29. februar 2016).
15. Klemenčič, Goran, Bećir Kečanović in Miroslav Žaberl. 2002. *Vaše pravice v policijskih postopkih.* Ljubljana: Založba Pasadena.
16. Kovačič, Matej. 2006. *Nadzor in zasebnost v informacijski družbi.* Ljubljana: Fakulteta za družbene vede.
17. Lampe, Rok. 2004. *Sistem pravice do zasebnosti*. Ljubljana: Bonex založba.
18. Microdrones. 2015. *Microdrones at a glance.* Dostopno prek: http://www.microdrones.com/en/prod ucts/md4-200/at-a-glance/ (28. februar 2015).
19. Mil Sistemika. 2016. PES (Personal Eye System). Dostopno prek: http://pes.milsistemika.com/ (20. april 2016).
20. Ministrstvo za notranje zadeve. *Usmeritve policiji in nadzor nad njenim delom.* Dostopno prek: http://www.mnz.gov.si/si/varnost_in_nadzor/usmeritve_policiji_ in_nadzor_nad_njenim_delom/ (30. maj 2016).
21. Mozetič, Polona. 2007. Utemeljeni razlogi za sum. *Revija za kriminalistiko in kriminologijo* 58(2): 146 – 159.
22. Neuro technology. 2015. *Face identification and movement detection, Verilook Surveillance SDK.* Dostopno prek: http://www.neurotechnolo gy.com/verilook-surveillance.html (28. februar 2015).
23. Nacionalni Sistem Integritete. 2016. *Organi pregona – policija, tožilstvo*. Dostopno prek: http://nis.integriteta.si/organi-pregona (20. april .2016).
24. Podgoršek, Borut. 2008. *Brezpilotni letalniki.* Dostopno prek: http://sierra5.net/index.php?option=com_content&task=view&id=591 (27. junij 2016).
25. Pipan, Boštjan. 2009. *Uporaba specialne tehnike pri odkrivanju organiziranega kriminala*. Maribor: Fakulteta za varnostne vede.
26. *Predlog zakona o spremembah in dopolnitvah zakona o kazenskem postopku (Predlog ZKP-M).* Redni postopek EVA 2013-2030-0106. Dostopno prek:

http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/mp.gov.si/PDF/zakonodaja/131206_ZKP-M_6.12.13.pdf (29. avgust 2015).

27. *Rtl-sdr*. 2016. Dostopno prek: http://www.rtl-sdr.com/ (22. avgust 2016).
28. Svete, Uroš, Janja Vuga Beršak, Anica Ferlin, Tadej Hlavaček, Jure Mišigoj, Žiga Polajnar in Sebastijan Zajc. 2015. Brezpilotni letalniki: od varnostnih nalog do komercialne rabe – kako urediti njihovo uporabo? *Ujma* 29: 350-356.
29. *Synology*. 2015. Dostopno prek: https://www.synology.com/en-us/surveillance/7.0/overview (28. februar 2015).
30. *Technovelgy*. 2016. Dostopno prek: http://www.technovelgy.com/ct/technology-article.asp (23. avgust 2016).
31. *Uredba o oborožitvi, vojaški opremi, specialni operativni tehniki in naročilih zaupne narave* Ur. L. RS 76/2001. Dostopno prek: http://www.pisrs.si /Pis.web/pregledPredpisa?id=URED1843# (28. september 2015).
32. US Department of Homeland Security. 2010. *Privacy Impact Assassements.* Dostopno prek: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_gu_idance_june2010.pdf (3. marec 2015).
33. *Varuh človekovih pravic*. 2016. Dostopno prek: http://www.varuh-rs.si/o-instituciji/o-instituciji-varuha-clovekovih-pravic-rs/ (30. avgust 2016).
34. *Zakon o elektronskih komunikacijah* (uradno prečiščeno besedilo) (ZEKom-1). Ur. L. RS 109/2012. Dostopno prek: https://www.uradni-list.si/1/content?id=111442 (26. oktober .2015).
35. *Zakon o elektronskem poslovanju in elektronskem podpisu* (uradno prečiščeno besedilo) (ZEPEP-UPB1). Ur. L. RS 98/2004 Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=200498&stevilka=4284 (26. oktober 2015).
36. *Zakon o elektronskem poslovanju na trgu* (ZEPT). Ur. L. RS 61/2006. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=200661&stevilka=2566b (26. oktober 2015)
37. *Zakon o kazenskem postopku* (uradno prečiščeno besedilo) (ZKP). Ur. L. RS 32/2012. Dostopno prek: https://www.uradni-list.si/1/content?id=108445 (26. oktober 2015).
38. *Zakon o spremembah in dopolnitvi Zakona o kazenskem postopku* (uradno prečiščeno besedilo) (ZKP-M). Ur. L. RS 87/2014. Dostopno prek: https://www.uradni-list.si/1/content?id=119567 (20. april 2016).

39. *Zakon o varstvu osebnih podatkov* (uradno prečiščeno besedilo) (ZVOP-1-UPB1). Ur. L. RS 94/2007. Dostopno prek: https://www.uradni-list.si/1/content?id=82668 (26. oktober 2015).
40. Zaugg, Evan C., Derek L. Hudson in David G. Long. 2006. *The BYU μSAR: A Small, Student-Built SAR for UAV Operation*. Dostopno prek: https://pdfs.semanticscholar.org/072b/d2b0f49fecec021bacb84614dd76402ea496.pdf (23. avgust 2016).
41. Žaberl, Miroslav. 2006. *Temelji policijskih pooblastil*. Ljubljana: Fakulteta za varnostne vede.
42. Železnikar, Tomaž. 2011. *Pravica do zasebnosti in uporaba mobilne telefonije*. Ljubljana: Fakulteta za družbene vede.