Uvodnik

Spoštovane bralke in bralci, pred vami je druga številka revije v slovenskem jeziku v tem letu. Prinaša pet člankov, poročila s štirih okroglih miz in poročilo o ekskurziji magistrskih študentov Fakultete za varnostne vede v Sarajevo.

Avtorji Iztok Rakar, Ester Debeljak in Bojan Tičar predstavljajo inšpekcijski nadzor in ugotavljajo njegov prispevek k varnosti v občinah. Ugotavljajo, da je slednji odvisen od tega, ali so situacije, ki predstavljajo varnostno tveganje, ustrezno zajete in urejene s predpisi in če je inšpekcijski nadzor učinkovit, pri čemer seveda ne gre brez problemov. Andreja Rožnik in Gorazd Meško odgrinjata tančico iz, vsaj v Sloveniji, malo poznane in raziskane tematike, to je električnih in elektronskih odpadkov. Ti predstavljajo večplasten problem tako zaradi svoje toksičnosti kot tudi zaradi neustreznega recikliranja v želji po pridobivanju dragocenih kovin. Anže Zaletel, Jaka Žužek, Lavra Horvat, Katja Zupan, Sara Železnik, Nina Goršič in Maruša Lipušček v prispevku opisujejo projekt varnostnega testiranja v razvoju in produkciji fizičnega kripto-modula, ki je nujno potrebno pred lansiranjem izdelka na trg. Rezultat ni samo izdelek Code 1 Secure, ampak tudi detajlni zapis celotnega postopka, vključno z določenimi ugotovitvami. Da dandanes na človeka pretijo nevarnosti tako iz socialnega, naravnega in virtualnega okolja, nas opozarja tudi Mateja Bitenc, ko nam v svojem prispevku razlaga viktimološki pogled na naložbene prevare. Posebej je zanimiva njena ugotovitev, da žrtve takšnih prevar ne utrpijo samo materialne, ampak tudi čustvene, psihološke in zdravstvene posledice. Zadnji prispevek, ki sta ga pripravila Jaroš Britovšek in Aleš Čretnik, pa argumentirano predstavlja kar tri možne modele reorganizacije obveščevalno-varnostnega sistema, s katerim v Sloveniji nihče ni prav posebej zadovoljen, a po navadi bistveno dalje od destruktivnega kritikantstva ne zmoremo. Avtorjema gre vsekakor priznati pogum, da sta se lotila tako zahtevne naloge.

V uredništvu smo se odločili, da v tokratno številko uvrstimo podrobne zapise kar štirih okroglih miz, ki so potekale na letošnjih Dnevih varstvoslovja v Kranjski Gori. Kompetentni razpravljavci in moderatorji ter konstruktivne razprave so porok, da se lahko odločevalci (oblikovalci politik) naslonijo tudi na ugotovitve okroglih miz. Prispevke so pripravili Saša Kuhar (varnost na javnih prireditvah), Kaja Prislan in Sara Kandolf (vodenje v policiji), Miha Dvojmoč (regulativa v panogi detektivske dejavnosti) in Aleš Godec (t. i. mariborske vstaje). Za zaključek je Kristina Pavli pripravila še zapis o strokovni ekskurziji magistrskih študentov Fakultete za varnostne vede na različnih institucijah kazenskega pravosodja v Sarajevu – mestu, ki si že samo po sebi zasluži zanimanje varstvoslovcev.

Spoštovano bralstvo, če sem v zadnjih nekaj uvodnikih zapisal nekaj sočnih o evropski in slovenski varnostni stvarnosti, pa naj tokrat uvodnik končam popolnoma drugače, optimistično. In od kod izvira ta moj optimizem? Sredi septembra se je »zgodil« (upam, da zgolj »prvi«) Dan nacionalne varnosti. Tisto, kar me pri njem navdušuje, ni zgolj dejstvo, da so pri njem družno sodelovale vse ključne službe nacionalnovarnostnega sistema, kot so vojska, policija, zaščita in reševanje, pravosodna policija, mestno redarstvo, zasebno varstvo, ampak tudi visokošolske in srednješolske ustanove ter številne nevladne organizacije,

ki delujejo na področju varnosti. In tisto, kar je še posebej pomembno – Dan nacionalne varnosti je bil organiziran na pobudo in ob velikem angažmaju prav ene izmed njih, to je Inštituta za varnostno kulturo, kateremu so vsi omenjeni subjekti prisluhnili in pobudo podprli. Prav bi bilo, da takšne iniciative in dogodke podpiramo tudi v bodoče. To je veliko, a hkrati najmanj, kar lahko storimo za varnost v naši družbi!

Izr. prof. dr. Andrej Sotlar
Glavni in odgovorni urednik

VARSTVOSLOVJE,
letn. 18
št. 3
str. 251–269

Inšpekcijski nadzor na državni in lokalni ravni ter njegov prispevek k varnosti v občinah

Iztok Rakar, Ester Doljak, Bojan Tičar

Namen prispevka:

Namen prispevka je prikaz pravne ureditve inšpekcijskega nadzora na državni in lokalni ravni in umestitev inšpekcijskega nadzora v proces modernizacije in razvoja slovenske javne uprave. Prispevek je namenjen tudi razumevanju pravnega položaja inšpektorjev in strank ter inšpekcijskih postopkov z vidika državne in občinske regulative ter z vidika prispevka k varnosti v občinah.

Metode:

Raziskovalni pristop je kombinacija pravnih metod deskriptivne, primerjalne (komparativne) jezikovne in teleološke razlage s študijami šestih primerov ureditve v treh večjih in treh manjših oz. srednje velikih občinah. S teleološko razlago avtorji prikažejo *ratio legis* zakonodajalca v zakonski ureditvi pravnega položaja inšpektorjev, njihovih pooblastil ter pravnega položaja strank v teh postopkih.

Ugotovitve:

Inšpekcijski nadzor prispeva k večji varnosti v občinah, če so s predpisi ustrezno zajete in urejene situacije, ki predstavljajo varnostno tveganje, in če je učinkovit. Učinkovitost inšpekcijskega nadzora se praviloma obravnava parcialno, in sicer kvantitativno, kar ni skladno s kompleksnostjo upravnega, političnega in družbenega sistema. Učinkovitost inšpekcijskega nadzora in večja varnost v občinah torej nista odvisna samo od inšpekcij, ampak tudi od številnih drugih dejavnikov. Dosedanji razvoj na tem področju v Sloveniji kaže na težavnost uvajanja sistemskih sprememb na državni ravni, zlasti na organizacijskem področju, na občinski ravni pa na uspešnost v obliki ustanavljanja medobčinskih inšpektoratov in redarstev.

Izvirnost/pomembnost prispevka:

Članek bralcu predstavi veljavno pravno ureditev inšpekcijskega nadzora v Republiki Sloveniji in njegovo umestitev v kontekst modernizacije in reforme slovenske javne uprave. Izpostavlja dobre in slabe strani dosedanjega razvoja in predlaga rešitve. Na primeru izbranih občinskih aktov in sodne prakse prikaže prispevek inšpekcijskega nadzora k varnosti v občinah.

UDK: 35.078.3

Ključne besede: inšpekcija, inšpekcijski postopek, inšpektorat, upravni postopek, lokalna samouprava, medobčinsko sodelovanje

Inspection at State and Municipal Level and the Contribution Thereof to Security in Municipalities

Purpose:

The article aims to provide an overview of the statutory regulation of inspection at the national and local levels and its placement in the process of modernization of Slovenian public administration. The article is intended to deepen the understanding of the legal position of inspectors and parties to inspection procedures, as well as the inspection procedure itself from the perspective of national and local regulations and the legal regulation of certain security aspects in local communities.

Design/Methods/Approach:

The applied research approach is a combination of the legal methods of descriptive, comparative linguistic, and teleological interpretations, combined with an analysis of six cases involving the application of the relevant regulation in three larger and three smaller or medium sized municipalities. By means of teleological interpretation, the authors demonstrate the *ratio legis* of the legislature in the statutory regulation of the state and local legal positions of inspectors, their powers, and the legal position of parties to these procedures.

Findings:

Inspections contributes to security in municipalities, if situations that pose a security risk are regulated properly and if it is effective. The effectiveness of inspections is normally considered partially, especially quantitative, which is not consistent with the complexity of administrative, political and social system. The effectiveness of inspection and higher security in municipalities therefore depend not only on inspections, but also on many other factors. The current development in this field in Slovenia shows the difficulties of introducing systemic changes at the national level, especially in the field of organization, and success at the municipal level in the form of the establishment of inter-municipal inspectorates and local police.

Originality/Value:

The article is a summary presentation that provides readers with an overview of the legal regulation of the institute of inspection in the Republic of Slovenia and its placement in the context of modernization and reform of Slovenian public administration. It highlights the strengths and weaknesses of current development and proposes solutions. By using selected municipal acts and the case law it presents the contribution of inspections to the security in the municipalities.

UDC: 35.078.3

Keywords: inspection, inspection procedure, inspectorate, administrative procedure, local self-government, inter-municipal cooperation

1 UVOD

Inšpekcijski nadzor je oblika upravnega nadzora, v okviru katerega državni in občinski organi nadzorujejo, kako posamezniki, organizacije in skupnosti spoštujejo predpise (pasivnost – izogibanje dejanjem, ki bi pomenila kršitev) oziroma izvršujejo predpise (aktivnost – izvajanje dolžnih ravnanj) (Eichhorn et al., 2003).

Pravno gledano je glavni element inšpekcijskega nadzora in primarni objekt varstva javni interes, izražen v zakonih, podzakonskih predpisih in drugih oblastnih splošnih pravnih aktih (Kovač, 2016a). Javni interes je zaščiten, če subjekti, ki jim predpisi nalagajo pravice in obveznosti, ravnajo v skladu s predpisanimi pravili. Zakonito stanje torej predstavlja zaščito javnega interesa. Namen inšpekcijskega nadzora je torej ta, da ugotavlja, ali subjekti nadzora – zavezanci – ravnajo v skladu s predpisi. Inšpekcijski nadzor se zato izvaja na vseh upravnih področjih, na katerih javni interes naslovnikom pravil narekuje ali prepoveduje oz. omejuje določeno ravnanje (Grafenauer in Brezovnik, 2006; Virant, 2009). Primarna odgovornost za zakonito delovanje kljub temu ostaja pri zavezancih – inšpekcijski nadzor predstavlja zgolj sekundarno odgovornost za stanje na določenem upravnem področju (Jerovšek in Kovač, 2008).

Z vidika upravne znanosti inšpekcijski nadzor zagotavlja povratne informacije in s tem začetek novega cikla oblikovanja oz. spreminjanja javnih politik. Je torej sestavni del oblikovanja in izvajanja oblasti ter hkrati pomembna družbena funkcija, preko katere se kaže družbena realnost in v njenem okviru razmerje med oblastjo in člani družbe (Kovač, 2016b).

Inšpekcijski nadzor je ena od temeljnih funkcij državne uprave in ena od izvirnih nalog samoupravnih lokalnih skupnosti, v okviru katere le-te nadzirajo izvajanje in spoštovanje predpisov, ki jih same izdajajo (Zakon o državni upravi [ZDU-1], 2002: 10. čl.; Zakon o lokalni samoupravi [ZLS], 1993: 21. čl.). Državna uprava in občinske uprave nadzirajo posameznike in njihove povezave (t. i. hierarhični nadzor) ter svoje lastno delovanje (t. i. horizontalni nadzor). V okvir slednjega sodita npr. proračunska in upravna inšpekcija (Tičar in Rakar, 2011).

Razvojno gledano je nadzora več, a se spreminja v svojih ključnih značilnostih. Če je v obdobju t. i. klasične Weberjanske javne uprave (19. stol.) prevladovalo zagotavljanje zakonitosti, nadrejenost nadzornikov in inkvizicijska metoda dela in v obdobju t. i. novega javnega menedžmenta (20. stol.) premik k predhodnemu opozarjanju, usmerjenost k nadzorovancem in partnerska metoda dela, potem za sedanje obdobje (t. i. dobro javno upravljanje in dobra uprava – angl. *good governance, good administration*) veljajo kombinacija represije in preventive, sorazmerje med pooblastili in ukrepi nadzornikov ter pravicami nadzorovanih in celovita metoda delovanja (Kovač, 2016b).

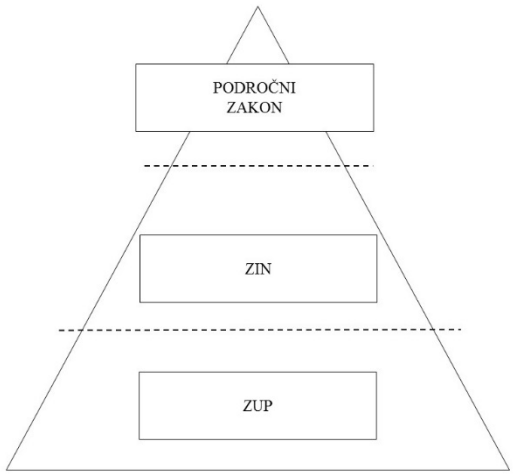
2 PRAVNA UREDITEV INŠPEKCIJSKEGA NADZORA V POZITIVNI ZAKONODAJI

2.1 Uvod

Pravo Evropske unije (EU) ne ureja (organiziranosti) inšpekcijskega nadzorstva, zato je primerjalno gledano to področje raznoliko, ob hkratnem obstoju nekaterih

podobnosti, ki so posledica pričakovanja učinkovitega izvajanja pravnega reda EU. Slovenska pravna ureditev inšpekcijskega nadzora je kompleksna. Ustava Republike Slovenije (URS, 1991) nima izrecnih določb, ki bi se nanašale na inšpekcijski nadzor, seveda pa predstavlja temelj in okvir zakonski ureditvi in delovanju inšpekcij. Inšpekcijski nadzor je urejen v Zakonu o državni upravi (ZDU-1, 2002), ki v 10. členu določa, da državna uprava opravlja inšpekcijski nadzor nad izvajanjem predpisov in da inšpekcijski nadzor ureja poseben zakon. Ta zakon, ki sistemsko ureja inšpekcijski nadzor, je Zakon o inšpekcijskem nadzoru (ZIN, 2002). ZIN vsebuje tri vrste določb, in sicer postopkovne, organizacijske in materialne (Pirnat et al., 2004). Postopkovna vprašanja urejajo še področni zakoni, zakoni, ki urejajo nekatere področne inšpekcije, in zakon, ki ureja splošni upravni postopek (Zakon o splošnem upravnem postopku [ZUP], 1999). Med temi zakoni je vzpostavljeno razmerje subsidiarnosti (za razvoj pravne ureditve gl. Kovač, 2016b).

Slika 1: Razmerje subsidiarnosti na področju zakonskega urejanja inšpekcijskega nadzora



ZIN (2002) velja za vsa upravna področja nadzora (npr. tržno, s področja notranjih zadev ipd.), za državni in občinski inšpekcijski nadzor (pri slednjem ne velja glede organiziranosti) in v celoti za vse t. i. zunanje inšpekcije in delno za vse t. i. notranje inšpekcije (npr. načela ter položaj, pravice in obveznosti inšpektorjev) (ZIN, 2002: 3. čl.). ZIN (2002) uporabljajo tudi nekatere regulatorne agencije, npr. Agencija RS za energijo (Energetski zakon [EZ-1], 2014: 422. čl.). Kot že rečeno, ZLS (1993: 20. čl.) med izvirnimi nalogami občin navaja tudi inšpekcijski nadzor nad izvajanjem občinskih predpisov in drugih aktov, s katerimi ureja zadeve iz svoje pristojnosti, če ni z zakonom drugače določeno.

Temeljni namen inšpekcijskega nadzora je zagotoviti spoštovanje predpisa, zato so upravni inšpekcijski postopki in njihovi ukrepi praviloma preventivne narave. Ker pa mora biti nadzor učinkovit, je zakonodajalec določena ravnanja in opustitve opredelil kot kazniva v najširšem smislu – kot prekrške. Inšpekcijski organi imajo zato tudi kaznovalno funkcijo v vlogi prekrškovnega organa in vodijo prekrškovne postopke. V skladu z Zakonom o prekrških (ZP-1, 2003) so namreč prekrškovni organi upravni in drugi državni organi ter nosilci javnih pooblastil, ki izvajajo nadzorstvo nad izvrševanjem zakonov in uredb, s katerimi so določeni

prekrški, in organi samoupravnih lokalnih skupnosti, ki so s posebnimi predpisi pooblaščeni za odločanje o prekrških (ZP-1, 2003: 45. čl.) (podr. v Kovač, 2016b).

V nadaljevanju na kratko predstavljamo izbrane vidike pravne ureditve inšpekcijskega nadzora, in sicer organiziranost in pravni položaj inšpektorjev, v okviru slednjega pa posebej načelo samostojnosti in načelo varstva javnega in zasebnih interesov.

2.2 Organiziranost inšpekcijskega nadzora

2.2.1 Državna raven

V okviru državne uprave se inšpekcijski nadzor praviloma organizira v inšpektoratih kot organih v sestavi ministrstev, ki jih vodijo glavni inšpektorji kot uradniki na položajih skladno z Zakonom o javnih uslužbencih (ZJU, 2002). Obstajajo pa tudi primeri, ko se organizira kot notranja organizacijska enota druge vrste organa v sestavi (npr. inšpekcija za varno hrano, veterinarstvo in varstvo rastlin v okviru Uprave RS za varno hrano, veterinarstvo in varstvo rastlin kot organa v sestavi Ministrstva za kmetijstvo, gozdarstvo in prehrano). Za medsebojno koordinacijo dela in doseganje večje učinkovitosti različnih inšpekcij je ustanovljen Inšpekcijski svet kot stalno medresorsko delovno telo, ki ga vodi minister, pristojen za upravo (Ministrstvo za javno upravo, 2016; ZIN, 2002; Zakon o veterinarstvu [ZVet-1], 2001). Inšpektorati, ki delujejo na državni ravni, so prikazani v tabeli 1.

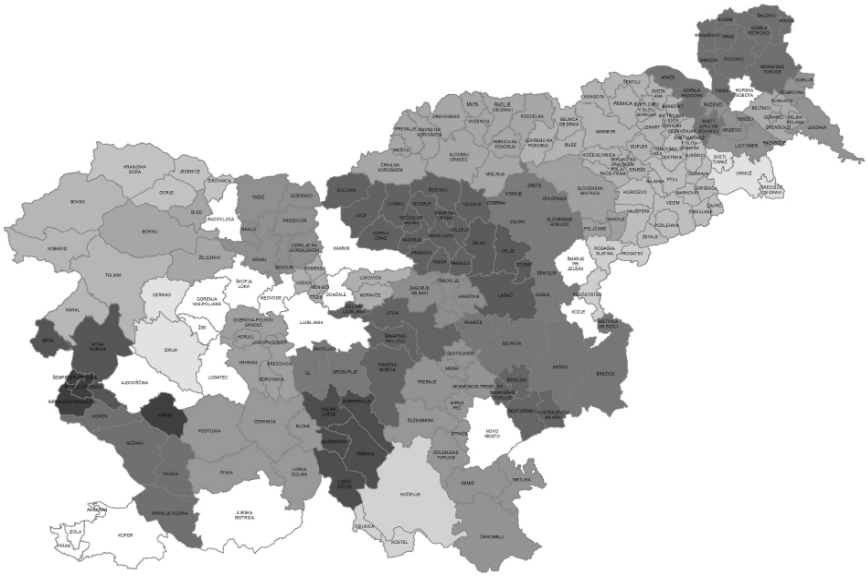
Ministrstvo	Organ v sestavi
1. Ministrstvo za notranje zadeve	Inšpektorat RS za notranje zadeve
2. Ministrstvo za javno upravo	Inšpektorat za javni sektor
3. Ministrstvo za obrambo	Inšpektorat za obrambo Inšpektorat za varstvo pred naravnimi in drugimi nesrečami
4. Ministrstvo za delo, družino, socialne zadeve in enake možnosti	Inšpektorat RS za delo
5. Ministrstvo za finance	Proračunska inšpekcija v okviru Urada RS za nadzor proračuna
6. Ministrstvo za gospodarski razvoj in tehnologijo	Tržni inšpektorat RS
7. Ministrstvo za infrastrukturo	Inšpektorat RS za infrastrukturo
8. Ministrstvo za izobraževanje, znanost in šport	Inšpektorat RS za šolstvo in šport
9. Ministrstvo za kmetijstvo, gozdarstvo in prehrano	Inšpektorat RS za kmetijstvo in okolje Inšpekcija za varno hrano, veterinarstvo in varstvo rastlin v okviru Uprave RS za varno hrano, veterinarstvo in varstvo rastlin
10. Ministrstvo za kulturo	Inšpektorat RS za kulturo in medije
11. Ministrstvo za okolje in prostor	Inšpekcija za sevalno in jedrsko varnost v okviru Uprave RS za jedrsko varnost
12. Ministrstvo za zdravje	Zdravstveni inšpektorat RS Inšpekcija za kemikalije v okviru Urada RS za kemikalije

Tabela 1: Seznam ministrstev in pripadajočih inšpektoratov (Vir: Vlada Republike Slovenije, n. d.)

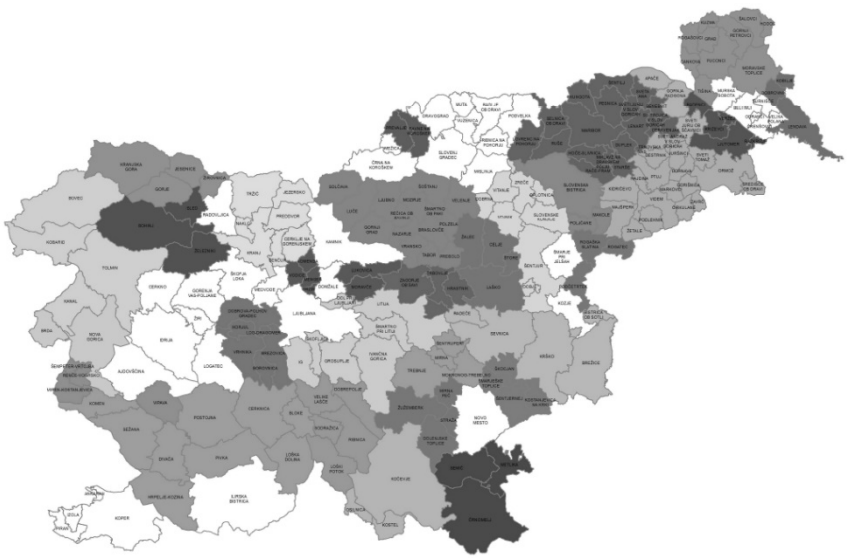
Na področju javne varnosti je treba posebej izpostaviti vlogo Inšpektorata RS za notranje zadeve kot organa v sestavi Ministrstva za notranje zadeve, ki ima hkrati položaj prekrškovnega organa. Če so namreč pri inšpekcijskih nadzorih s področja notranjih zadev ugotovljeni prekrški, le-ta vodi hitri postopek o prekršku na prvi stopnji. Pri tem je treba omeniti, da inšpektorat vodi prekrškovne postopke tudi v primeru kršitev Zakona o občinskem redarstvu (ZORed, 2006). Kriteriji za določanje prioritet njihovega delovanja v letu 2016 so javno objavljeni in temeljijo na dejavnikih iz t. i. ocene tveganja (Ministrstvo za notranje zadeve, 2016).

2.2.2 Lokalna raven

Na lokalni ravni je inšpekcija organizirana v okviru občinske uprave. Dve ali več občin skupaj lahko ustanovijo medobčinski inšpektorat, ki je pogosto povezan tudi z medobčinskim redarstvom in pokriva območja vključenih občin (sliki 2 in 3). Empirični podatki kažejo, da je ustanavljanje medobčinskih inšpektoratov in redarstev ena od najpogostejših oblik medobčinskega sodelovanja na področju izvajanja upravnih nalog (Rakar, Tičar in Klun, 2015). Medobčinsko sodelovanje zagotovi strokovno usposobljenost in specializacijo kadrov za raznovrstne naloge, ki jih inšpekcija opravlja, na drugi strani pa omogoči racionalnejše organizirano delo, sama organizacija dela pa je tudi cenejša (Železnik, 1999). Razlogov za tako pogosto medobčinsko sodelovanje na tem področju je več (Rakar in Grmek, 2011), izpostavili pa bi sofinanciranje stroškov teh organov s strani države v obsegu 50 % in neposredne finančne učinke delovanja teh organov (globe kot vir financiranja občin).



Slika 2: Vključenost občin v organe skupnih občinskih uprav – področje inšpekcij (vir: Fonda in Žohar, 2015: 121)



Slika 3: Vključenost občin v organe skupnih občinskih uprav – področje redarstva (vir: Fonda in Žohar, 2015: 128)

Pravna podlaga za oblikovanje inšpekcijske službe je določba 21. člena ZLS (1993), ki med izvirnimi nalogami, ki jih občina opravlja, določa tudi opravljanje inšpekcijskega nadzorstva nad izvajanjem občinskih predpisov, s katerimi občina ureja zadeve, ki spadajo v njeno pristojnost. Podrobnejšo določbo o inšpekciji na lokalni ravni najdemo v 50.a členu, ki določa, da nadzorstvo nad izvajanjem omenjenih predpisov izvaja občinska uprava, za opravljanje le-tega nadzorstva pa se lahko ustanovi občinska inšpekcija. Inšpekcijsko nadzorstvo opravljajo občinski inšpektorji kot uradne osebe s posebnimi pooblastili in odgovornostmi, v skladu z zakonom, ki ureja inšpekcijski nadzor (ZIN, 2002). ZLS (1993) v 67. členu določa, da o upravnih zadevah iz občinske pristojnosti odloča občinska uprava na prvi stopnji, na drugi stopnji pa župan, če zakon ne določa drugače. O pritožbah zoper odločbe, ki jih izda organ skupne občinske uprave, torej odloča župan občine. Župan katere občine odloča, je odvisno od tega, v katero krajevno pristojnost zadeva spada (ZLS, 1993). Občinske inšpekcijske službe so del občinske uprave, kar pomeni, da občinski inšpektor vodi inšpekcijski nadzor na prvi stopnji, med tem ko ga na drugi stopnji vodi župan (Kušar, 2005).

Pristojnosti občinskih inšpekcij urejajo posamezni predpisi in na njihovi podlagi sprejeti občinski prepisi, ki posegajo na klasična področja delovanja občin, in sicer varstvo okolja, urejanje in izvajanje gospodarskih javnih služb, urejanje in vzdrževanje občinskih cest, urejanje prometa ter urejanje javnega reda in miru (Železnik, 1999).

2.3 Pravni položaj inšpektorja

2.3.1 Splošno

Neposredne naloge inšpekcijskega nadzorstva opravljajo posebej pooblaščene fizične osebe, inšpektorji. Pravni položaj oz. pravni status inšpektorja v slovenski

ureditvi je posebne vrste (lat. *sui generis*). Njegova pooblastila so širša od pooblastil običajnih uradnikov, samostojnost njegovega dela je še posebej izpostavljena, saj imajo npr. pooblastilo za odločanje v upravnem postopku že neposredno na podlagi zakona (ZUP, 1999: 28. čl.).

Če področni predpisi ne določajo drugače, je za inšpektorja lahko imenovana oseba, ki ima: predpisano izobrazbo v skladu z zakonom, ki ureja sistem javnih uslužbencev, ustrezne delovne izkušnje in strokovni izpit za inšpektorja. Izjemoma se za inšpektorja ob sklenitvi delovnega razmerja lahko imenuje oseba, ki nima strokovnega izpita za inšpektorja, vendar mora ta izpit opraviti najkasneje v šestih mesecih od dneva imenovanja za inšpektorja. Inšpektor, ki nima strokovnega izpita za inšpektorja, lahko opravlja posamezna strokovna dejanja (npr. priprava analiz, informacij itd.) na področju inšpekcijskega nadzora. Inšpektor se mora stalno usposabljati za opravljanje svojih nalog v skladu s programom, ki ga predpiše predstojnik. Inšpektorju, ki v roku šestih mesecev po sklenitvi pogodbe o zaposlitvi, iz razlogov, ki so na njegovi strani, ne opravi strokovnega izpita, delovno razmerje preneha. Med razloge, ki so na strani inšpektorja, ne šteje upravičena odsotnost z dela zaradi bolezni oziroma druga odsotnost, daljša od enega meseca, v času katere prejema nadomestilo plače v skladu z zakonom. Inšpektorja, ki je premeščen in v roku šestih mesecev po premestitvi ne opravi strokovnega izpita za inšpektorja iz razlogov, ki so na njegovi strani, se premesti na delovno mesto, za katero izpolnjuje pogoje. Če takega delovnega mesta ni, se inšpektorja premesti po postopku, kot je določen za premestitev iz poslovnih razlogov (ZIN, 2002: 12.–13. čl.).

Položaj inšpektorja je posebej varovan. Inšpektorja se ne sme zaradi delovnih potreb brez njegovega soglasja premestiti na drugo delovno mesto, za katero ni določeno izvrševanje inšpekcijskih pooblastil. Po drugi strani pa zanj veljajo nekatere omejitve. Inšpektor ne sme opravljati dejavnosti oziroma ne sme opravljati dela za drugega delodajalca na področju, na katerem opravlja naloge inšpekcijskega nadzora, razen če gre za znanstveno ali pedagoško delo. Inšpektor mora varovati tajnost, s katero se seznani pri opravljanju nalog inšpekcijskega nadzora, in to tudi po prenehanju delovnega razmerja. Poleg tega je inšpektor dolžan varovati tajnost vira prijave in vira drugih informacij, na podlagi katerih opravlja inšpekcijski nadzor (ZIN, 2002: 14.–16. čl.).

Inšpektor je posebej odgovoren, če pri opravljanju nalog nadzora opusti izvršitev nalog oziroma ne sprejme ustreznih ukrepov, ki jih je skladno z zakonom dolžan izvršiti oziroma sprejeti; če ne poda prijave oziroma ne obvesti pristojnih organov o kršitvah zakonov ali drugih predpisov, ki jih je ugotovil pri izvrševanju nalog inšpekcijskega nadzora, in če opravlja dejavnost oziroma dela, ki jih zakon prepoveduje. Kršitev posebnih odgovornosti šteje za hudo kršitev obveznosti iz delovnega razmerja.

Inšpektorji imajo nekatera specifična pooblastila in lahko izrekajo posebne ukrepe. Pooblastila so pristojnosti, ki jih ima inšpektor v fazi ugotavljanja in dokazovanja pravno pomembnih dejstev o kršitvi predpisov, ukrepi pa so pristojnosti inšpektorja, ko ugotovi, da so bili predpisi kršeni – z ukrepi naj bi se vzpostavilo zakonito stanje. Pri opravljanju nalog inšpekcijskega nadzora ima tako inšpektor npr. pravico (ZIN, 2002: 19.–20. čl.): pregledati prostore, objekte,

naprave, delovna sredstva, napeljave, predmete, blago, snovi, poslovne knjige, pogodbe, listine in druge dokumente ter poslovanje in dokumentacijo državnih organov, gospodarskih družb, zavodov, drugih organizacij in skupnosti ter zasebnikov, vstopiti na parcele in zemljišča fizičnih in pravnih oseb, pregledati poslovne knjige, pogodbe, listine in druge dokumente ter poslovanje in dokumentacijo, kadar se vodijo in hranijo na elektronskem mediju ter zahtevati izdelavo njihove pisne oblike, ki mora verodostojno potrjevati elektronsko obliko, zaseči predmete, dokumente in vzorce v zavarovanje dokazov, opraviti navidezni nakup in opraviti druga dejanja, ki so v skladu z namenom inšpekcijskega nadzora.

Po končanem ugotovitvenem in dokaznem postopku lahko inšpektor odredi preventivne ukrepe, redne (kurativne) ukrepe, posebne ukrepe in ukrepe za varovanje pravic drugih oseb. V prvo skupino sodi ustno opozorilo, v drugo odreditev ukrepov z upravno odločbo, v tretjo začasna prepoved opravljanja dejavnosti in v četrto objava odločbe v sredstvih javnega obveščanja (Jerovšek in Kovač, 2008). Inšpekcijski postopek se torej zaključi z izdajo odločbe (če so ugotovljene kršitve; izrečejo se ukrepi) ter s sklepom o ustavitvi postopka ali v obliki zapisa o ustavitvi postopka na koncu zapisnika o inšpekcijskem pregledu, v primeru vzorčenja pa se to navede na spremni dopis, ko je zavezancu poslan izvid analize (ZIN, 2002: 28. čl.; Kovač, 2016b). Pritožba zoper odločbo inšpektorja praviloma ne zadrži njene izvršitve (30. člen ZIN (2002) v povezavi z 2. odst. 224. člena ZUP (1999)). O pritožbi zoper odločbo inšpektorja, ki jo je izdal v okviru prvostopenjskega organa državne inšpekcije (praviloma inšpektorata), odloča ministrstvo, v okviru katerega ta organ deluje. O odločbi inšpektorjev, ki delujejo v okviru občinske uprave, odločajo župani.

Inšpektorji morajo opravljati svoje naloge tako, da pri izvrševanju svojih pooblastil posegajo v delovanje pravnih in fizičnih oseb le v obsegu, ki je nujen za zagotovitev učinkovitega inšpekcijskega nadzora. Pri izbiri ukrepov inšpektor ob upoštevanju teže kršitve izreče ukrep, ki je za zavezanca ugodnejši, če je s tem dosežen namen predpisa (načelo sorazmernosti, ZIN, 2002: 7. čl.). V skladu s tem ZIN (2002) predvideva tudi stopnjevanje ukrepov. Pri določitvi roka za odpravo nepravilnosti mora inšpektor upoštevati težo kršitve, njene posledice za javni interes in okoliščine, od katerih je odvisno, v kolikšnem času lahko zavezanec ob dolžni skrbnosti odpravi nepravilnosti. Načelo javnosti (ZIN, 2002: 6. čl.) inšpektorju nalaga, da o svojem delovanju obvešča javnost, s čimer bi se lahko zavarovale pravice fizičnih oziroma pravnih oseb oziroma bi te osebe lahko ravnale preventivno. Tipičen primer je obvestilo o nevarnosti proizvodov, ki se objavi v sredstvih javnega obveščanja in na spletni strani inšpektorata (Tržni inšpektorat RS, 2016).

2.3.2 Načelo samostojnosti

Inšpektorji so pri opravljanju nalog inšpekcijskega nadzora v okviru svojih pooblastil samostojni (načelo samostojnosti, ZIN, 2002: 4. čl.). Inšpektor pri opravljanju nalog inšpekcijskega nadzora samostojno vodi postopek ter izdaja odločbe in sklepe v upravnem in prekrškovnem postopku. Načelo samostojnosti ima dve razsežnosti, in sicer individualno in organizacijsko. Individualna

razsežnost se nanaša na inšpektorja, ki je pri izvajanju pooblastil in izrekanju ukrepov samostojen. V tem smislu ZIN (2002) predstavlja ponovitev načela samostojnosti iz ZUP (1999: 12. čl.). Inšpektor je sicer dolžan upoštevati navodila in usmeritve predstojnika oziroma nadrejenega (ZIN, 2002: 18. čl.), a gre pri tem praviloma za splošna navodila in usmeritve izvajanja inšpekcijskega nadzora na določenem področju, ne pa npr. za navodila, kako naj se presojajo kateri dokazi. Glavni inšpektor v okviru svojih pooblastil odgovarja za zakonitost, kakovost in učinkovitost dela inšpekcije, za kar mora seveda imeti določene mehanizme glede organizacije in usmerjanja dela.

Zelo pomemben element samostojnosti je dejstvo, da ima inšpektor pooblastilo za odločanje, ki vsebuje tudi pooblastilo za vodenje postopka, že po samem zakonu (ZUP, 1999: 28. čl.; ZIN, 2002: 18. čl.). To pomeni, da mu pooblastil ne podeljuje predstojnik inšpekcijskega organa. Pooblastilo ima tisti inšpektor, ki mu zadeva pripade po naravi stvari in po razporedu ter programu dela. Ne glede na to pa predstojnik inšpekcijskega organa lahko oziroma mora odvzeti pooblastilo za vodenje že začetega postopka in zadevo dodeliti drugemu inšpektorju ali vodenje postopka prevzeti sam, če so podani t. i. izločitveni razlogi po ZUP ali ko je zoper inšpektorja uveden disciplinski postopek (Jerovšek in Kovač, 2008).

Organizacijska razsežnost samostojnosti se nanaša na status organizacij, v katerih se izvaja inšpekcijski nadzor. Na državni ravni inšpekcijski nadzor praviloma izvajajo inšpektorati, ki imajo status organov v sestavi ministrstva. Organi v sestavi ministrstva imajo namreč v razmerju do ministrstva tri vrste avtonomije, in sicer strokovno, kadrovsko in finančno (Jerovšek in Kovač, 2008). Na občinski ravni se, kot že povedano, vedno bolj uveljavlja ustanavljanje medobčinskih inšpektoratov kot organov skupne občinske uprave (Rakar et al., 2015).

2.3.3 Načelo varstva javnega in zasebnih interesov

V skladu z načelom varstva javnega in zasebnih interesov (ZIN, 2002: 5. čl.) mora inšpektor skrbeti za to, da se preprečijo ali onemogočijo dejanja fizičnih in pravnih oseb, ki pomenijo poseg v javni interes, določen z materialnim pravom, ki daje podlago za inšpekcijski nadzor, in varovati interese fizičnih in pravnih oseb, ki so v skladu z materialnim pravom. Inšpektor mora torej enakopravno varovati tako javni kot zasebni interes, pri čemer mora v primeru kolizije med obema, ki imata zakonsko podlago, dati prednost javnemu interesu. V primeru dvoma, ali je prizadet javni interes, pa mora ravnati v korist stranke (Pirnat, 2002). Varstvo javnega interesa in varstvo zasebnih interesov je nekoliko spremenjeno oziroma nadgrajeno načelo varstva pravic strank in varstva javnih koristi iz ZUP (1999).

Stranka inšpekcijskega postopka je fizična ali pravna oseba, katere ravnanje se nadzira. Imenuje se zavezanec, kajti zavezana je spoštovati oziroma izvrševati predpise. Zavezanec ima položaj pasivne stranke, kajti gre za stranko, zoper katero se vodi postopek. Oseba ne more zahtevati uvedbe postopka zoper sebe, da bi se ugotovila skladnost njenega ravnanja s predpisi (Jerovšek in Kovač, 2008). ZIN izrecno določa, da prijavitelj kršitve nima položaja stranke inšpekcijskega postopka, kajti inšpekcijski postopek se kljub prijavi vedno začne po uradni dolžnosti. Inšpektor na prijavo ni vezan, vendar jo mora ne glede na to obravnavati,

tudi če je anonimna, in ustrezno ukrepati. Če inšpektor v postopku ugotovi, da je prijava lažna, postopek ustavi. Šteje se, da je prijava lažna, če jo vlagatelj vloži, čeprav ve, da zavezanec ni kršil zakona ali drugega predpisa (ZIN, 2002: 24. čl.).

3 INŠPEKCIJSKI NADZOR Z VIDIKA VARNOSTI V OBČINAH

3.1 Uvod

Varnost na lokalni ravni je inkluzivna javna dobrina, ki mora biti dostopna vsem (Tičar, 2015). Varnost na lokalni ravni v ožjem smislu zagotavljata predvsem policija in občinsko redarstvo, v širšem smislu pa tudi inšpektorati in občinske inšpekcije. V najširšem smislu pa je k temu treba dodati tudi organe političnega odločanja in neformalne mreže (Modic, 2015). Ko gre za zagotavljanje varnosti, se torej prepletajo trije ključni referenčni objekti, in sicer država, samoupravna lokalna skupnost in posameznik (Sotlar, 2015).

3.2 Pristojnosti (med)občinskih inšpektoratov in sodna praksa

Za konkretizacijo do sedaj povedanega v nadaljevanju povzemamo pregled stvarne pristojnosti (med)občinskih inšpektoratov v izbranih občinah in predstavljamo izbrane primere upravnosodne prakse. V pregled smo vključili tri večje in tri manjše oz. srednje velike občine in s tem zagotovili primeren vzorec za namen tega prispevka. V prikaz upravnosodne prakse smo vključili tri novejše primere, da bi prikazali, kaj normativna ureditev pomeni v praksi.

Analiza stvarne pristojnosti izbranih organov kaže, da se področja v večini prekrivajo (gl. prilogo). Skupna področja pri izvajanju inšpekcijskih nadzorov v izbranih občinah so naslednja: nadzor nad oskrbo s pitno vodo, ravnanjem s komunalnimi odpadki in odvajanjem ter čiščenjem odpadnih komunalnih voda oziroma varstvom okolja na splošno, nadzor nad javnim redom in mirom ter občinskimi cestami in prometom. Našteta področja se dotikajo tudi varnosti, saj inšpekcijski nadzor nad varstvom okolja zagotavlja ne zgolj ohranitve narave, temveč tudi varnost občanov, kajti pitna voda v občini in primerno ravnanje z odpadki ter odpadnimi komunalnimi vodami je ključno za zdravje ljudi, ki živijo na področju posamezne občine. Tako na primer izvajanje nadzora nad čistilnimi napravami zagotavlja doseganje predpisanih standardov, ki ne ogrožajo ljudi ali okolja. Prav tako pa nadzor nad cestnim prometom in občinskimi cestami predstavlja način zagotavljanja varnosti za občane, preko inšpekcijskih nadzorov se ohranja vzdrževanje občinskih cest, hkrati pa izvajanje nadzora nad prometom, čeprav imajo tukaj veliko pooblastil občinski redarji. Z varnostjo je povezano tudi izvajanje nadzora nad samim urejanjem javnih površin, naselij, katerih potencialna neurejenost lahko zaradi nezanimanja za vlaganje sredstev v vzdrževanje pri prebivalcih vzbudi občutek, da živijo v nevarni soseski in povečuje občutek ogroženosti.

Pravkar omenjene povezave med pristojnostmi občinskih inšpekcij in varnostjo izhajajo tudi iz sodne prakse. Sodba Upravnega sodišča Republike Slovenije št. II U 292/2014 se nanaša na preglednost odseka kategorizirane

ceste. Občinska inšpekcija je med izvajanjem nadzora ugotovila, da je nasajena vegetacija motila preglednost v minimalni razdalji 45 metrov in posledično ni zagotavljala polja preglednosti, ki bi ga križišče moralo imeti. Tožeča stranka v postopku po opravljenem kontrolnem inšpekcijskem pregledu ni odpravila dela žive meje, ki je bil sporen. Zagovarjala se je, da posajene rastline ne vplivajo na preglednost in da odstranitev žive meje posega v varnost zasebnega življenja. Tožba je bila zavrnjena, zasebni interes se je moral podrediti javnemu interesu (Upravno sodišče RS, 2015).

V zadevi št. II U 460/2009 tožnik ni imel ustreznega soglasja s strani občinskega upravnega organa za položitev odtočnih cevi, ki jih je napeljal pod občinsko cesto. S strani inšpektorja odrejena odstranitev in vzpostavitev prejšnjega stanja je bila po mnenju sodišča utemeljena. Ugotovljeno je bilo, da je tožnik iz stanovanjske hiše napeljal odtočno cev pod občinsko cesto (omenjena cev je bila namenjena odpadni meteorni vodi in fekalni vodi), na nasprotni strani ceste pa se je navedena voda iztekala iz odtočne cevi v obcestni jašek. Glede na občinski odlok je mogoče izvajati dela ali nameščati kakršnekoli objekte v bližini ceste (to dejanje pa cesto lahko poškoduje) le ob soglasju občinskega upravnega organa, hkrati pa je prepovedano na cesto odvajati vodo, odplake in druge tekočine. Tožba je bila zavrnjena (Upravno sodišče RS, 2011).

V sodbi Upravnega sodišča RS, Sodba št. I U 600/2012 pa je šlo za komunalne odpadke. Občinska inšpekcija je izvajala nadzor nad upoštevanjem določb Zakona o varstvu okolja in Odloka o ravnanju s komunalnimi odpadki v Občini Jesenice. Ko gre za nezakonito odložene odpadke na zemljišču v lasti osebe zasebnega prava, imajo pooblastila za odstranitev komunalnih odpadkov občinske inšpekcije, pooblastila za odstranitev ostalih vrst odpadkov pa državna inšpekcija. Med inšpekcijskim nadzorom je bilo ugotovljeno, da odpadki na dveh parcelah v lasti osebe zasebnega prava niso organizirani in skladiščeni, temveč je šlo za komunalne odpadke, ki bi jih bilo treba odstraniti. Določen je bil 120-dnevni rok za odpravo nepravilnosti. Tožnik bi moral odpadke na svoje stroške odstraniti in to dokazati z ustreznim potrdilom izvajalca. Sodišče je menilo, da je bila izrečena odločba utemeljena, saj je šlo za odpadke, ki onesnažujejo okolje in motijo samo okolico, zato je tožbo zavrnilo (Upravno sodišče RS, 2014).

3.3 Občinsko redarstvo

Samoupravne lokalne skupnosti lahko poleg medobčinskega inšpektorata ustanovijo tudi (med)občinsko redarstvo, ki sta nato vključena v isto skupno upravo (npr. Medobčinski inšpektorat in redarstvo Maribor). Pravna podlaga sta ZLS (1993) in ZORed (2006). Delovno področje in naloge občinskega redarstva so urejene v 3. členu ZORed (2006). Občinsko redarstvo v skladu z zakonom in občinskim programom varnosti iz 6. člena ZORed (2006) skrbi za javni red in varnost na območju občine. Njegove pristojnosti segajo na raven nadzorovanja varnega in neoviranega cestnega prometa v naseljih; varovanje cest in okolja v samih naseljih in na občinskih cestah, ki so zunaj naselij; skrb za varnost na občinskih javnih poteh, rekreacijskih ter drugih javnih površinah; varovanje javnega premoženja, naravne in kulturne dediščine ter vzdrževanje javnega reda in miru.

Naloge občinskega redarstva opravljajo vodja občinskega redarstva in občinski redarji kot pooblaščene uradne osebe (ZORed, 2006: 5. čl.). Pri opravljanju svojega dela imajo naslednja pooblastila: opozorilo, ustna odredba, ugotavljanje istovetnosti, varnostni pregled osebe, zaseg predmetov, zadržanje storilca prekrška in kaznivega dejanja, uporaba prisilnih sredstev, med katera se štejejo fizična sila, sredstva za vklepanje in vezanje ter plinski razpršilec (ZORed, 2006: 10. čl.). Določena pooblastila pa najdemo tudi v področnih zakonih, npr. v Zakonu o pravilih cestnega prometa (ZPrCP, 2010). Pri izvajanju nadzora nad največjo dovoljeno hitrostjo redarji npr. nimajo pravice ustaviti voznika, temveč prekršek le slikovno dokumentirajo z napravami in sredstvi za nadzor (ZPrCP, 2010).

Pri opravljanju nalog in pooblastil občinski redarji sodelujejo s policisti. Če občinski redarji opravljajo naloge, ki jih določa zakon, skupaj s policisti, so dolžni ravnati po navodilu policista oziroma vodje policijske enote (ZORed, 2006: 9. čl.; Leben, 2014). Do razmejitev med pooblastili v varnosti cestnega prometa pa prihaja na podlagi kategorizacije cest (ZPrCP, 2010: 13. in 15. čl.).

4 RAZPRAVA

Prikaz normativne ureditve sam po sebi ne pove nič o neposrednem izvajanju nadzora, njegovi učinkovitosti in s tem o prispevku inšpekcijskega nadzora k varnosti v občinah. Normativna ureditev seveda vpliva na delovanje inšpekcijskih organov, zato se stremi k temu, da bi bila v tem smislu čim boljša. Ker pa namen tega prispevka ni statistično dokazovati korelacije med normativno ureditvijo in varnostjo v občinah, bi v zvezi s tem radi izpostavili zgolj nekaj ključnih vprašanj in dejstev, ki terjajo pozornost in nadaljnje raziskovanje.

Učinkovitost inšpekcijskega nadzora je nedvomno v interesu tako države kot občin. Institucionalni rezultat le-tega je ustanovitev Inšpekcijskega sveta in njegov Strateški načrt ukrepov za učinkovitejše delo inšpekcij, ki ga je sprejel 2013. Kot ugotavlja vlada, pa se le-ta zaradi različnih razlogov ne izvaja v celoti (pomanjkanje finančnih sredstev, nespoštovanje sprejetih sklepov, kadrovska problematika, nepoznavanje dela in pristojnosti inšpektorjev, neobstoj enotnega informacijskega sistema, ki bi podpiral delo inšpekcij) (Kern Pipan, Arko Korošec in Aškerc, 2015). V tem kontekstu je torej treba opozoriti na dejavnike, ki ovirajo modernizacijo oziroma reformo javne uprave in so v literaturi že podrobno razdelani (Koprić, 2014).

Dodaten problem predstavlja sam pojem učinkovitosti, saj se razlaga različno, pogosto kvantitativno in tehnicistično (Kovač, 2016b). Odbor za merjenje uspešnosti, učinkovitosti in kakovosti dela inšpekcijskih služb, ki deluje v okviru Inšpekcijskega sveta, je v letu 2013 sicer pripravil spremenjene kazalnike delovanja inšpekcij (Inšpekcijski svet, 2016), a so le-ti še vedno izrazito kvantitativni (npr. povprečno število inšpekcijskih nadzorov (zadev) na inšpektorja, odstotek uspešnih pritožb v inšpekcijskem postopku in število dni usposabljanja na zaposlenega). Kovačeva (2016b) zato predlaga celovitejši pristop, ki vključuje funkcionalno, procesno in organizacijsko razsežnost učinkovitosti. V zvezi s tem se lahko navežemo na nekatere ugotovitve Funkcijske analize

subjektov javnega sektorja, ki jo je naročilo ministrstvo, pristojno za upravo (A. T. Kearney Svetovanje, 2015). Skladno z njihovimi ugotovitvami npr. podporne aktivnosti analiziranih inšpektoratov predstavljajo 27 % vseh aktivnosti inšpektoratov. Čeprav inšpektorati niso navedeni med prioritetnimi organi, kjer bi z združevanjem teh dejavnosti dosegli največji dvig produktivnosti, to seveda ne pomeni, da ta ukrep ni potreben oziroma smiseln. Kot prioritetni pa so inšpektorati izpostavljeni na področju poročanja, čeprav je po drugi strani ugotovljeno, da niso največji generator poročil. Prav tako so kot prioritetni izpostavljeni na področju organizacijskih ravni, kar ne preseneča, saj je ta problem znan že dalj časa in se je doslej večkrat skušal neuspešno reševati v paketu s spremembami na področju teritorialne organiziranosti državne uprave (upravne enote) in lokalne samouprave (A. T. Kearney Svetovanje, 2015; Kovač, 2014/15).

Za področje občinskih inšpekcij in redarstev po našem vedenju ne obstaja tej raziskavi primerljiva raziskava, kar predstavlja pomemben manko pri podlagah za odločanje o morebitnih organizacijskih in drugih spremembah. Predlog Strategije razvoja lokalne samouprave sicer neposredno ne omenja inšpekcijskega nadzorstva, a je to kljub temu zajeto v več pogledih (Ministrstvo za javno upravo, 2015), in sicer: učinkovitost kot eden od treh elementov, na katerih temelji sodobna evropska lokalna samouprava, partnersko razmerje med državo in lokalno samoupravo, medinstitucionalni dialog, razvoj sposobnosti zadovoljevanja skupnih potreb in interesov prebivalcev na lokalni ravni (medobčinsko sodelovanje in povezovanje) in finančna avtonomija občin.

Po drugi strani pa je posodobitev (državnega) inšpekcijskega nadzora sestavni del Strategije razvoja javne uprave 2015–2020 (Kern Pipan et al., 2015). Spremembe so usmerjene predvsem v vzpostavitev ustreznih podlag in medsebojno povezljivost in izmenjavo informacij inšpektoratov. Pri teh spremembah bo treba preučiti in smiselno uporabiti tudi dokument OECD, ki je leta 2014 v okviru načela dobrih praks za regulatorno politiko izdal priporočila za izvajanje predpisov in inšpekcije (Kern Pipan et al., 2015; Organisation for Economic Co-operation and Development, 2014).

5 ZAKLJUČEK

Inšpekcijski nadzor je učinkovit, če je na podlagi njegove izvedbe kršitev manj – posledično se poveča tudi varnost, ob predpostavki, da so s predpisi ustrezno zajete in urejene situacije, ki predstavljajo varnostno tveganje. Kot smo prikazali, učinkovitost inšpekcijskega nadzora ni odvisna samo od inšpekcij, ampak tudi od številnih drugih dejavnikov. Ker je upravni sistem povezan s političnim in družbenim sistemom, so njegove spremembe pogosto povezane z različnimi ovirami. Slaba stran dosedanjega razvoja na tem področju je ta, da so bili sistemski premiki zelo težki in počasni. Dobra stran pa je, da obstajajo primeri uspeha, kamor je treba šteti zlasti ustanavljanje medobčinskih inšpektoratov in redarstev. Za nadaljnje izboljšanje menimo, da bi bilo koristno izvesti funkcijsko analizo organiziranosti inšpekcij in redarstev na lokalni ravni, nadaljevati z letnimi posveti o delovanju skupnih občinskih uprav, ki jih soorganizira ministrstvo, pristojno za upravo, in intenzivneje vključiti izvajalce predpisov in javnost v njihovo pripravo.

UPORABLJENI VIRI

A. T. Kearney Svetovanje. (2015). *Funkcijska analiza subjektov javnega sektorja*. Ljubljana: Ministrstvo za javno upravo. Pridobljeno na http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/SOJ/Funkcijska_analiza/Funkcijska_analiza_-_Metodolsko_porocilo_fin.pdf

Eichhorn, P., Friedrich, P., Jann, W., Oeschler, W. A., Puettner, G. in Reinermann, H. (ur.) (2003). *Verwaltungslexikon* (3. Aufl.). Baden-Baden: Nomos Verlagsgesellschaft.

Energetski zakon [EZ-1]. (2014). *Uradni list RS,* (17/14).

Fonda, M. in Žohar, F. (2015). Predstavitev kart sodelovanja v skupnih občinskih upravah po posameznih področjih nalog. V F. Žohar (ur.), *Zbornik VIII. posveta Delovanje skupnih občinskih uprav v Sloveniji* (str. 116–129). Ljubljana: Skupnost občin Slovenije, Združenje občin Slovenije, Ministrstvo za javno upravo. Pridobljeno na http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/JAVNA_UPRAVA/svlsrp.gov.si/pageuploads/lok-sam-2015/splosno-ls-ls/medob-sodel/sou/8-posvet-sou-2015/zbornik-sou-fu-Ljubljana-2632015.pdf

Grafenauer, B. in Brezovnik, B. (2006). *Javna uprava*. Maribor: Pravna fakulteta.

Inšpekcijski svet. (2016). *Poročilo Inšpekcijskega sveta za leto 2015*. Pridobljeno na http://www.mju.gov.si/si/o_ministrstvu/inspekcijski_svet/letna_porocila_inspekcijskega_sveta/

Jerovšek, T. in Kovač, P. (2008). *Posebni upravni postopki*. Ljubljana: Fakulteta za upravo.

Kern Pipan, K., Arko Korošec, M. in Aškerc, M. (ur.) (2015). *Javna uprava 2020: strategija razvoja javne uprave 2015–2020.* Ljubljana: Ministrstvo za javno upravo. Pridobljeno na http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/JAVNA_UPRAVA/Kakovost/Strategija_razvoja_JU_2015-2020/Strategija_razvoja_SLO_final_web.pdf

Koprić, I. (ur.) (2014). *Upravna znanost*. Zagreb: Pravni fakultet.

Kovač, P. (2014/15). Better local governance by integrative reorganization of state administration and self-government (in Slovenia). *The NISPAcee Journal of Public Administration and Policy, 7*(2), 117–134.

Kovač, P. (2016a). Inspection regulation between general procedural codification and field specifics – A case study of Slovenia. *Danube: Law and Economics Review*, *7*(1), 1–17.

Kovač, P. (ur.). (2016b). *Inšpekcijski nadzor*. Ljubljana: Uradni list Republike Slovenije.

Kušar, J. (2005). Inšpekcijske službe v občinah. *Pravna praksa*, *24*(31/32), VII–VIII.

Leben, M. (2014). *Policisti in občinski redarji – sodelovanje in razmejitev pristojnosti* (Diplomsko delo). Ljubljana: Fakulteta za upravo.

Mestna občina Ljubljana. (2016). *Inšpektorat.* Pridobljeno na http://www.ljubljana.si/si/mol/mestna-uprava/prekrskovna-organa/inspektorat/

Mestna občina Maribor. (n. d.). *Medobčinski inšpektorat in redarstvo Maribor.* Pridobljeno na http://www.maribor.si/podrocje.aspx?id=566

Mestna občina Novo mesto. (n. d.). *Občinski inšpektorat.* Pridobljeno na http://www.novomesto.si/si/obcina/uprava/organi/insp/?cookieu=ok

Ministrstvo za javno upravo. (24. 11. 2015). *Strategija razvoja lokalne samouprave v Republiki Sloveniji (gradivo za javno razpravo)*. Pridobljeno na http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/JAVNA_UPRAVA/BESEDILO-javna_razprava_25_11_2105.pdf

Ministrstvo za javno upravo. (2016). *Inšpekcijski svet.* Pridobljeno na http://www.mju.gov.si/si/o_ministrstvu/inspekcijski_svet/

Ministrstvo za notranje zadeve. (2016). *Inšpekcijski nadzor.* Pridobljeno na http://www.mnz.gov.si/si/varnost_in_nadzor/inspektorat_rs_za_notranje_zadeve/inspekcijski_nadzor/

Modic, M. (2015). Vloga in vidiki sodelovanja občin pri zagotavljanju varnosti na lokalni ravni – predstavitev ugotovitev ciljnega raziskovalnega projekta. V G. Meško (ur.), *Varnost v lokalnih skupnostih: zbornik prispevkov* (str. 46–54). Ljubljana: Fakulteta za varnostne vede.

Občina Cerkno. (n. d.). *Medobčinski inšpektorat.* Pridobljeno na http://www.cerkno.si/o-obcini/obcinska-uprava/sluzbe-in-kontakti/medobcinski-inspektorat/

Občina Metlika. (n. d.). *Medobčinska inšpekcija in redarstvo.* Pridobljeno na http://www.metlika.si/content.asp?sif_co=81

Občina Slovenj Gradec. (2012). *Medobčinski inšpektorat Koroške.* Pridobljeno na http://www.slovenjgradec.si/medobcinski-inspektorat-koroske.html

Organisation for Economic Co-operation and Development. (2014). *Regulatory enforcement and inspections*. OECD Publishing. Pridobljeno na http://www.oecd.org/gov/regulatory-enforcement-and-inspections-9789264208117-en.htm

Pirnat, R. (2002). Ustavnopravni položaj uprave. *Podjetje in delo*, *28*(6/7), 1271–1279.

Pirnat, R., Bugarič, B., Jerovšek, T., Kerševan, E., Pličanič, S., Korade Purg Š. et al. (2004). *Komentar zakonov s področja uprave*. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti.

Rakar, I. in Grmek, M. (2011). Racionalnost na lokalni ravni – primer organov skupnih občinskih uprav. *Javna uprava, 47*(3/4), 131–152.

Rakar, I., Tičar, B. in Klun, M. (2015). Inter-municipal cooperation: Challenges in Europe and in Slovenia. *Transylvanian Review of Administrative Sciences*, (45E), 185–200.

Sotlar, A. (2015). Reševanje varnostnih problemov – med nacionalno, lokalno in človekovo varnostjo. V G. Meško (ur.), *Varnost v lokalnih skupnostih: zbornik prispevkov* (str. 26–33). Ljubljana: Fakulteta za varnostne vede.

Tičar, B. (2015). Pravna ureditev varnosti na lokalni ravni. V G. Meško (ur.), *Varnost v lokalnih skupnostih: zbornik prispevkov* (str. 34–45). Ljubljana: Fakulteta za varnostne vede.

Tičar, B. in Rakar, I. (2011). *Pravo javnega sektorja.* Maribor: Inštitut za lokalno samoupravo in javna naročila.

Tržni inšpektorat RS. (15. 5. 2016). *Nevarni proizvodi.* Pridobljeno na http://www.ti.gov.si/fileadmin/ti.gov.si/pageuploads/nevarni_proizvodi/index.html

Upravno sodišče RS. (2011). Sodba II U 460/2009 z dne 7. 4. 2011. Pridobljeno na http://www.sodnapraksa.si/?q=ob%C4%8Dinske%20in%C5%A1pekcije&dat

abase[SOVS]=SOVS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2010040815256985
Upravno sodišče RS. (2014). Sodba I U 600/2012 z dne 9. 7. 2014. Pridobljeno na http://www.sodnapraksa.si/?q=ob%C4%8Dinske%20in%C5%A1pekcije&database[SOVS]=SOVS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2012032113067708.
Upravno sodišče RS. (2015). Sodba II U 292/2014 z dne 10. 7. 2015. Pridobljeno na http://www.sodnapraksa.si/?q=ob%C4%8Dinske%20in%C5%A1pekcije&database[SOVS]=SOVS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=1&id=2012032113080594.
Ustava Republike Slovenije. (1991, 1997, 2000, 2003, 2004, 2006, 2013). *Uradni list RS*, (33/91-I, 42/97, 66/00, 24/03, 69/04, 68/06, 47/13).
Virant, G. (2009). *Javna uprava*. Ljubljana: Fakulteta za upravo.
Vlada Republike Slovenije (n. d.). *Ministrstva.* Pridobljeno nahttp://www.vlada.si/o_vladi/ministrstva/
Zakon o državni upravi [ZDU-1]. (2002, 2003, 2004, 2005, 2009, 2012, 2013, 2014, 2016). *Uradni list RS,* (52/02, 56/03, 61/04, 123/04, 93/05, 48/09, 21/12, 47/13, 12/14, 90/14, 51/16).
Zakon o inšpekcijskem nadzoru [ZIN]. (2002, 2007, 2014). *Uradni list RS*, (56/02, 26/07, 40/14).
Zakon o javnih uslužbencih [ZJU]. (2002, 2005, 2007, 2008). *Uradni list RS*, (56/02, 23/05, 113/05, 33/07, 65/08).
Zakon o lokalni samoupravi [ZLS]. (1993, 1994, 1995, 1997, 1998, 2000, 2002, 2005, 2007, 2008, 2009, 2010). *Uradni list RS*, (72/93, 57/94, 14/95, 26/97, 70/97, 10/98, 74/98, 70/00, 51/02, 72/05, 60/07, 76/08, 79/09, 51/10).
Zakon o občinskem redarstvu [ZORed]. (2006). *Uradni list RS*, (139/06).
Zakon o pravilih cestnega prometa [ZPrCP]. (2010). *Uradni list RS*, (109/10).
Zakon o prekrških [ZP-1]. (2003, 2004, 2005, 2006, 2008, 2009, 2011, 2013) *Uradni list RS,* (7/03, 86/04, 44/05, 40/06, 51/06, 115/06, 17/08, 21/08, 108/09, 9/11, 21/13, 111/13).
Zakon o splošnem upravnem postopku [ZUP]. (1999, 2000, 2002, 2004, 2005, 2007, 2008, 2010, 2013). *Uradni list RS*, (80/99, 70/00, 52/02, 73/04, 119/05, 126/07, 65/08, 8/10, 82/13).
Zakon o veterinarstvu [ZVet-1]. (2001). *Uradni list RS*, (33/01).
Železnik, M. (1999). Pristojnosti inšpekcijskih služb v občinah. V S. Vlaj (ur.), *Občinske inšpekcije* (str. 31–34). Ljubljana: Inštitut za lokalno samoupravo pri Visoki upravni šoli.

O avtorjih:

Dr. Iztok Rakar, docent za področje javne uprave. Raziskuje na področjih upravnega prava in lokalne samouprave. Od leta 2013 je slovenski član skupine neodvisnih strokovnjakov za Evropsko listino lokalne samouprave pri Svetu Evrope. E-pošta: rakar.iztok@gmail.com

Ester Doljak, redna študentka Fakultete za varnostne vede Univerze v Mariboru in predmetna tutorka za področje pravne ureditve javne uprave. V študijskem letu 2014/2015 je bila uvrščena med najboljših 5 % v svoji generaciji. E-pošta: ester.doljak@student.um.si

Dr. Bojan Tičar, redni profesor za področje prava na Fakulteti za varnostne vede Univerze v Mariboru. Njegova področja raziskovanja so upravno pravo, pravna ureditev javne uprave in pravni vidiki upravljanja organizacij. E-pošta: bojan.ticar@fvv.uni-mb.si

PRILOGA: Pristojnosti (med)občinskih inšpektoratov

V Mestni občini Ljubljana (2016) opravlja inšpektorat nadzorne naloge na področjih:

- nadzor nad predpisi občine in drugih aktov, s katerimi mestna občina ureja stvari iz svoje pristojnosti,
- vodenje prekrškovnega postopka v skladu z zakonom,
- okoljsko nadzorstvo, in sicer nadzor nad ravnanjem s komunalnimi odpadki,
- sodelovanje pri pripravi odlokov in drugih splošnih aktov,
- vodenje evidenc o izrečenih ukrepih in evidenc v zvezi s prekrškovnim organom.

V Mestni občini Maribor (n. d.) Medobčinski inšpektorat pokriva nadzor nad določbami naslednjih odlokov:

- občinske ceste in varnost v prometu na le-teh,
- ravnanje s komunalnimi odpadki,
- oglaševanje in reklamiranje,
- občinske takse,
- taksi službe,
- naravne in kulturne znamenitosti,
- pokopališka dejavnost,
- urejanje in vzdrževanje javnih in zelenih površin,
- odvajanje in čiščenje odpadnih voda,
- drugi odloki, na področju katerih ima inšpektorat pooblastila.

V Mestni občini Novo mesto (n. d.) Občinski inšpektorat izvaja inšpekcijski nadzor na področju:

- občinskih cest in prometa,
- odpadnih in padavinskih voda (odvajanje in čiščenje),
- odlaganju komunalnih odpadkov,
- oskrbi s pitno vodo,
- urejanju javnih tržnic, javne razsvetljave, zelenih površin in pokopališke dejavnosti,
- urejanju in uporabi javnih površin,
- plakatiranju,
- pristojnosti kot prekrškovni organ.

V občini Metlika Medobčinski inšpektorat izvaja naloge s področja (Občina Metlika, n. d.):

- oskrbe s pitno vodo,
- odvajanja, čiščenja komunalnih odpadnih voda in padavinskih voda,
- ravnanja in odlaganja komunalnih odpadkov,
- javne snage,

- urejanja javnih površin in zelenih površin,
- urejanja javnih poti in površin za pešce,
- vzdrževanja lokalnih javnih cest in urejanja le-teh,
- pokopališke in pogrebne dejavnosti,
- plakatiranja,
- občinskih in turističnih taks,
- zimske službe,
- označevanja cest in ulic ter naselji ter zgradb.

V Cerknem opravlja Medobčinski inšpektorat naloge na področjih (Občina Cerkno, n. d.):

- oskrba s pitno vodo,
- odvajanje in čiščenje komunalnih odpadnih voda in padavinskih voda,
- komunalnih odpadkov,
- urejanje in vzdrževanje javnih poti,
- urejanje površin za pešce in zelenih površin,
- vzdrževanje lokalnih javnih cest,
- pokopališka dejavnost,
- urejanje javnih tržnic,
- oglaševanje,
- občinske in turistične takse,
- druga področja, določena z občinskimi in drugimi predpisi.

Medobčinski inšpektorat Koroške izvaja inšpekcijski nadzor nad (Občina Slovenj Gradec, 2012):

- varstvom okolja,
- urejenostjo naselij,
- ravnanjem z odpadki in plodno zemljo,
- javnimi potmi in prometnimi površinami,
- zelenimi in drugimi javnimi površinami, objekti in napravami,
- vodnimi viri,
- oskrbo z vodo,
- odvajanjem in čiščenjem odpadnih voda in padavinskih voda,
- označevanjem ulic, trgov, cest, naselij in zgradb,
- oglaševanjem in plakatiranjem,
- pokopališko dejavnostjo,
- tržnim redom,
- zimsko službo,
- izobešanjem zastav,
- drugimi področji, določenimi s predpisi ali občine ustanoviteljice ali države.

VARSTVOSLOVJE,
letn. 18
št. 3
str. 270–287

Električni in elektronski odpadki – grožnja in izziv za človeka

Andreja Rožnik, Gorazd Meško

Namen prispevka:

Namen prispevka je predstaviti električne in elektronske odpadke ter problematiko, ki jo s seboj prinašajo. Tovrstni odpadki so najhitreje rastoč mednarodni problem, ki se ga mora posameznik zavedati. S prispevkom želimo bralcu predstaviti dokaj nepoznano področje e-odpadkov.

Metode:

V prispevku je bila uporabljena analiza primarnih in sekundarnih virov, vključno s kratkim pregledom mednarodnih in nacionalnih predpisov o urejanju področja elektronskih in električnih odpadkov.

Ugotovitve:

E-odpadki so večplasten problem, ki zadeva številne akterje, vključene v postopek ravnanja z e-odpadki. Toksičnost e-odpadkov negativno vpliva na človeka in naravo, kljub temu pa se velike količine e-odpadkov neustrezno reciklira z namenom pridobivanja dragocenih kovin. E-odpadki pa po drugi strani predstavljajo izziv za države, saj jih združujejo in povezujejo v mreže, ki se borijo zoper naraščanje e-odpadkov in z njim povezane kriminalitete.

Uporabnost raziskave:

Analiza prispevka o električnih in elektronskih odpadkih nam daje osnovo za nadaljnje raziskovanje preučevanega problema, s katerim se moramo učinkovito soočiti, saj postaja grožnja človeku in naravi.

Izvirnost/pomembnost prispevka:

Prispevek strukturirano prikazuje področje električnih in elektronskih odpadkov. Bralcu ponuja kratek vpogled v razumevanje problema e-odpadkov ter groženj in izzivov, ki jih prinaša. Prispevek obravnava temo, ki je v Sloveniji slabo poznana in raziskana.

UDK: 628.477.6:504

Ključne besede: električni odpadki, elektronski odpadki, e-odpadki, grožnje, izzivi

Electrical and Electronic Waste – a Threat and a Challenge for a Human

Purpose:

The purpose of the paper is to present the electrical and electronic waste and also problems caused by these waste. The electrical and electronic waste (shorter

e-waste) is one of the fastest growing global problem we have to confront with. Our intent is to introduce a quite unknown area of the e-waste to a reader.

Design:

An analysis of the primary and secondary sources, including a short review of international and national regulations regarding the management of electrical and electronic waste, was used in the paper.

Findings:

E-waste is multilayered problem, concerning many actors involved in e-waste circle. E-waste toxicity has a negative impact on human and nature. Regardless this fact the enormous quantities of e-waste are improperly recycled in order to recover valuable metals. On other hand, e-waste is a challenge for countries because it unites and connects them into networks, which fight against the growing quantities of e-waste and its criminality.

Practical Implications:

The analysis of electrical and electronic waste presents the basis for further more in-depth research of studied problem, which is a threat to human and nature. This is the main reason we have to confront this problem effectively.

Originality/Value:

The paper structurally presents the area of electrical and electronic waste. It offers a short insight into understanding of the e-waste problem, its threats and challenges. The paper deals with a topic that is poorly known and researched in Slovenia.

UDC: 628.477.6:504

Keywords: electrical waste, electronic waste, e-waste, threats, challenges

1 UVOD

Razvoj informacijske tehnologije z različnimi inovativnimi električnimi in elektronskimi napravami in opremo posamezniku omogoča čedalje bolj lagodno življenje, a po drugi strani prinaša negativno in dokaj skrito grožnjo človeku in naravi. Vsako tehnološko in informacijsko napravo sčasoma nadomesti novejša naprava zaradi različnih razlogov (ali se je naprava ali oprema pokvarila, ali je postala neuporabna ali pa je zgolj zastarela oziroma se ji je iztekla življenjska doba), kar posledično pomeni, da je ta oprema prešla v naslednjo fazo, fazo odpadne naprave. Baldé et al. (2015b) v raziskavi o električnih in elektronskih odpadkih[1] (krajše e-odpadki) ugotavljajo, da so ti najhitreje rastoči produkt proizvodnje industrije na svetu in ocenjujejo, da je bilo okoli 41,8 milijonov metričnih ton

1 *Direktiva 2012/19/EU Evropskega parlamenta in Sveta o odpadni električni in elektronski opremi (2012) v Prilogi 1A navaja 10 kategorij električne in elektronske opreme, ki so: veliki gospodinjski aparati; mali gospodinjski aparati; oprema za IT in telekomunikacije; oprema za zabavno elektroniko; oprema za razsvetljavo; električna in elektronska orodja; igrače, oprema za prosti čas in šport; medicinske naprave; instrumenti za spremljanje in nadzor in avtomati.*

(Mt) e-odpadkov[2] proizvedenih v letu 2014. Za prihodnost pa napoveduje, da se bo količina e-odpadkov do leta 2018 povečala na 50 Mt. Količina e-odpadkov, ki bo nastala do leta 2018, je velika, vendar skrita in temna stran e-odpadkov je poleg količine predvsem njihova sestava oziroma sestavni deli opreme, ki omogočajo delovanje in neustrezno recikliranje dotične opreme, ki jo posameznik zavrže. Zgolj okoli 10 do 40 % e-odpadkov pa naj bi bilo ustrezno recikliranih in odloženih na odlagališča (United Nations Office on Drugs and Crime [UNODC], 2013). Widmer, Oswald-Krapfova, Sinha-Khetriwal, Schnellmann in Böni (2005) ocenjujejo, da osem odstotkov vseh komunalnih odpadkov predstavljajo e-odpadki. Baldé et al. (2015b) nadaljujejo, da je od 41,8 Mt e-odpadkov zgolj 6,5 Mt ustrezno dokumentiranih in recikliranih, preostali delež ni statistično zabeležen. Po podatkih UNODC (2013) naj bi okoli 80 % globalne količine e-odpadkov končalo v Aziji. Robinson (2009) meni, da bodo v okviru desetih let Kitajska, Vzhodna Evropa in Latinska Amerika postale večinske proizvajalke e-odpadkov. Grant et al. (2013) dodajajo, da ne narašča samo količina e-odpadkov, ampak tudi bolezni in zdravstvene težave ljudi zaradi onesnaženega zraka, zemlje in vode. Onesnaževanje okolja, zaradi nezakonitega izvoza e-odpadkov v države v razvoju in tretje države, umeščamo v kategorijo ekološke kriminalitete[3].

Ekološka kriminaliteta je glede na poročila tako različnih institucij (Europol, 2015; Interpol, 2009) kot tudi različnih raziskovalcev (Baird, Curry in Cruz, 2014; Huisman et al., 2015; Rucevska et al., 2015; White, 2013) zelo resna problematika, ki ima mednarodne razsežnosti in v primeru e-odpadkov zajema nezakoniti izvoz in uvoz e-odpadkov, vpletenost organizirane kriminalitetne združbe, beloovratniške korupcije ter drugih akterjev, ki so posredno in neposredno vključeni v nezakonite posle z e-odpadki.

E-odpadki so torej ena izmed najhitreje rastočih vej komunalnih odpadkov, pri čemer ni izjema niti Slovenija. V osnutku[4] Programa ravnanja z odpadki in programa preprečevanja odpadkov Republike Slovenije (Ministrstvo za okolje in prostor, 2015: 73–74) je na področju e-odpadkov navedena statistika, in sicer je bilo v letu 2013 na trg dane 28.493 ton električne in elektronske opreme (krajše e-opreme), kar pomeni več kot 14 kg na prebivalca, in zbranih več kot 6.000 ton e-odpadkov. Slovenija je kot država članica Evropske unije [EU] sledila pravu EU in implementirala direktive na področju e-odpadkov in opreme v nacionalno pravo. Ohlapno spisane direktive državam omogočajo, da oblikujejo termin e-odpadki glede na svoje potrebe in zahteve po urejenosti tega področja.

2 *Ti e-odpadki so sestavljeni iz 1,0 Mt opreme za razsvetljavo (predvsem luči), 6,3 Mt zaslonov, 3,0 Mt majhne opreme informacijske tehnologije (kot so mobilni telefoni, žepna računala, osebni računalniki, tiskalniki ipd.), 12,8 Mt mali gospodinjski aparati (sesalec, mikrovalovna pečica, toaster ipd.), 11,8 Mt veliki gospodinjski aparati (pralni stroji, sušilne naprave za perilo, pomivalni stroji, električne pečice, fotovoltaični paneli ipd.) in 7,0 Mt hladilnih in zamrzovalnih aparatov (Baldé et al., 2015b).*

3 *Ekološko kriminaliteto se definira kot »vsako začasno ali trajno pravno opredeljeno odklonsko ravnanje, ali opustitev ravnanja, ki povzroči umetno spremembo, poslabšanje, obremenitev, propadanje ali uničenje (človekovega) okolja ali zaviranje njegovih naravnih sprememb« (Eman, 2008: 227). V ekološko kriminaliteto White (2013) umešča kriminaliteto, ki je povezana z onesnaževanjem (zrak, voda, zemlja) in kriminaliteto zoper divje živali (vključujoč nezakonito izsekavanje in trgovanje z gozdovi in z živalmi).*

4 *Program ravnanja z odpadki in program preprečevanja odpadkov Republike Slovenije (Ministrstvo za okolje in prostor, 2015), ki ga je pripravilo Ministrstvo za okolje in prostor, kljub roku za pripombe in dopolnitve (1. 2. 2016) do maja 2016 še ni bil potrjen s strani Vlade RS.*

V prispevku bomo na kratko predstavili problematiko definiranja e-odpadkov, past oziroma grožnjo, ki jo predstavljajo e-odpadki, in nadalje tudi pravno urejanje tega področja. Nadaljujemo z izzivi in nazadnje v zaključku predlagamo rešitve za reševanje globalnega problema e-odpadkov.

2 E-ODPADEK KOT GROŽNJA ČLOVEKU

Človek se premalo zaveda, da so lahko e-odpadki grožnja človeštvu, živalim in okolju. Povprečni EU prebivalec odvrže v koš za mešane odpadke med 1 in 2 kg e-odpadkov (npr. mobitel, svetilka, električna zobna ščetka, električne igrače ipd.) (Baldé, Wang, Kuehr in Huisman, 2015a). Okoli 0,7 Mt e-odpadkov proizvedejo države članice EU (Baldé et al., 2015a). Grožnja e-odpadkov je skrita v posameznikovi neozaveščenosti, da so tudi majhne e-opreme problematične glede sestave in so strupene ob nepravilnem recikliranju. Grožnjo še toliko bolj spodbuja dejavnik hitrega in enostavnega zaslužka z dragocenimi kovinami, ki ga e-odpadki vsebujejo. Dobiček imajo tudi posamezniki in združbe, ki so vključeni v cikel izvoza/uvoza e-odpadkov in se ne ukvarjajo z vprašanjem, če na končni destinaciji osebe na okolju varen način reciklirajo e-odpadke. Velik zaslužek z nizkim tveganjem za kaznovanje za storjeno dejanje kot tudi pravna neurejenost in dileme pri opredeljevanju termina e-odpadek v državah po svetu pretehta človekovo odgovorno obnašanje in občutek za ustrezno ravnanje z e-odpadki.

2.1 Dileme opredeljevanja termina električni in elektronski odpadki

E-odpadki predstavljajo dilemo poimenovanja oziroma definiranja termina električni in elektronski odpadki (Baldé, 2015a; Rucevska et al., 2015; StEP, 2014). Rucevska et al. (2015) izpostavljajo, da je za naraščajočo kriminaliteto z e-odpadki ključno poimenovanje tega termina v zakonodaji držav. Izziv predstavlja klasifikacija opreme, ki spada v področje e-odpadkov kot tudi oblikovanje posebnih kod za e-odpadke, saj sta slednja bistvena za podatkovno obdelavo baz in kreiranje profilov, s katerimi bi tarčno odkrivali pošiljke z e-odpadki (Rucevska et al., 2015).

Kot že omenjeno, je za e-odpadke problematično različno poimenovanje termina e-odpadek. Predstavniki StEP se zavedajo problematike naraščajoče grožnje e-odpadkov in se zavzemajo za mednarodno definicijo e-odpadkov, zato izhajajo pri oblikovanju definicije za termin e-odpadek iz pomena besede v terminu, in sicer je beseda »odpadek« samopojasnjujoča in logično implicira, da se le-ta predmet ne bo več uporabljal, je zavržen kot neuporaben ali odvečen za lastnika (2014: 4). Glede na razlago pomena besed so pripravili splošno definicijo, in sicer e-odpadek je termin, ki se uporablja za vse tipe opreme, ki je električnega in elektronskega izvora kot tudi njihovi sestavni deli, ki jih lastnik zavrže brez namena ponovne uporabe (StEP, 2014). Podobno so Baldé et al. (2015b) oblikovali termin e-odpadek, ki predstavlja oziroma le-ta opisuje stvari/izdelke, ki v celoti predstavljajo opremo električnega ali elektronskega izvora ali pa izdelek vsebuje zgolj en del električnega ali elektronskega izvora in ki ga lastnik zavrže kot

odpadek, brez namere po nadaljnji uporabi. Lutherjeva (2010) pa je uporabila termin e-odpadek za zastarelo, poškodovano ali nepopravljivo elektronsko opremo (kot so televizija, centralne procesorske enote računalnika, računalniški monitorji, prenosni računalnik, tiskalniki, optični čitalci), vključno s pripadajočimi žičnimi povezavami. Medtem ko Puckett in Smith (2002) opredeljujeta e-odpadke kot široko vključujoče in naraščajoče elektronske naprave, ki imajo razpon od majhne do velike domače opreme (npr. hladilniki, klimatske naprave, mobilni aparati, radijski aparati, osebna elektronika), vse do računalnikov, ki so jih lastniki zavrgli. Organisation for Economic Co-operation and Development (2001) dodaja k različnim definicijam e-odpadkov tudi svoj termin, kjer opredeljuje e-odpadek kot katerokoli napravo, ki deluje na elektriko in je dosegla t. i. »end-of-life« fazo oziroma fazo zastarelosti oziroma iztek življenjske dobe.

V slovenskem pravnem sistemu je sprejeta definicija e-odpadkov z implementacijo direktiv[5] EU, in sicer 16. odstavek 3. člena Uredbe o odpadni električni in elektronski opremi (2015) določa, da »OEEO[6] je EEO[7], ki je odpadek[8] v skladu z zakonom, ki ureja varstvo okolja, vključno z vsemi sestavnimi deli, podsestavi in potrošnim materialom, ki je del proizvoda, ko se ta zavrže«.

Pravna regulacija e-odpadkov je tako na mednarodnem kot na državnem nivoju pomembna, saj je pomembno, da se zavedamo, da imajo ti odpadki dvojno vlogo. Prva vloga je vloga odpadka, ki ga je treba ustrezno reciklirati zaradi nevarnih delov, ki sestavljajo e-opremo in predstavljajo nevarnost človeku in naravi ter druga, ustrezna obdelava in zbiranje dragocenih kovin, ki jih vsebujejo e-odpadki, kateri so primerni za ponovno uporabo pri izdelavi nove e-opreme.

2.2 Toksična past e-odpadkov

E-odpadki predstavljajo tako naraščajoči problem kot tudi poslovno priložnosti, ki je čedalje bolj pomembna, saj glede na obseg e-odpadkov, ki je generiran, vsebuje tako nevarne/strupene kot dragocene materiale. Za reševanje problema z e-odpadki je na začetku treba razumeti sestavo e-odpadkov, ki je ključnega pomena za pravilno ravnanje z e-odpadki. Jaiswal, Samuel, Patel in Kumar (2015) dodajajo, da je za poznavanje sestavnih delov e-odpadkov posledično odvisna izbira ustrezna reciklažnega postopka in tehnike, s katero na okolju varen način recikliramo e-odpadke.

Widmer et al. (2005) ugotavljajo, da je frakcije v e-odpadkih, ki vsebujejo železo, baker, aluminij, zlato in ostale kovine, več kot 60 %, medtem ko je

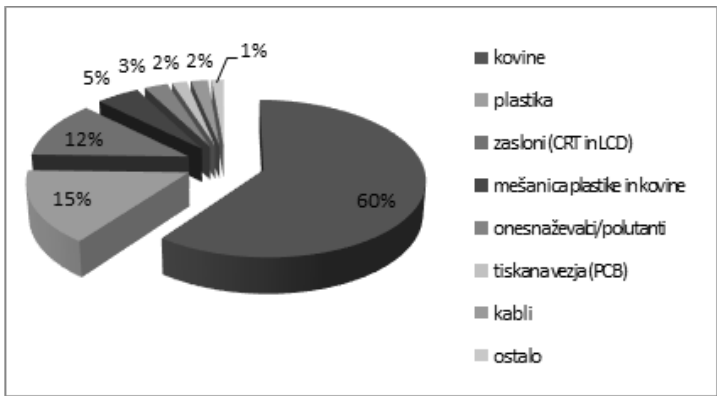
5 *Pravni pregled urejanja področja e-odpadkov je predstavljen v poglavju 2.4.*

6 *V slovenskem pravnem redu se za termin e-odpadek uporablja kratica OEEO, ki pomeni odpadna električna in elektronska oprema.*

7 *Kratica EEO pomeni električna in elektronska oprema, ki je definirana v 6. odstavku 3. člena Uredbe o odpadni električni in elektronski opremi (2015), ki določa: »EEO je oprema, ki za svoje pravilno delovanje potrebuje električni tok ali elektromagnetno polje, in oprema za proizvodnjo, prenos in merjenje toka in polj, ter je oblikovana za uporabo za napetostni razred, ki ne presega 1000 voltov za izmenični tok in 1500 voltov za enosmerni tok«.*

8 *V Zakonu o varstvu okolja (ZVO-1, 2016) je odpadek definiran kot snov ali predmet, ki ga imetnik zavrže, namerava zavreči ali mora zavreči. Gre za vse, kar se v gospodinjstvu, vsakdanjem življenju izloči, zavrže kot neuporabno ali kar se pri predelavi, obdelavi česa odstrani, izloči kot neuporabno za prvotni namen.*

onesnaževalcev (oziroma polutantov) približno 2,70 %. Slika 1 prikazuje najbolj pogosto sestavo komponent, ki jih vsebujejo e-odpadki.



Slika 1: Prikaz tipične frakcije v e-odpadku (vir: Widmer et al., 2005).

Slika 1 prikazuje tipično sestavo frakcije e-odpadkov, in sicer kar 60 % predstavljajo kovine, 15 % plastika, 12 % zasloni (CRT in LCD), 5 % je mešanica plastike in kovine, 3 % so nevarne snovi (onesnaževalci/polutanti, ki so v nadaljevanju prispevka predstavljeni), 2 % so tiskana vezja, 2 % predstavljajo kabli in preostali odstotek predstavljajo drugi elementi in materiali. Tipična sestava frakcij e-odpadkov ni vedno enaka, saj Robinson (2009) izpostavlja, da kemijska sestava v e-odpadkih različno variira glede na vrsto[9] e-odpadka. Težji e-odpadki, kot je npr. pomivalni stroj, vsebujejo več jekla in manj okolju nevarnih sestavnih delov v primerjavi s prenosnim računalnikom, ki je lažji in vsebuje manj kovine, vendar večje število nevarnih sestavnih delov (npr. več bromiranih zaviralcev gorenja in težkih kovin).

Puckett in Smith (2002) opisujeta nevarne sestavne dele, ki se nahajajo v e-odpadkih, in kako vplivajo na človeka in naravo. V posameznem e-odpadku (največ v računalniku in pripadajočih komponentah, v monitorju kot tudi v hladilniku s hladilno tekočino) se nahaja več kot 60 različnih kemičnih elementov (Grant et al., 2013), ki so nevarni ne samo človeku, ampak tudi celotnemu ekosistemu.

Puckett in Smith (2002) navajata, da e-odpadki vsebujejo toksične sestavne dele, ki vsebujejo svinec[10], kadmij, živo srebro[11], šestvalentni krom/ IV krom[12],

9 *Težji e-odpadki, kot je npr. pomivalni stroj, vsebujejo več jekla in manj okolju nevarnih sestavnih delov v primerjavi s prenosnim računalnikom, ki je lažji in vsebuje manj kovine, vendar večje število nevarnih sestavnih delov (npr. več bromiranih zaviralcev gorenja in težkih kovin).*

10 *Največ svinca je v računalnikih, in sicer v matičnih ploščah. Svinec poškoduje centralni in periferni živčni sistem, krvni sistem, jetra in reproduktivne organe pri človeku. Prav tako ima škodljiv učinek na okolje, živali in ostale mikroorganizme.*

11 *Živo srebro lahko povzroči škodo tako različnim notranjim organom človeka kot tudi fetusu. Okoli 22 % letne svetovne porabe živega srebra se uporabi v e-opremi (termostati, senzorji, svetilke, mobilnih telefonih, baterije ipd.).*

12 *Šestvalentni krom/IV krom – uporablja se kot zaščita pred korozijo v neobdelanih pocinkanih in jeklenih ploščah in kot utrjevalec jeklenih ohišij. Zlahka prehaja skozi kožo ter poškoduje DNK in je ekstremno toksičen za naravo.*

barij, berilij, plastiko[13], bromirane zaviralce ognja[14] ipd. Vsem kemijskim elementom, ki so del sestavnih delov e-odpadkov, je skupno to, da povzročajo resno kontaminacijo zraka, prahu, zemlje in vode (Chen, Dietrich, Huoin in Ho, 2011; Grant et al. 2013; Ogunseitan, Samphores, Nixon in Shapiro, 2009; Schmidt, 2006; Tang et al., 2010; Wong et al., 2007) predvsem v tistih državah, ki so uvoznice e-odpadkov (države v razvoju in države tretjega sveta) (Robinson, 2009). Tam ljudje neustrezno ravnajo z e-odpadki, ki vsebujejo nevarne sestavne dele, z namenom pridobivanja dragocenih kovin, kot so zlato, srebro, baker, cink, železo, kositer in ostale kovine, ki prinašajo zaslužek (Huo et al. 2007). Raziskovalci Schluep et al. (2009) ugotavljajo, da se v eni toni mobilnih telefonov (brez baterije) nahaja 3,5 kg zlata, 340 g srebra, 14 g paladija in 130 kg bakra. Na prvi pogled so količine majhne, vendar se je v letu 2007 prodalo 1,2 bilijona mobilnih telefonov, kar vodi v ogromno povpraševanje po dragocenih kovinah (Schluep et al., 2009).

E-odpadki predstavljajo past v obliki zaslužka, ki je močna motivacija za posameznika, ki z neprimerno opremo in metodo dela reciklira e-odpadke z namenom pridobivanja dragocenih kovin. Ker se večina e-odpadkov izvozi v države v razvoju in v tretje države, kjer večina prebivalstva izhaja iz nižjega sloja prebivalstva, posamezniki tvegajo svoje zdravje za zaslužek in hkrati omogočajo ekološko katastrofo.

2.3 Ravnanje z e-odpadki

Način ravnanja z e-odpadki je zelo pomemben, saj se na okolju varen način reciklira zelo malo e-odpadkov v primerjavi z razvojem informacijske tehnologije, ki neprestano razvija novosti na področju e-opreme. Lundgren (2012) ugotavlja, da se v Kitajsko in v nekatere države Afrike uvozi kar do 80 % e-odpadkov na globalnem nivoju. V teh državah je želja po dobičku visoka in se z namenom zniževanja morebitnih stroškov z recikliranjem, posamezniki odločajo za praktične, enostavne in preproste metode ravnanja z e-odpadki. Raziskovalci Huo et al. (2007) opisujejo neustrezne metode ravnanje z odpadki v mestu Guiyu[15] z namenom pridobivanja dragocenih kovin. Neustrezno ravnanje z e-odpadki pomeni uporabo primitivnih oblik recikliranja, kot je demontaža starih e-odpadkov z uporabo kladiva, električnega svedra in izvijača na posamične komponente, kot so monitor, trdi disk, žice, kabli/vodniki, tiskana vezja, tranzistorji, napajalniki, baterije, plastična in kovinska ohišja, ki jih prodajo z namenom ponovne uporabe ali jih reciklirajo v drugih delavnicah. Recikliranje tiskanega vezja računalnikov in ostale večje opreme poteka tako, da jih segrevajo in talijo nad ognjem z namenom pridobivanja dragocenih električnih komponent, kot so diode, upori in mikročipi. Tiskano vezje mobilnih telefonov in ostalih manjših naprav se razgradi

13 *Plastika predstavlja 6,26 kilograma v posamičnem računalniku (zaščita kablov, ohišje računalnika ipd.). PVC se uporablja zaradi lastnosti zaustavljanja gorenja, kljub temu pa PVC vsebuje klor, ki ob gorenju sprošča dioksine, ki so škodljivi ob vdihavanju ter lahko vodijo do zastrupitve in smrti.*

14 *Bromirani zaviralci gorenja (krajše BFR) – uporabljeni so v plastičnih ohišjih e-opreme z namenom preprečevanja vnetljivosti, ob neustreznem ravnanju z e-odpadkom so izredno strupeni.*

15 *Guiyu je mesto v Kitajski v provinci Guangdong, kjer se več kot 80 % prebivalstva ukvarja z recikliranjem e-odpadkov. Glede na statistike je letno recikliranih 138.000 ton plastike, 258.000 ton kovine in 6,7 ton dragocenih kovin (5 ton zlata, 1 tona srebra in 0,7 tone paladija) (Zhang, 2007).*

z elektrotermično napravo, ki ogroža človekovo življenje in naravo. Mikročipe in posamične dele računalnika potopijo v kadi s kislino in izločijo dragocene kovine, kot sta zlato in paladij, preostali kislinski del odpadka pa zavržejo na bližnje travnike in v potoke. Kable/vodnike in žice slečejo ali pa jih stalijo z namenom pridobivanja kovin. Plastiko (PVC) ločijo po trdoti, barvi in videzu. Plastične ostanke, ki jih ne razvrstijo, zažgejo na prostem. Drug način razvrščanja plastike je ločevanje plastike po teži. Te dajo v keramične posode s slanico, nato to posušijo na pločnikih ali cesti. Za namene recikliranja vržejo vse odpadne delce v stroj za mletje, ki zmelje plastiko v majhne koščke. Transformatorje, polnilce, baterije in katodne cevi ločijo in jih razbijejo s kladivom z namenom recikliranja kovin (baker, jeklo, srebro, aluminij) in predelave v surovi material. Takšen način obdelave in predelave e-odpadkov z namenom pridobivanja redkih in dragocenih kovin je skrajno škodljiv za človeka in naravo. Evropska unija se je na nivoju vseh držav članic soočila s to problematiko ter postavila prve okvire za nadzor in ustrezno ravnanje z e-odpadki.

Delavci, ki na primitivni način pridobivajo dragocene kovine, so predvsem otroci in ženske. Neposredno ravnanje z e-odpadki škoduje njihovemu zdravju in ima posledično tudi okoljski negativni vpliv. Interpol (2009) ugotavlja, da je na svetu zgolj pet primerno opremljenih talilnih tovarn za baker in dragocene kovine, ki proizvajajo minimalno vrednost dioksina v ozračje in manj kot 20 primernih talilnih tovarn za CRT steklene zaslone. Če primerjamo podatke o proizvedenih skorajšnjih 42 tonah e-odpadkov v letu 2014 (Baldé et al., 2015b), ugotovimo, da je na okolju varen način ravnanja z e-odpadki težko izvedljiv in se bo posledično nezakoniti izvoz v te države še naprej izvajal. Z namenom omejevanja naraščajočega nezakonitega izvoza e-odpadkov so se predstavniki EU zavzeli za urejanje področja e-odpadkov z direktivami in mednarodnimi konvencijami.

2.4 Mednarodni predpisi, ki urejajo tranzit z e-odpadki

Posameznikova temeljna človekova pravica je dostop do čistega zraka, čiste vode in zemlje oziroma okolja. Na področju e-odpadkov ima velika večina dostop do teh pravic, razen prebivalci v državah v razvoju in v tretjih državah, kjer so prisiljeni poleg neprimernega recikliranja e-odpadkov tudi živeti neposredno v krajih, kjer delajo, saj si tako minimalizirajo stroške prevoza in bivanja. Rešitev, ki bi omejila nezakoniti izvoz e-odpadkov, predstavlja Baselska konvencija o čezmejnem nadzorovanju gibanja nevarnih odpadkov in njihovega odlaganja (Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and their Disposal: Protocol on liability and compensation for damage resulting from transboundary movements of hazardous wastes and their disposal, 1989).

Baselska konvencija ima do leta 2016[16] že 184 držav članic, ki so ratificirale Baselsko konvencijo, brez Združenih držav Amerike[17], ki se še vedno izmika

16 *Podatki o številu ratifikacij so pridobljeni na uradni internetni strani Baselske konvencije (Basel Convention, 2016).*

17 *V letu 2014 so bile Združene države Amerike največji proizvajalec e-odpadkov in to kar 7,1 milijona ton (Baldé et al., 2015a).*

podpisu (Basel Convention, 2011). Baselska konvencija je ena izmed redkih sporazumov, ki opredeljuje nezakonito aktivnost trgovine in prometa z nevarnimi odpadki kot kaznivo dejanje, pri čemer določa, da gre za nezakonit promet z nevarnimi odpadki v primeru, ko pride do prehoda nevarnih odpadkov čez mejo brez vednosti[18] države, v katero se je uvozil odpadek, ali ni pristanka države za uvoz, ali pa je bil pristanek države dosežen s ponarejanjem dokumentov ali goljufije, ali pa je izvoznik namerno odvrgel/odložil nevarne odpadke v določeno državo in kršil načela te konvencije (Rucevska et al., 2015). Leta 1995 je bil na tretji konferenci pogodbenic (COP-3) sprejet amandma h konvenciji (t. i. Basel Ban ali Baselska prepoved), ki na splošno prepoveduje izvoz iz držav OECD, EU in Liechtensteina v države, ki niso članice OECD, vendar še do leta 2015 ni začel veljati (Mitsilegas et al., 2015; Rucevska et al., 2015).

Poleg krovne Baselske konvencije so nastale tudi regionalne konvencije,[19] kot sta Bamako konvencija (Bamako Convention, 1991), ki je nastala na podlagi združenja afriških držav, ki nasprotujejo nezakonitemu uvozu e-odpadkov, in Waigani konvencija (Waigani Convention, 1995), ki zajema države na južnem delu Pacifika z namenom dodatne regulacije in nadzora nad pošiljkami odpadkov ter preprečevanja nezakonitega uvoza e-odpadkov v te države.

Poleg Baselske konvencije ima pomembno vlogo tudi Rotterdamska konvencija (Rotterdam Convention on the Prior Informed Consent Procedure for Certain Hazardous Chemicals and Pesticides in International Trade, 1998), ki govori o postopku soglasja po predhodnem obveščanju za določene nevarne kemikalije in pesticide v mednarodni trgovini, saj se članice EU zavedajo, da odpadki vsebujejo nevarne kemikalije, in morajo ob izvozu predhodno obvestiti državo uvoznico, kateri lahko šele po odobrenem potrdilu uvozijo nevarne snovi. Naslednja pomembna konvencija je Stockholmska konvencija (Stockholm Convention, 2001), katere glavni cilj je zaščita zdravja ljudi in okolja, in sicer prepoveduje proizvodnjo, uporabo, uvoz in izvoz kemikalij, ki jih določa s seznamom nevarnih kemikalij, ki so del e-odpadkov.

Na področju EU so se od leta 2003 dalje sprejemale direktive, ki zavezujejo države članice, da morajo besedilo direktiv implementirati v svoje pravne akte.

2.5 Slovenski predpisi, ki urejajo področje e-odpadkov

Slovenija kot država članica EU ureja področje e-odpadkov z implementacijo direktiv, in sicer je implementirala Direktivo 2002/96/EC (2003), katera ima prioritetni cilj preprečevanje nastanka ogromnih količin e-odpadkov ter pravilno

18 *Baselska konvencija z namenom zaščite držav v razvoju pred pošiljkami odpadkov vzpostavlja sistem soglasja po predhodnem dogovoru (angl. prior informed consent) z namenom zmanjševanja čezmejnega prehoda odpadkov (Mitsilegas, Fitzmaurice, Fasoli in Fajado, 2015). Državi daje pravico odklonitve uvoza odpadkov, če pa bi v primeru pisne potrditve sprejela odpadke, državo uvoznico obvezuje, da odpadke na okolju varen način razgradi (Mitsilegas et al., 2015).*

19 *Razlog za nastanek regionalnih sporazumov je obrambni mehanizem teh držav pred državami, kot so npr. Združene države Amerike, ki so velike proizvajalke e-odpadkov in niso podpisnice Baselske konvencije. Noben sporazum ali podpis konvencije jih ne obvezuje, da ne bi izvažale e-odpadke v države v razvoju in tretje države.*

ravnanje[20] z e-odpadki z namenom ponovne uporabe in/ali pravilnega uničenja e-odpadkov kot tudi Direktivo 2002/95/ES (2003), ki omejuje uporabe nekaterih nevarnih snovi[21] v e-opremi. Slednjo direktivo je nasledila Direktiva 2011/65/EC (2011), ki je prepoznavna tudi pod imenom RoHS Direktiva in je prepovedala uporabo svinca, kadmija, VI kroma, živega srebra, različnih oblik polikloriranih bifenilov v e-opremi, ki se daje v promet v EU po letu 2006.

Direktivo 2002/96/EC (2003) je prenovila Direktiva 2012/19/EC (2012) o e-odpadkih, z namenom izboljšanja okoljske učinkovitosti vseh subjektov, vključenih v življenjski krog e-opreme (proizvajalcev, distributerjev, potrošnikov) s poudarkom na načelu odgovornosti proizvajalca, saj predstavljajo kompleksen problem uspešnosti recikliranja e-odpadkov prav različne nacionalne politike.

Slovenija je sledila implementaciji direktiv postopoma, in sicer je sprejela več pravilnikov, ki so urejevali področje e-odpadkov. Kronološko je sprejela Pravilnik o ravnanju z odpadno električno in elektronsko opremo (2004), Pravilnik o omejevanju uporabe določenih nevarnih snovi v električni in elektronski opremi (2009) in Pravilnik o omejevanju uporabe določenih nevarnih snovi v električni in elektronski opremi (2012). V letu 2015 pa je Slovenija sprejela Uredbo o odpadni električni in elektronski opremi (2015).

Uredba o odpadni električni in elektronski opremi (2015) je pomembna zaradi implementiranih ciljev Direktive 2012/19/EC (2012), in sicer je direktiva uvedla ambiciozen cilj zbiranja e-odpadkov: cilj prvotnih 4 kg zbranih e-odpadkov iz gospodinjstev letno na prebivalca je spremenila v cilj, določen glede na količine dane e-opreme na trg v preteklih letih. Postopno morajo države članice v letih od 2016 do 2021 letno zbrati količino e-odpadkov, ki znaša od 45 do 65 % na trg dane e-opreme v preteklih treh letih. Prav tako se za 5 % zvišujejo predpisani deleži ponovne uporabe, recikliranja in predelave za posamezne razrede e-opreme. Poudarja tudi pripravo e-odpadkov za ponovno uporabo, ki je obveznost proizvajalca, da e-odpadke prevzame (načelo razširjene odgovornosti proizvajalca[22]), prav tako pa se morajo vsi proizvajalci ustrezno registrirati v državah članicah EU. Izpostavljen je tudi ukrep nad večjim nadzorom pošiljk rabljene e-opreme, in sicer se za preprečevanje prekrivanja izvoza e-odpadkov v nezakonito obdelavo v tretje države kot izvoza rabljene e-opreme določajo pravila za pošiljanje pošiljk rabljene e-opreme oziroma merila za razlikovanje med pošiljkami rabljene e-opreme in e-odpadkov.

Ukrep večjega nadzora pomeni izziv za posamezno državo, saj mora poskrbeti, da se e-odpadki, ki nastanejo znotraj države, kot tudi e-odpadki, ki se dnevno transportirajo znotraj meja, ustrezno nadzorujejo in dokumentirajo.

20 *Med drugim direktiva določa tudi stopnjo ločenega zbiranja e-odpadkov, ki naj bi jo članice EU dosegale, in sicer naj bi do konca leta 2006 ločeno zbrale vsaj štiri kilograme e-odpadkov iz zasebnega gospodinjstva na prebivalca na leto (Direktiva 2002/96/EC, 2003: 4. čl., 5. točka).*

21 *Nevarne snovi oziroma kemijske elemente, ki se nahajajo v e-odpadkih, smo opisali v podpoglavju 2.3.*

22 *V Sloveniji se lahko načelo razširjene odgovornosti proizvajalca, ki je obveznost vsakega proizvajalca, izpolnjuje posamezno ali skupinsko, kar določa Uredba o odpadni električni in elektronski opremi (2015). V praksi pa se to načelo izvaja v obliki sistemov zbiranja e-odpadkov (uradno so v Sloveniji registrirana štiri podjetja, in sicer Zeos d. o. o., Interseroh d. o. o., Slopak d. o. o. in Trigana d. o. o.).*

3 IZZIVI, KI JIH PREDSTAVLJAJO E-ODPADKI

Izzivi, ki jih predstavljajo e-odpadki, so kompleksne narave, ki ima mednarodne razsežnosti. Nadzor in dokumentiranje uvoza in izvoza kot tudi zbiranje in ustrezno recikliranje e-odpadkov ni odvisno samo od posamezne države, ampak je problem, ki ga morajo reševati vse države. V Sloveniji tako Program ravnanja z odpadki in program preprečevanja odpadkov Republike Slovenije (Ministrstvo za okolje in prostor, 2015) kot revizija Računskega sodišča RS (2013) ugotavljata, da prihaja do neskladja med poročili, ki jih izdajajo nosilci skupinskih shem o predelavi e-odpadkov, in sporočanimi podatki v statistični evidenci o predelavi odpadkov. Kot vzrok neskladja med poročili Program ravnanja z odpadki in program preprečevanja odpadkov Republike Slovenije (Ministrstvo za okolje in prostor, 2015) navaja tehnično nadgradnjo opreme, predelavo opreme, odmetavanje e-odpadkov v mešane komunalne odpadke in tudi izvoz[23] v tujino in neposredno prodajo drugim osebam. Računsko sodišče RS (2013) pa ugotavlja dodatno neskladje med podatki o uvozu in izvozu odpadkov držav izvoznic in držav uvoznic.

Nadalje je izziv za področje e-odpadkov spoštovanje pravnih aktov. Če posamezna država ne spoštuje mednarodnih sporazumov (ali ni podpisnica) in ne sprejme določb v svoj pravni sistem, omogoča prost pretok e-odpadkov. Slovenija sicer ni neposredno omogočala prostega pretoka e-odpadkov, saj je sprejela različne pravilnike za urejanje področja e-odpadkov, vendar ni upoštevala rokov za prenos določb direktiv v nacionalno zakonodajo. Neposlušnost Slovenije pri zadnji Direktivi 2012/19/EC (2012) je trajala tako dolgo, da je morala Evropska komisija [EK] tožiti Slovenijo pred Sodiščem EU. EK je aprila 2015 Sodišču predlagala, da se Sloveniji naloži denarno kazen v višini 8.408,4 evrov za vsak dan, dokler ne bo uspešno ratificirana nova direktiva v zakonodaji (European Commission, 2015). Po tožbi EK je Slovenija sprejela Uredbo o odpadni električni in elektronski opremi (2015) julija 2015 ter se tako izognila plačilu denarne kazni za neupoštevanje evropske zakonodaje. Vendar Slovenija ni bila edina država, podobno se je dogajalo tudi s Poljsko.

Poslušnost držav do mednarodnih sporazumov in konvencij je zagotovo eden izmed izzivov, ki ga morajo predstavniki držav, kot vplivni in pomembni ljudje, prvi spoštovati in upoštevati, saj so vzor preostalim ljudem. Vendar se glede na ugotovitve, da je v postopku ravnanja z e-odpadki vpletena ne samo organizirana kriminalna skupina, ampak tudi koruptivni sloj beloovratnikov (Interpol, 2009; Ormond et al., 2012), se ideja o pravičnih in moralno odgovornih ljudeh na zahtevnih položajih hitro podre. Kot dodaja Bučar-Ručman (2009: 123), da »velike korporacije namenjajo veliko denarja za lobiranje za sprejemanje ustrezne zakonodaje in (de)regulacijskih ukrepov, ki zagotavljajo nizke okoljevarstvene standarde. Na račun onesnaževanja, degradacije in ogrožanja okolja, živali in ljudi se privarčuje denar in poveča dobiček«. Rucevska et al. (2015) predlagajo, da bi se lahko problematično področje akterjev, ki so vključeni v verigo z e-odpadki, lažje razkrivalo z učinkovito mrežo na nacionalnem in mednarodnem nivoju.

23 *Podatki za Slovenijo prikazujejo, da Slovenija predela malo več kot 50 % e-odpadkov, preostale e-odpadke izvozi v tujino. Slovenija glede na podatke ne uvaža e-odpadkov (Ministrstvo za okolje in prostor, 2015).*

Velik izziv, ki ga predstavljajo e-odpadki, je primerno kaznovanje za storjeno dejanje – ekološka kriminaliteta. V Veliki Britaniji se je šele leta 2014 zaključil prvi primer, kjer je bil posameznik obsojen na zaporno kazen (16 mesecev) za kaznivo dejanje nezakonite trgovine z e-odpadki (Rucevska et al., 2015). Sodba v letu 2014 dokazuje, da se dokazovanje in sojenje akterjem nezakonite trgovine z e-odpadki težko dokaže. V primerjavi s sprejemanjem mednarodnih in evropskih zakonodajnih okvirov regulacije prometa e-odpadkov, ki se je razvijala v obdobju med letoma 1980 in 1990 kot posledica medijskega odkritja in objav o toksičnosti odpadkov na odlagališčih držav v razvoju (Bisschop, 2013).

Slovenija na področju e-odpadkov deluje v okviru policije, carine in inšpekcije. Pri pregledu Načrta dela Inšpektorat Republike Slovenije za okolje in prostor za leto 2016 (Ministrstvo za okolje in prostor, Inšpektorat Republike Slovenije za okolje in prostor [IRSOP], 2016a) je v tabeli prioritet umeščeno področje nadzora nad ravnanjem z e-odpadki kot II. prioriteta, kar pomeni, da ni najbolj pomembno področje inšpekcijskega nadzora. V nadaljevanju pa med kriterije tveganja inšpekcijskih zavezancev pod I. prioriteto umešča družbe, ki ravnajo z e-odpadki, pri katerih mora potekati redni letni inšpekcijski nadzor nad zavezanci najmanj enkrat letno. Vse prispele prijave, povezane z zavezanci, se obravnavajo prioritetno (IRSOP, 2016a). V nadaljevanju obravnavajo tudi aktivnosti, ki jih bodo nadaljevali iz leta 2015 v letu 2016 na področju nadzora čezmejnega pošiljanja odpadkov (IRSOP, 2016a). V letu 2015 so opravili 4.945 nadzorov nad ravnanjem z odpadki, izrekli 1.028 inšpekcijskih ukrepov ter izvedli 192 prekrškovnih postopkov. To predstavlja okoli 50 % vseh kršitev, ki jih IRSOP obravnava na letni ravni (IRSOP, 2016b). Dotično za problematiko e-odpadkov v letu 2015 IRSOP ne navaja podatkov[24]. Eman in Franca (2013) opozarjata glede kriminalitete z e-odpadki na pomembno dejstvo in to je lega Slovenije, saj ima Slovenija Luko Koper kot edino slovensko tovorno pristanišče, skozi katero poteka čezmejno pošiljanje odpadkov in je zaradi ogromnih količin tovora, ki se ne more ustrezno pregledati, v prid kriminalnim združbam. Za slovensko delo uradnih organov na področju e-odpadkov je potrebna predvsem dodatna zaposlitev zaposlenih, ki bodo nadzirali nezakoniti tok in recikliranje e-odpadkov kot tudi premestitev iz nižjih prioritet dela na višje, saj se mora e-odpadke strožje nadzirati in tudi ustrezno kaznovati.

4 ZAKLJUČEK

Vpliv e-odpadkov je globalen, saj so skoraj vse države, kjer je e-oprema, udeležene v cikel ravnanja z e-odpadki. Države imajo lahko vlogo izvoznice, uvoznice ali zgolj vmesno fazo prehoda oziroma tranzita e-odpadkov. E-odpadki vplivajo na države tako pozitivno kot negativno, vendar so pozitivni[25] učinki v primerjavi

24 *Inšpekcija za okolje in naravo [ION] je v Poročilu o delu ION (Ministrstvo za kmetijstvo in okolje, 2012) izpostavila problematiko ravnanja z odpadki (kovinski kosovni odpadki, e-oprema, izrabljena motorna vozila) in tudi neustrezno ravnanje z odpadki, predvsem sežig odpadnih električnih kablov, predvsem v krajih, kjer so romska naselja. Nadalje so inšpektorji opravili pregled pri 28 zavezancih, ki so vpisani v evidenco proizvajalcev in pridobiteljev e-opreme, in niso odkrili nobene nepravilnosti.*

25 *Edini pozitivni učinek, ki skoraj ne spada v okvir pozitivnosti, je digitalni razvoj držav v razvoju, saj prejemajo ogromne količine e-odpadkov, ki so lahko popravljivi in funkcionalni.*

z negativnimi minimalni. Grožnja, ki jo predstavlja e-odpadek, je torej njegova nevarna sestava, ki povzroča ekološko kriminaliteto (onesnaževanje vode, zraka in zemlje ter rastlinstva in živali), prav tako tudi negativno vpliva na človeka, ki je v neposrednem stiku z e-odpadki. Zdravstvene težave ter v veliki večini prezgodnja smrt predvsem žensk in otrok so toksična kazen za neustrezno recikliranje z e-odpadki. Zaradi zbiranja dragocenih kovin v državah v razvoju in v tretjih državah trpi tudi ekonomija držav izvoznic. Ogromne ekonomske (zaposlovanje delavcev) in finančne izgube trpijo reciklažne industrije, saj kot že predhodno povedano, je primernih reciklažnih podjetij malo, hkrati pa je postopek reciklaže zelo drag. Slovenija nima ustreznega reciklažnega postopka in opreme, da bi e-odpadke na okolju varen način reciklirala. Nosilci skupinskih shem za zbiranje, obdelavo in predelavo e-odpadkov večino e-odpadkov ločeno sortirajo in delno razstavijo ter izvozijo v tujino (predvsem v sosednjo državo, Avstrijo). Kljub urejenemu sistemu navzven in na papirjih žal dejanskega uradnega stanja o količinah nezakonitega izvoza nimamo.

V Sloveniji se v zadnjem obdobju pojavlja nešteto akcij, ki jih organizirajo različni nosilci shem v sodelovanju s komunalnimi podjetji z namenom ustreznega recikliranja starih e-odpadkov, saj lahko s tem dejanjem vsak Slovenec prispeva k čistejšemu okolju. Namen akcije je narejen v dobrem duhu in želji po boljšem svetu, v katerem živimo, saj statistike prikazujejo podatke, da ima velika večina ljudi v svojem domu še vedno staro, (ne)uporabno e-opremo, ki je skrita v kleti ali na podstrešju. Le-to moramo predati ljudem, ki so primerno usposobljeni za ravnanje z e-odpadki. Večina akcij torej temelji na motivaciji posameznika, da odgovorno ravna do okolja in ločuje odpadke. Ob zaključku akcij organizatorji skoraj nikoli ne razkrijejo podatkov, razen o teži zbrane količine, o postopku recikliranja ter o dobičku, ki ga dobijo z dragocenimi kovinami iz recikliranih e-odpadkov. Rucevska et al. (2015) izpostavljajo podoben primer, kot so dobrodelne organizacije, ki delujejo na podoben način kot akcije zbiranja stare e-opreme, s to razliko, da pri dobrodelnih organizacijah druge institucije zbirajo staro e-opremo od ljudi in v zameno za staro e-opremo nakažejo denar. Ponovno pridemo do problematike pomanjkljivih podatkov glede recikliranja zbranih e-odpadkov, lahko zgolj predvidevamo in sumimo, da so ti odpadki že na poti v države v razvoju in tretje države. Institucije torej zaslužijo dvojno, prvič z brezplačno pridobitvijo stare e-opreme in drugič, ko ljudje, ki se nezakonito ukvarjajo s preprodajo in izvozom e-odpadkov v tretje države, odkupijo e-odpadke z namenom prodaje končnim osebam v ciljnih državah uvoza e-odpadkov.

Problematika e-odpadkov je sestavljena predvsem iz nevarnih snovi v e-odpadkih ter akterjev, ki so vključeni v nezakonite posle preprodaje in izvoza/uvoza e-odpadkov v končne destinacije, kjer se e-odpadki dokončno reciklirajo. V prvem delu problematike bi morali pri nevarnih snoveh in kemičnih elementih, ki jih vsebujejo e-odpadki, še bolj zaostriti konvencije in direktive o prepovedi nevarnih snovi v e-opremi. Tehnologija se razvija z veliko hitrostjo in bi lahko hitro našli nadomestne, okolju varne snovi, ki bi opravljale enako funkcijo kot nevarne snovi v e-opremi. Nekoliko težje pa je reševati ekološko kriminaliteto, ki vključuje organizirane kriminalitetne združbe kot predstavnike institucij in firm, ki se ukvarjajo z nezakonitim poslovanjem. Storjena kazniva dejanja so težko dokazljiva

in postopek sojenja je dolgotrajen. Veliko število akterjev je posredno (posameznik v svojem podjetju pripravi dokumentacijo, ki temelji na goljufiji in ponarejanju dokumentacije o e-odpadkih, ki se nahajajo v posamezni pošiljki) in neposredno (poznamo t. i. »waste tourists« oziroma turiste, ki odkupujejo e-odpadke od vrat do vrat, nadalje se neposredno ukvarjajo z e-odpadki prevozniki in končni akterji, ki se ukvarjajo z recikliranjem idr.) vključenih v verigo z e-odpadki, kar posledično otežuje dokazovanje storitve kaznivega dejanja ekološke kriminalitete in kaznovanje le-teh akterjev. Pristop podpisa mednarodnih sporazumov in implementacije direktiv za vse države bi bil pomemben korak o omejevanju kriminalitete z e-odpadki.

Ne nazadnje bi morala vsaka država poskrbeti za ustrezno beleženje in spremljanje postopkov recikliranja e-odpadkov. Prav tako bi se morali uradni organi (policija, carina in inšpekcija) še močneje povezati v različne mreže, kot so Europol, Interpol in Impel (Inšpekcija za okolje in naravo je včlanjena v organizacijo Impel, ki združuje evropske institucije za izvajanje in uveljavljanje zakonodaje na področju okolja) ter ažurno izmenjavati podatke o monitoringih in medsebojno izmenjati dobre prakse dela.

UPORABLJENI VIRI

Baldé, C. P., Wang, F., Kuehr, R. in Huisman, J. (2015a). *The global e-waste monitor – 2014*. Bonn: United Nations University, IAS – SCYCLE. Pridobljeno na https://i.unu.edu/media/unu.edu/news/52624/UNU-1stGlobal-E-Waste-Monitor-2014-small.pdf

Baldé, C. P., Kuehr, R., Blumenthal, S., Grill, F. S., Kern, M., Micheli, P. et al. (2015b). *E-waste statistics: Guidelines on classifications, reporting and indicators*. Bonn: United Nations University, IAS – SCYCLE. Pridobljeno na http://i.unu.edu/media/ias.unu.edu-en/project/2238/E-waste-Guidelines_Partnership_2015.pdf

Bamako Convention. (1991). *Bamako Convention on the ban of the import into Africa and the control of transboundary movement and management of hazardous waste within Africa*. Pridobljeno na http://www.unep.org/delc/Portals/119/Bamako%20Convention%20-%20Text%20English.pdf

Baird, J., Curry, R. in Cruz, P. (2014). An overview of waste crime, its characteristics and the vulnerability of the EU waste sector. *Waste Management & Research*, *32*(2), 97–105.

Basel Convention. (2011). *Overview*. Pridobljeno na http://www.basel.int/Implementation/TechnicalAssistance/Partnerships/ENFORCE/Overview/tabid/4526/Default.aspx

Basel Convention. (2016). *Parties to the Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and their Disposal.* Pridobljeno na http://www.basel.int/Countries/StatusofRatifications/PartiesSignatories/tabid/4499/Default.aspx#enote1

Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and their Disposal: Protocol on liability and compensation for damage resulting from transboundary movements of hazardous wastes and their disposal. (1989). Châte-

laine: Secretariat of the Basel Convention. Pridobljeno na http://www.basel.int/Portals/4/Basel%20Convention/docs/text/BaselConventionText-e.pdf

Bisschop, L. (2013). Is it all going to waste? Illegal transport of e-waste in a European trade hub. V R. White (ur.), *Transnational environmental crime* (str. 246–273). Burlington: Ashgate.

Bučar-Ručman, A. (2009). Okoljska kriminaliteta skozi pogled zelene kriminologije. *Revija za kriminalistiko in kriminologijo, 60*(2), 118–130.

Chen, A., Dietrich, K. N., Huo, X. in Ho, S. (2011). Developmental neurotoxicants in e-waste: An emerging health concern. *Environmental Health Perspectives, 119*(4), 431–438. Pridobljeno na http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3080922/

Direktiva 2002/95/ES Evropskega parlamenta in Sveta z dne 27. januarja 2003 o omejevanju uporabe nekaterih nevarnih snovi v električni in elektronski opremi. (2003). *Uradni list EU,* (L 037). Pridobljeno na http://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:32002L0095&from=EN

Direktiva 2002/96/EC Evropskega Parlamenta In Sveta z dne 27. januarja 2003 o odpadni električni in elektronski opremi (OEEO). (2003). *Uradni list EU,* (L 037). Pridobljeno na http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0096

Direktiva 2011/65/EC Evropskega parlamenta in Sveta o omejevanju uporabe nekaterih nevarnih snovi v električni in elektronski opremi. (2011). *Uradni list EU,* (L 174/88). Pridobljeno na https://www.gzs.si/pripone/RoHs%202011-65-ES.pdf

Direktiva 2012/19/EU Evropskega Parlamenta in Sveta o odpadni električni in elektronski opremi (OEEO). (2012). *Uradni list EU*, (L 197/38). Pridobljeno na http://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32012L0019

Eman, K. (2008). Uvod v fenomenološko analizo ekološke kriminalitete. *Varstvoslovje*, *10*(1), 220–239.

Eman, K. in Franca, B. (2013). Vpliv ekonomske krize na gibanje ekološke kriminalitete v Sloveniji. *Revija za kriminalistiko in kriminologijo, 64*(4), 358–370.

European Commission. (2015). *Environment: Commission takes POLAND and SLOVENIA to Court for e-waste failings.* Pridobljeno na http://europa.eu/rapid/press-release_IP-15-4875_en.htm

Europol. (2015). *Exploring tomorrow's organised crime*. Pridobljeno na https://www.europol.europa.eu/sites/default/files/edi/EuropolReportDigitalToC.html

Grant, K., Goldizen F. C., Sly, P. D., Brune M., Neira, M., van den Berg, M. et al. (2013). Health consequences of exposure to e-waste: A systematic review. *Lancet Glob Health, 1*(6), 350–361. Pridobljeno na http://www.ncbi.nlm.nih.gov/pubmed/25104600

Huo, X., Peng, L., Xu, X., Zheng, L., Qiu B., Qi, Z. et al. (2007). Elevated blood lead levels of children in Guiyu, an electronic waste recycling town in China. *Environmental Health Perspectives, 115*(7), 1113–1117.

Huisman, J., Botezatu, I., Herreras, L., Liddane, M., Hintsa, J., Luda di Cortemiglia, V. et al. (2015). *Countering WEEE illegal trade summary report*. Pridobljeno na http://www.cwitproject.eu/wp-content/uploads/2015/09/CWIT-Final-Report.pdf

Interpol. (2009). *Electronic waste and organized crime, assesing the links*. Lyon: Interpol.

Jaiswal, A., Samuel, C., S. Patel, B. in Kumar, M. (2015). Go green with WEEE: Eco-friendly approach for handling e-waste. *Procedia Computer Science*, *46*, 1317–1324.

Lundgren, K. (2012). *The global impact of e-waste: Addressing the challenge.* Geneva: Inernational Labour Office. Pridobljeno na http://www.ilo.org/wcmsp5/groups/public/@ed_dialogue/@sector/documents/publication/wcms_196105.pdf

Luther, L. (2010). *Managing electronic waste: Issues with exporting e-waste. Report prepared for members and committees of Congress*. Pridobljeno na https://fas.org/sgp/crs/misc/R40850.pdf

Ministrstvo za kmetijstvo in okolje. (2012). *Poročilo o delu inšpekcije za okolje in naravo v letu 2012*. Pridobljeno na http://www.iko.gov.si/fileadmin/iko.gov.si/pageuploads/ION/Porocila/POROCILO-O-DELU-INSPEKCIJE-ZA-OKOLJE-IN-NARAVO-2012.pdf

Ministrstvo za okolje in prostor. (2015). *Program ravnanja z odpadki in program preprečevanja odpadkov Republike Slovenije: osnutek.* Pridobljeno na http://www.mop.gov.si/fileadmin/mop.gov.si/pageuploads/osnutki/program_ravnanja_z_odpadki.pdf

Ministrstvo za okolje in prostor, Inšpektorat Republike Slovenije za okolje in prostor [IRSOP]. (2016a). *Načrt dela Inšpektorat Republike Slovenije za okolje in prostor za leto 2016.* Pridobljeno na http://www.iop.gov.si/fileadmin/iop.gov.si/pageuploads/5_O_INSPEKTORATU/Porocila_in_nacrti_dela/Letni_nacrt_dela_2016.pdf

Ministrstvo za okolje in prostor, Inšpektorat Republike Slovenije za okolje in prostor [IRSOP]. (2016b). *Poročilo o delu za leto 2015*. Pridobljeno na http://www.iop.gov.si/fileadmin/iop.gov.si/pageuploads/5_O_INSPEKTORATU/Porocila_in_nacrti_dela/Porocilo_IRSOP_2015.pdf

Mitsilegas, V., Fitzmaurice, M., Fasoli, E. in Fajado, T. (2015). *Analysis of international legal instruments relevant to fighting environmental crime:* S*tudy in the framework of the Efface project*. London: Queen Mary University of London. Pridobljeno na http://efface.eu/analysis-international-legal-instruments-relevant-fighting-environmental-crime

Ogunseitan, O. A., Samphores J. D. M., Nixon, H. in Shapiro, A. A. (2009). How much e-waste is there in US basements and attics? Results from a national survey. *Journal of Environmental Management, 90*(11), 3322–3331.

Organisation for Economic Co-operation and Development. (2001). *Extended producer responsibility: A guidance manual for governments*. Pridobljeno na http://www.oecd-ilibrary.org/environment/extended-producer-responsibility_9789264189867-en

Ormond, T., ten Brink, P., Dukalska, L., Göbel, K., Kollberg, P., Lindgren, M. et al. (2012). *Obrati za ravnanje z odpadki: priročnik: identifikacija in nadzor »začetnega dela verige« obratov za skladiščenje in obdelavo problematično za izvoz.* Pridobljeno na http://www.impel.eu/wp-content/uploads/2015/11/2012-18-Waste-Sites-Manual-Slovenian-translation1.pdf

Pravilnik o ravnanju z odpadno električno in elektronsko opremo. (2004). *Uradni list RS,* (118/04).

Pravilnik o omejevanju uporabe določenih nevarnih snovi v električni in elektronski opremi. (2009). *Uradni list RS,* (87/09).

Pravilnik o omejevanju uporabe določenih nevarnih snovi v električni in elektronski opremi. (2012). *Uradni list RS,* (102/12).

Puckett J. in Smith, T. (2002). *Exporting harm: The high-tech trashing of Asia. Basel Action Network and Silicon Valley Toxics Coalition*. Pridobljeno na http://www.ban.org/Ewaste/technotrashfinalcomp.pdf

Računsko sodišče Republike Slovenije. (2013). *Revizijsko poročilo: Čezmejni promet z odpadki.* Pridobljeno na http://www.rs-rs.si/rsrs/rsrs.nsf/I/AA542E6DAAC48BF8C1257BEA00463C52

Robinson, B. H. (2009). E-waste: An assessment of global production and environmental impacts. *Science of The Total Environment, 408*(2), 183–191.

Rotterdam Convention on the Prior Informed Consent Procedure for Certain Hazardous Chemicals and Pesticides in International Trade: Texts and annexes. (1998). Geneva: UNEP. Pridobljeno na http://www.pic.int/TheConvention/Overview/TextoftheConvention/tabid/1048/language/en-US/Default.aspx

Rucevska, I., Nellemann, C., Isarin, N., Yang, W., Liu, N., Yu, K. et al. (2015). *Waste crime – waste risks: Gaps in meeting the global waste challenge: A UNEP rapid response assessment.* Nairobi; Arendal: United Nations Environment Programme and GRID-Arendal. Pridobljeno na http://www.unep.org/delc/Portals/119/publications/rra-wastecrime.pdf

Schluep, M., Hagelueken, C., Kuehr, R., Magalinic, F., Maurer, C., Meskers, C. et al. (2009). *Recycling from e-waste to resources*. Berlin: Oktoberdruck AG.

Schmidt, C. W. (2006). Unfair trade: E-waste in Africa. *Environmental Health Perspectives 114*(4), 232–235.

StEP. (2014). *Solving the E-waste problem (step) white paper: One global definition of e-waste*. Pridobljeno na http://www.step-initiative.org/files/step/_documents/StEP_WP_One%20Global%20Definition%20of%20E-waste_20140603_amended.pdf

Stockholm Convention. (2001). *Stockholm Convention on Persistent Organic Pollutants.* Pridobljeno na http://www.pops.int/documents/convtext/convtext_en.pdf

Tang, X., Shen, C., Shi, D., Cheema, S. A., Khan, M., Zhang, C. et al. (2010). Heavy metal and persistent organic compound contamination in soil from Wenling: An emerging e-waste recycling city in Taizhou area, China. *Journal of Hazardous Materials, 173*(1–3), 653–660.

Uredba o odpadni električni in elektronski opremi. (2015). *Uradni list RS,* (55/15).

United Nations Office on Drugs and Crime [UNODC]. (2013). *Transnational organized crime in East Asia and the Pacific.* Pridobljeno na https://www.unodc.org/toc/en/reports/TOCTA-EA-Pacific.html

Waigani Convention. (1995). *Convention to ban the importation into forum island countries of hazardous and radioactive wastes and to control the transboundary movement and management of hazardous wastes within the South Pacific Region*. Pridobljeno na https://sprep.org/attachments/Waigani_Convention.pdf

Widmer, R., Oswald-Krapf, H., Sinha-Khetriwalb, D., Schnellmann, M. in Böni, H. (2005). Global perspectives on e-waste. *Environmental Impact Assessment Review, 25*(5), 436–458.

White, R. (2013). Introduction. V R. White (ur.), *Transnational environmental crime* (str. xiii-xxix). Burlington: Ashgate.

Wong, M. H., Wu, S.C., Deng, W. J., Yu, X. Z., Luo, Q., Leung, A. O. W. et al. (2007). Export of toxic chemicals: A review of the case of uncontrolled electronic-waste recycling. *Environmental Pollution, 149*(2), 131–140.

Zakon o varstvu okolja (ZVO-1). (2016). *Uradni list RS*, (30/16).

Zhang, K. (2007). Rough times in Guiyu. *Recycling Magazine, 5.* Pridobljeno na http://archive.ban.org/library/Features/070500_rough_times_in_guiyu.html

O avtorjih:

Andreja Rožnik, doktorska študentka Fakultete za varnostne vede Univerze v Mariboru, kjer pripravlja doktorsko disertacijo na področju raziskovanja e-odpadkov. Njena področja zanimanja so električni in elektronski odpadki, situacijsko preprečevanje kriminalitete in ekološka kriminaliteta. E-pošta: andreja.roznik@gmail.com

Dr. Gorazd Meško, redni profesor za kriminologijo na Fakulteti za varnostne vede Univerze v Mariboru. Njegova področja raziskovanja so preprečevanje kriminalitete in zagotavljanje varnosti, legitimnost, strah pred kriminaliteto in ekološka kriminaliteta. E-pošta: gorazd.mesko@fvv.uni-mb.si

VARSTVOSLOVJE,
letn. 18
št. 3
str. 288–302

Varnostno testiranje fizičnega kripto-modula za navidezna zasebna omrežja

Anže Zaletel, Jaka Žužek, Lavra Horvat, Katja Zupan, Sara Železnik, Nina Goršič, Maruša Lipušček

Namen prispevka:

Namen prispevka je predstaviti projekt[1] varnostnega testiranja v razvoju in produkciji fizičnega kripto-modula, ki je nujno potrebno pred lansiranjem izdelka na trg. Delo na projektu je bilo usmerjeno v izdelek Code 1 Secure (v nadaljevanju VPN kripto-modul C1S), za katerega je bila narejena primerjava s sorodnimi izdelki, predlagane različne ergonomične oblike ter opisani postopki potrebnih testiranj izdelka za pridobitev certifikatov oz. za doseganje standardov.

Metode:

Uporabljena je bila deskriptivna metoda s pomočjo študije primarnih in sekundarnih virov. Za potrebe opisa orodij za avtomatizirano testiranje smo delovanje orodij preizkusili in opravili vzorčna testiranja.

Ugotovitve:

Testiranje programske opreme in njene združljivosti s šifrirnimi algoritmi predstavlja najzahtevnejši del testiranj. Ključno stičišče projekta je predstavljal kolaboracijski portal, preko katerega se je evidentiral in spremljal napredek dela. S preizkušanjem orodij za avtomatizacijo opravil je bilo ugotovljeno, da avtomatizirano testiranje prihrani veliko časa in denarja.

Omejitve/uporabnost raziskave:

Projektno delo je bilo ciljno naravnano na izdelek VPN kripto-modula C1S, zato se tudi ugotovitve navezujejo nanj. Kljub temu lahko ugotovitve apliciramo na sorodne izdelke.

Praktična uporabnost:

S primerjavo sorodnih izdelkov se pokažejo konkurenčne prednosti VPN kripto-modula C1S pred podobnimi izdelki na trgu ter možnosti za izboljšave.

1 *Projekt »Varnostna testiranja v razvoju in produkciji kripto-modula« je potekal pod okriljem javnega razpisa »Po kreativni poti do praktičnega znanja«, ki so ga financirali Javni sklad Republike Slovenije za razvoj kadrov in štipendije, Ministrstvo za izobraževanje, znanost in šport ter Evropska unija iz Evropskega socialnega sklada.*

Pri projektu sta kot vodji sodelovala dr. Igor Bernik s Fakultete za varnostne vede in Milan Bunjevac s podjetja Miška, d. o. o., ter mag. Boštjan Knap in Blaž Malneršič kot strokovna mentorja s podjetja Miška, d. o. o.

Pri projektu so kot izbrani študenti dodiplomskih in podiplomskih študijskih programov na Fakulteti za varnostne vede sodelovali Anže Zaletel, Jaka Žužek, Lavra Horvat, Katja Zupan, Nina Goršič, Sara Železnik, Maruša Lipušček, Tina Slavec, Nina Gašparut in Matic Volk.

Predlagane so različne ergonomične oblike izdelka glede na ciljne skupine kupcev. Opis možnih testiranj, ki so potrebna za VPN kripto-modul C1S, poda okvirno predstavo o obsegu preizkušanj slehernega tehnološkega izdelka.

Izvirnost/pomembnost prispevka:

Glede na povišan trend zlorab v kibernetskem prostoru je področje kibernetske varnosti, v katerega spada tudi VPN kripto-modul C1S, izrednega pomena. Za ustrezno delovanje kripto-modulov in doseganje pričakovanj uporabnikov je te naprave pomembno dobro testirati.

UDK: 004.056

Ključne besede: informacijska varnost, šifriranje podatkov, kripto-modul, testiranje, analiza trga

Security Testing of a Hardware Virtual Private Network Crypto Module

Purpose:

The purpose of the paper is to present security testing approach in the phase of development and production of a hardware crypto-module, which is indispensable before the product goes on the market. The project work was focused on the product Code 1 Secure (from here on VPN crypto module C1S) for which a comparison with other similar products was made, different ergonomically designed shapes were proposed and product's necessary testing to gain certificates or/and achieve certain standards was described.

Methods:

A descriptive method with the study of primary and secondary sources was used. For the purposes of showing how the automated testing tools work, several testing activities were made.

Findings:

Testing the software and software's compatibility with encryption algorithms poses the most difficult part of all the testing activities needed to be done. The collaborative web portal had a major role in keeping track and progress of the project's work. Testing some of the automated tools showed that their usage saves time and consequently money.

Research Limitations/Implications:

Because the project work was focused on the product VPN crypto module C1S, all the findings are linked to it. However, most of them could be applied to related products.

Practical Implications:

Comparison of similar products shows competitive edge of VPN crypto module C1S and points out potentials for improvements. There were some ergonomically designed shapes presented with the intention of targeting certain costumers. Description of potential testing needed for the C1S, gives a rough estimate of testing's scope of every technological product.

Originality/Value:

VPN crypto-module is a subject of cyber security which has a great importance in everyday life, because of the increased trend of abuses in cyberspace. For the proper functioning of the crypto-modules and meet the expectations of the users, these devices must be appropriately tested.

UDC: 004.056

Keywords: information security, encryption, crypto-module, testing, market analysis

1 UVOD

Vse oblike varnostnih groženj, prisotnih v kibernetskem prostoru, so v porastu in predstavljajo vedno večjo nevarnost za različne vrste informacij in informacijskih sistemov, pomembnih tako za države, organizacije, podjetja kot posameznika (PwC, 2014). Ena izmed rešitev za zagotavljanje večje varnosti in zaščite informacij, ki se izmenjujejo preko kibernetskega prostora, predstavlja uporaba različnih metod šifriranja podatkov in uporaba navideznega zasebnega omrežja (angl. *Virtual private network – VPN*), ki s pomočjo tunelskih protokolov (npr. L2TP/IPSec ali PPTP) (Microsoft, 2003) omogoča vzpostavitev šifrirane povezave med dvema točkama izmenjevanja podatkov preko kibernetskega prostora. S šifriranjem na nižjih nivojih ISO/OSI in TCP/IP protokol prenosa podatkov se uporabnik kibernetskega prostora zaščiti pred grožnjami, ki so prisotne na višjih nivojih (predvsem na aplikacijskem nivoju), in s tem zagotovi zaščito informacij pred nepooblaščenim dostopom (Senetas, 2013) ter posledično večjo zaupnost, celovitost in razpoložljivost informacij, ki predstavljajo ključne elemente CIA triade. CIA triada (angl. *Confidentiality, Integrity in Availability triad*) predstavlja tri najpomembnejše principe informacijske varnosti, ki bi morali biti zagotovljeni v vsakem varnem informacijskem sistemu (Dimov, 2013).

Kripto-moduli za navidezno zasebno omrežje predstavljajo visok nivo zaščite informacij, zaradi česar bi jih bilo smiselno uvajati tako v poslovno kot osebno okolje uporabnikov pri interakciji s kibernetskim prostorom. Kripto-moduli uporabljajo različne šifrirne algoritme za zaščito podatkov in informacij ter uporabniku nudijo možnost izbire med standardnimi šifrirnimi algoritmi (npr. AES, 3DES, RSA ...) ali namestitvijo manj standardnih šifrirnih načinov zaščite podatkov (npr. Blowfish, Serpent, ECC ...). Prednost uporabe fizičnih kripto-modulov za navidezno zasebno omrežje pred programskimi rešitvami je v njihovi zmožnosti zagotavljanja naključno izbranih šifrirnih ključev. Programske rešitve za šifriranje podatkov, uporabljajo psevdo naključno generiranje števil. To pomeni, da so naključno izbrana števila pravzaprav vnaprej določena z matematično formulo, medtem ko so resnično naključno generirana števila izbrana s pomočjo naključnih naravnih pojavov. Med omenjene naravne pojave sodijo fizični pojavi, kot so na primer atmosferski ali ostali šumi, ki se pojavijo ob vklopu kripto-modula (Haahr, 2015).

Kripto-moduli za navidezno zasebno omrežje predstavljajo varnostno rešitev za tako imenovano E2EE šifriranje (angl. *End to end encryption*). Ta uporabnikom

na preprost in transparenten način zagotovi varno prenašanje informacij v kibernetskem prostoru od izvora do prejemnika, tj. naprave, na katero je v tistem trenutku priklopljen kripto-modul za navidezno zasebno omrežje. Na takšen način se uporabniki zavarujejo pred izgubo informacij zaradi kibernetskih groženj, kot je na primer prisluškovanje na omrežju. Kripto-moduli za navidezno zasebno omrežje, ki dosledno upoštevajo standarde iz družine FIPS 140 ter pridobijo ustrezen certifikat, so primerni za uporabo tudi pri prenosu tajnih informacij. FIPS 140 so ameriški računalniški standardi, ki določajo zahteve za izdelavo fizičnih in programskih kripto-modulov (National Institute of Standards and Technology, 2016). Sledenje omenjenim standardom zagotavlja najvišjo stopnjo zaščite pred kibernetskimi grožnjami, zato so kripto-moduli za navidezno zasebno omrežje primerni za prenos vseh vrst zaupnih in tajnih podatkov preko kibernetskega prostora.

V nadaljevanju so predstavljene ključne ugotovitve skupnega študentskega projekta Fakultete za varnostne vede Univerze v Mariboru in podjetja Miška, d. o. o., z naslovom *Varnostna testiranja v razvoju in produkciji kripto-modula*. Ugotovitve se nanašajo tako na področje analize tveganj celotnega projekta, patentiranja in certificiranja kripto-modula, primerjave s sorodnimi kripto-moduli kot na testiranje programske in strojne opreme ter obrazložitve testnega scenarija primernega za poljuben kripto-modul za navidezno zasebno omrežje.

2 ANALIZA TVEGANJ

Za uspešno sodelovanje pri razvojnem projektu smo predhodno izvedli analizo tveganj njegove izvedbe. Zbrali smo številna možna tveganja in proučili načine zaščite. Izračun verjetnosti tveganj in težo posledic, če se tveganja uresničijo, prikazuje tabela 1.

Verjetnost/pogostost tveganj Teže posledic	A – Zelo pogosto	B – Pogosto	C – Redko	D – Izjemoma
1 – Zelo majhne posledice	A1-III.	B1-IV.	C1-IV.	D1-IV.
2 – Majhne posledice	A2-II.	B2-III.	C2-III.	D2-IV.
3 – Večje posledice	A3-I.	B3-II.	C3-II.	D3-III.
4 – Hude/težke posledice	A4-I.	B4-I.	C4-I.	D4-II.

Tabela 1: Metodologija ocenjevanja tveganj z nivoji tveganja (I. –IV.)

Po izbrani metodi (Slak, 2009) I. nivo tveganja zahteva – takojšnje ukrepanje, II. nivo – ukrepanje, III. nivo – spremljanje, IV. nivo – je sprejemljiv. Izračunali smo tudi verjetnost pregledanih tveganj ter težo posledic, če se ranljivosti uresničijo. Za specifična tveganja smo podali lastnike tveganj, tiste osebe, ki morajo poskrbeti, da se tveganja ne uresničijo, ter časovne roke, ki predstavljajo omejitev za dosego zaščite pred tveganji. Tveganja smo v nadaljevanju prve faze projekta razdelili na tri skupine:

- človeški viri,
- procesi in
- IT infrastruktura.

Zatem smo tveganja nadaljnje razvrstili na takšna področja, s katerimi smo lahko preverili verjetnost tveganj in njihovih posledic, obenem pa opredelili zaščito pred njimi na način, kot je razviden v tabeli 1. Za posamezna tveganja ugotavljamo, da zelo pogosto predstavljajo tveganje ob delu na projektu. Ta tveganja imajo v primeru uresničitve hude posledice, zato je bilo za njih treba predvideti takojšnje ukrepanje. Lastnika tveganj sta bila mentorja projekta, ki sta imela nadzor nad izvajanjem projekta, hkrati pa odgovornost, da ta poteka za vse sodelujoče ter po predvidenem načrtu. Postavili smo roke za vzpostavitev definiranih zaščit. Pogosto so bili roki že pred izvedbo prvih nalog, saj smo le preko zaščit, kot je spletni portal ali ustrezno delegiranje nalog na posamezne člane, lahko mirno in kakovostno izvajali projekt. Tak primer je izobraževanje študentov na področju testiranj izdelka in ostalih nalog, kjer je bilo izobraževanje potrebno. Rezultat analize tveganj je ugotovitev, da je komunikacija med udeleženci, najpomembnejši proces in hkrati zaščita za večji del tveganj. Do uresničitve konkretnih tveganj in grožen ni prišlo prav zaradi dobre priprave na projekt.

3 ANALIZA TRGA

Namen primerjave na trgu dostopnih primerljivih kripto-modulov je analiza konkurence in spoznanj o trgu. To nam je v pomoč pri pridobivanju podatkov in kasnejšem odločanju za zmanjševanje tveganja in razvijanje novih, dodatnih idej, ki podjetju ohranjajo konkurenčnost na trgu (Mesojedec et al., 2015). Pri primerjavi primerljivih kripto-modulov je končna ugotovitev ključnega pomena za razvoj novega produkta, ki mora ob prihodu na trg imeti konkurenčne prednosti in s tem možnosti za ohranitev na trgu. Poznavanje lastnosti načrtovanega kripto-modula in njegovega namena je izhodišče primerjave. Pomembno je vedeti, kaj primerjamo; lastnosti, ki jih ima podjetje v načrtu vgraditi v produkt z namenom, da bi z ugotovitvami pri analizi trga predvideli, ali so načrtovane lastnosti konkurenčne in dejansko pomembne za končnega uporabnika – skladno s tem se lastnosti prilagaja ali spreminja. Nekatere od lastnosti, ki so v primeru prenosljivega kripto-modula za navidezno zasebno omrežje pomembne:

- Prenosljivost (teža in dimenzije) – manjši in lažji je kripto-modul, boljša je prenosljivost.
- Število in vrsta priključkov – povezava kripto-modula na druge naprave; koliko naprav lahko naenkrat povežemo in kateri priključki so najpogostejši ter najbolj uporabni pri povezljivosti.
- Izmenjava ključev in šifrirni algoritmi – zelo pomembno z vidika varnosti, predvsem za boljši nadzor nad kripto-modulom.
- Avtentikacija – potrditev, da kripto-modul uporablja samo pooblaščena oseba.
- Ergonomičnost – ravnovesje med kakovostjo izdelka, njegovo učinkovitostjo, zapletenostjo in uporabnostjo kripto-modula.
- Certificiranje – certifikacijski znak na proizvodu potrošnikom, trgovcem in pristojnim organom zagotavlja, da je izdelek skladen z zahtevami veljavnih harmoniziranih standardov.

Glede na omenjene lastnosti primerjave in cen sorodnih kripto-modulov na trgu se določijo potrebne, in za uporabnika koristne, lastnosti za optimalno

izdelavo in končno rabo izdelka. To je vodilo za nadaljnje raziskave in razvoj konkurenčnega ter uporabnega kripto-modula. Primerjava različnih produktov je razvidna v tabeli 2 (primer primerjave petih produktov), kjer smo med izvajanjem projekta primerjali 29 različnih produktov z lastnostmi, ki so zapisane zgoraj.

IME PRODUKTA	Država izvora	CENA	Max prepustnost VPN	Max število VPN tunelov	Podprti protokoli varnih VPN	Šifrirni algoritmi	Dimenzije D x Š x V (mm)	Teža (g)
Miška d. o. o. + Beyond Semiconductor d. o. o.								
Code 1 Secure	Slovenija	/	470 Mbps	32	IPSec	AES128/192/256, lahko dodaš svoje	/	/
TUTUS								
Färist Micro A300	Švedska	1200 EUR	10 Mbps	/	lasten mehanizem (modificiran SSL)	AES256, 3DES, lahko dodaš svoje	115 x 77 x 27	150
Tiny Hardware Firewall								
Belisarius	ZDA	48 EUR	7 Mbps	1	SSL (OpenVPN)	AES256	91 x 43 x 25,85	85
ZyXEL								
ZyXEL ZyWALL 310	Tajvan	570 EUR	500 Mbps	200 (IPsec), 50 (SSL)	IPSec in SSL	3DES	430 x 250 x 44	4626
BORDOTEK								
IP VPN ENCRYPTION HC-7825 10/20/100 MEGABIT VERSION	Švica	/	100 Mbps	250	/	HCA-480	444 x 260 x 44 mm	4200

Tabela 2: Primerjava sorodnih produktov (vir: Bordotek, n. d.; Tiny Hardware Firewall, n. d.; Tutus: Digital Gatekeepers, 2010; ZyXEL, 2016;).

Nekateri kripto-moduli so namenjeni (fizičnemu) prenosu, podobno kot VPN kripto-modul C1S, nekateri so narejeni v stacionarne namene za velike organizacije, nekateri so bolj »ceneni«. Vsi najdeni produkti opravljajo isto nalogo, vendar se razlikujejo po svojih lastnostih. Ugotavljamo, da je VPN kripto-modul C1S naprava, ki je konkurenčna ostalim, trenutno dostopnim produktom na trgu.

3.1 Ergonomski model kripto-modula za navidezno zasebno omrežje

Ergonomičnost pri kripto-modulu za navidezno zasebno omrežje razumemo kot optimalno ravnovesje med kakovostjo, učinkovitostjo, uporabnostjo ter zunanjim videzom izdelka, zato je ergonomičnost poleg osnovnih funkcionalnosti ena izmed ključnih lastnosti pri lansiranju produkta na trg. Kripto-modul je lahko po karakteristikah izjemen in cenovno konkurenčen, pa zaradi neustrezne ergonomije ni tržno uspešen. Iščemo pravo ravnovesje med kakovostjo, učinkovitostjo in uporabnostjo kripto-modula. Sestavni del kakovosti predstavljajo tudi standardi in certifikati. Le-ti so za mnoge organizacije velik finančni izziv. Glede na opravljeno analizo trga so si kripto-moduli na področju ergonomičnosti izredno podobni. Gre za tehnološko zahtevne izdelke, pri katerih je učinkovitost delovanja ter varnost

prenosa podatkov pomembnejša od samega zunanjega videza. Zagotovo pa ne smemo na račun »prijetnega« fizičnega oziroma vizualnega videza ter majhnosti in s tem prenosljivosti produkta žrtvovati zmogljivosti kripto-modula.

Po analizi sorodnih izdelkov na trgu sledi oblikovanje ergonomskega modela kripto-modula za navidezno zasebno omrežje. Poglaviten in osrednji cilj pri oblikovanju predlogov je ustvariti takšen kripto-modul za navidezno zasebno omrežje, ki omogoča šifriranje in zaščito podatkov ter ima zanimiv in eventualno drugačen dizajn. Namen je dati obliko izdelku, z upoštevanjem skladnosti med funkcionalnostjo, estetiko in tehnološkim procesom (Slovar slovenskega knjižnega jezika, 2014). Zato smo želeli z lastnim oblikovanjem predlogov za kripto-modul za navidezno zasebno omrežje in pripadajoče dodatne opreme prikazati, da se pri razvoju izdelka VPN kripto-modula C1S lahko z različnimi oblikami približamo široki množici ljudi – tako domačim kot poslovnim uporabnikom, ki varnost in morebitno tajnost podatkov postavljajo na prvo mesto.

Pripravili smo šest predlogov oblik VPN kripto-modula C1S:

- **C1S Mouse** zadošča potrebam o prenosljivosti, majhnosti in nizki teži samega produkta. Oblika miške je inovativen in hkrati zelo uporaben, saj za vnašanje kode PIN ne potrebujemo dodatne tipkovnice.
- **Premični C1S** je zasnovan z več različnimi vhodi (mrežni UTP priključek, direktni USB in dodatni vhodi za mikro USB).
- **C1S Multi** omogoča priklop več računalnikov oziroma uporabnikov na en kripto-modul za navidezno zasebno omrežje, ki ga upravlja ena oseba. Omenjeni produkt je odlična izbira za podjetja in organizacije, saj med drugimi prednostmi predstavlja tudi nižji strošek.
- **C1S USB Edition** predstavlja najmanjšo različico kripto-modula, ki v celoti ustreza kriterijem o prenosljivosti.
- **C1S Kids** je inovativna oblika kripto-modula, ki smo si ga zamislili za potrebe ozaveščanja mladih o varnosti na internetu ter seznanjanja mlajših otrok (vrtec, prva triada osnovne šole) o pomembnosti šifriranja.
- Pod dodatno opremo smo umestili še silikonske pokrovčke, tako imenovane **C1S Fashion**, ki s svojo barvitostjo in modnim (barve, razni junaki ...) videzom ciljajo na najširšo populacijo končnih uporabnikov. Pokrovčki nimajo zgolj estetske funkcije, temveč kripto-modulu za navidezno zasebno omrežje nudijo tudi dodatno zaščito.

Produkt VPN kripto-modul C1S je v osnovi namenjen zagotavljanju varnosti posredovanih in prejetih podatkov in je po vseh lastnostih konkurenčen trenutno dostopnim produktom na trgu, kot je razvidno iz tabele 2 v prejšnjem odstavku.

4 TESTIRANJE VPN KRIPTO-MODULA C1S

Testiranje izdelka, kot je VPN kripto-modul C1S, je zahteven proces, ki ga sestavlja več vrst testiranj. Ta se zgodijo na različnih ravneh delovanja izdelka in na različnih stopnjah razvoja. Večino testnih procesov je treba ponavljati v vseh fazah razvoja izdelka, saj je le tako mogoče preprečiti napake in zmanjšati stroške razvoja produkta.

4.1 Programsko testiranje

Programsko testiranje je proces, s katerim poskušamo prikazati, da v programski opremi, ki jo programiramo, ni napak (Mayers, 2004). Gre za izvajanje oziroma vrednotenje programa ali zgolj komponent z namenom, da se preveri, ali program ustreza zahtevam oziroma, da se prikaže razlika med pričakovanimi in dejanskimi izhodnimi vrednostmi (Dogša, 1993). S testiranjem tako lahko prikažemo zgolj prisotnost posameznih napak, nikakor pa ne moremo dokazati njihove odsotnosti. Pri testiranju se tako izvajajo testni scenariji, s katerimi se preverja specifične funkcionalnosti izdelka. Dejstvo pa je, da ni mogoče v celoti trditi, da je izbrani izdelek popolnoma brez napak. Nobenega sistema se ne da testirati v popolnosti, saj za to obstajajo teoretične omejitve. Ne omejujejo pa nas zgolj teoretične, temveč tudi praktične omejitve, saj se pri testiranju srečujemo z omejenim časom in omejenimi stroški. Zaradi omejenosti je tako potrebno razumno ravnanje z napakami (Lončarić et al., 2015). Najprimernejši metodi testiranja programske opreme VPN kripto-modula C1S sta se po analizi izkazali metodi črne in bele škatle (angl. *White and black box testing*). Pri testiranju po metodi črne škatle nimamo vpogleda v interno strukturo produkta, testiramo le funkcionalnosti produkta – ali se vneseni podatki skladajo s pričakovanimi izhodnimi podatki. Pri testiranju po metodi bele škatle poznamo notranjo strukturo in vse algoritme, po katerih deluje izdelek. Pri testiranju po metodi bele škatle torej določimo vhodne podatke ter tudi pričakovane, pravilne izhodne podatke (British Computer Society Specialist Interest Group in Software Testing (BCS SIGIST), 2001). Poleg omenjenega pa smo kot primerno, a nekoliko manj ključno ocenili tudi dinamično testiranje in testiranje po metodi sive škatle (angl. Gray box testing), kar pomeni, da mora oseba, ki opravlja test, vsaj delno poznati delovanje notranje strukture in algoritmov (Khan in Khan, 2012).

Testiranja, ki jih je treba izvajati v posameznih komponentah kripto-modula, predstavljajo osnovo oziroma stopenjsko testiranje programske opreme, ki je razvidno v tabeli 3.

Vrsta testiranja	Opis
Testiranje enot in modulov	*Test enot je metoda testiranja programske opreme, pri kateri se osredotočamo na posamezno enoto ali posamezen del programske kode.*
Integracijsko testiranje	*Z integracijskim testom želimo preveriti funkcionalnosti, zmogljivosti in zanesljivosti ključnih delov programske opreme.*
Sistemsko testiranje	*Sistemsko testiranje je metoda testiranja programske opreme, kjer se osredotočamo na celoten integriran sistem. Namen sistemskega testiranja je preveriti skladnost sistema z zahtevami, ki so bile predhodno določene v dokumentaciji.*
Testiranje sprejemljivosti	*Testiranje sprejemljivosti je metoda testiranja programske opreme, ki predstavlja zadnje testiranje pred predajo programske opreme v uporabo naročniku. Programska oprema, ki uspešno prestane test sprejemljivosti, naj bi ustrezala skoraj vsem zahtevam, ki jih je izpostavil naročnik oziroma razvijalec programa.*
Testiranje komponent vmesnika	*Testiranje komponent vmesnika je metoda testiranja programske opreme, ki se uporablja za preverjanje ravnanj s podatki med različnimi enotami ali komponentami. Namen te vrste testiranja je najti napake vmesnikov in napake v predpostavkah, povezanih z vmesniki.*

Tabela 3: Osnovna oziroma stopenjska testiranja programske opreme (vir: Kuzem, 2011).

Tabela 3: Nadaljevanje

Vrsta testiranja	Opis
Sistemsko integracijsko testiranje	*Pri omenjenem testiranju se pod drobnogled vzame več integriranih sistemov, ki so prestali sistemsko testiranje, hkrati pa se preveri tudi, kako delujejo zahtevane interakcije med samimi sistemi.*
Regresijsko testiranje	*Regresijsko testiranje je metoda testiranja programske opreme, ki se uporablja v primerih, ko se programska koda večkrat spremeni. Z omenjenim testiranjem tako preverjamo, ali so uvedene spremembe botrovale k nastanku novih napak, prav tako pa se s testiranjem iščejo napake, ki so bile v prvotni fazi odpravljene, a so se zaradi spremenjene kode zopet pojavile.*

V široki paleti testiranj, ki jih lahko izvajamo na končnem produktu, smo izbrali testiranja, prikazana v tabeli 4.

Tabela 4: Testiranja, ki jih izvajamo na končnem produktu (vir: Software testing, 2015).

Vrsta testiranja	Opis
»Smoke and sanity« testiranje	*»Smoke« testing pomeni predhodno testiranje, s katerim iščemo preproste napake, ki bi lahko bile tako hude, da bi onemogočile izdajo programske opreme. »Sanity« test je osnovni test za hitro ugotavljanje, ali so rezultati izračunov resnični. Pri tem testu se preverja programska koda in njena funkcionalnost.*
Testiranje povezljivosti	*Testiranje povezljivosti je sistemsko testiranje, ki preverja skladnost aplikacijske rešitve z njenimi nefunkcionalnimi zahtevami. Preverjamo torej, kako se je aplikacija zmožna povezati z računalniškim okoljem.*
Namestitveno testiranje	*Pri namestitvenem testiranju ugotavljamo, kaj bodo uporabniki morali storiti za pravilno namestitev in vzpostavitev delovanja programske opreme. Proces testiranja vključuje polno ali delno nadgrajevanje oziroma odstranjevanje programske opreme.*
Varnostno testiranje	*Varnostno testiranje je proces, s katerim se odkrivajo pomanjkljivosti v varnostnem mehanizmu informacijskega sistema, ki varuje podatke.*
Destruktivno testiranje	*Destruktivno testiranje se izvaja z namenom razumevanja strukturne zmogljivosti in vedenja materiala. Destruktivni testi pokažejo, v kakšnih razmerah in ob katerih dogodkih izdelek še deluje in kje pride do okvare ali napake v programski kodi.*
Beta testiranje	*Uporabniki, ki prejmejo beta različico programske opreme, poročajo razvijalcem o prisotnosti hroščev, na katere so naleteli, kar omogoča programskim razvijalcem lažje in hitrejše odpravljanje teh težav.*
Test uporabnosti	*Test uporabnosti se navezuje na testiranje sprejemljivosti, in sicer s testom uporabnosti preverimo, ali je uporabniški vmesnik lahek za uporabo ter razumljiv.*

Testiranja, ki bi jih bilo prav tako smiselno izvesti, vendar niso primarnega pomena, so prikazana v tabeli 5.

Tabela 5: Testiranja, ki bi jih bilo smiselno izvesti za VPN kripto-modul C1S (vir: Software testing, 2015).

Vrsta testiranja	Opis
Razvojno testiranje	*Razvojno testiranje je programsko-razvojni proces, ki vključuje sinhronizirano dodajanje širokega spektra procesov za preprečevanje napak in strategij za odkrivanje napak z namenom zmanjšanja tveganj, časa in stroškov pri razvoju programske opreme.*
A/B testiranje	*Princip delovanja A/B testiranja je preprost in temelji na tem, da imamo identična programa (A in B), pri katerih tekom testiranja spreminjamo različne spremenljivke in nato spremljamo odziv programov na nove (različne) spremenljivke.*
Testiranje delovanja programske opreme	*Testiranje delovanja programske opreme predstavlja testiranje, ki odgovori na vprašanje, kako sistem ali podsistem deluje v odzivnosti in stabilnosti, kadar je pod določeno delovno obremenitvijo.*
Testiranje po specifikacijah	*Testiranje po specifikacijah je testiranje, s katerim se ugotavlja skladnost izdelka z zahtevami specifikacij, pogodbe ali uredbe.*
Hkratno testiranje	*Hkratno testiranje predstavlja testiranje, ki določa stabilnost sistema ali aplikacije, kadar je izpostavljena normalnemu delovanju.*
Alfa testiranje	*Alfa testiranje je metoda testiranja programske opreme, kjer gre za simulirane oziroma dejanske operativne teste, ki so izvajani s strani potencialnih uporabnikov oziroma neodvisnih testnih skupin s strani razvijalca.*

Pri programskem testiranju so pomembni tudi procesi testiranja, ki so nekakšna osnova nadaljnjega razvoja produkta. Od obstoječih tipov tovrstnega testiranja so za izdelek VPN kripto-modul C1S najprimernejše agilne metoda (angl. *Agile software development*), čeprav je za testiranje primerna tudi uporaba tradicionalnih metod (npr. slapovni razvoj programske opreme). Ekstremno programiranje, kot ena izmed agilnih metod, je zaradi svojega načina delovanja na prvi pogled neprimerno za testiranje VPN kripto-modula C1S, vendar je ob sledenju modelom za prepoznavanje groženj (npr. Microsoft STRIDE) primerno tudi za testiranje in razvoj varne programske opreme (Bolboaca in Bolboaca, 2014; Microsoft, 2016). Pri delu s programsko kodo je uporabno tudi avtomatizirano testiranje, ki preverja predvsem delovanje osnovnih in manj zahtevnih funkcij. Pri VPN kripto-modulu C1S bi se za to vrsto testiranja lahko odločili pri testiranju grafičnega uporabniškega vmesnika ter pri testiranju programske kode in vmesnika za programiranje (Software testing, 2015). Vsi tipi programskega testiranja, primernih za VPN kripto-modul C1S, so predstavljeni v tabelah 3, 4 in 5.

Ko združimo skupaj različne stopnje in tipe testiranj, vidimo, da je celoten proces testiranja, od začetkov pisanja programske kode do uporabe končnega produkta, kompleksen in zahteven. V samem procesu testiranja programske opreme morajo sodelovati tako razvijalci opreme, testni inženirji kot končni uporabniki, saj le s sodelovanjem vseh akterjev izdelamo program ali izdelek, ki je primeren za uporabo na trgu.

Pri testiranju programske opreme je treba omeniti še samotestiranje, ki ga kripto-modul izvaja po priporočilih standarda FIPS 140-2. Kripto-modul opravi samotestiranje ob vsakem vklopu (angl. *Power-up self-test*) oziroma v primerih, kadar se zažene varnostna funkcija ali operacija, ki zahteva samotestiranje (angl. *Conditional self-test*). V primeru, kadar kripto-modul ne uspe zagnati samotestiranja oziroma je samotestiranje neuspešno, sporoči napako preko vmesnika za javljanje statusa naprave (angl. *Status output interface*). Če je kripto-modul v stanju napake, ne sme izvajati nobenih funkcij ali operacij (National Institute of Standards and Technology, 2001). Samotestiranje je pomemben del testiranja, ki omogoča nemoteno delovanje kripto-modula. Samotestiranje uvrstimo med vse tri tipe testiranj, ker zajema tako testiranje programske, strojne opreme ter kode nameščene na strojni opremi.

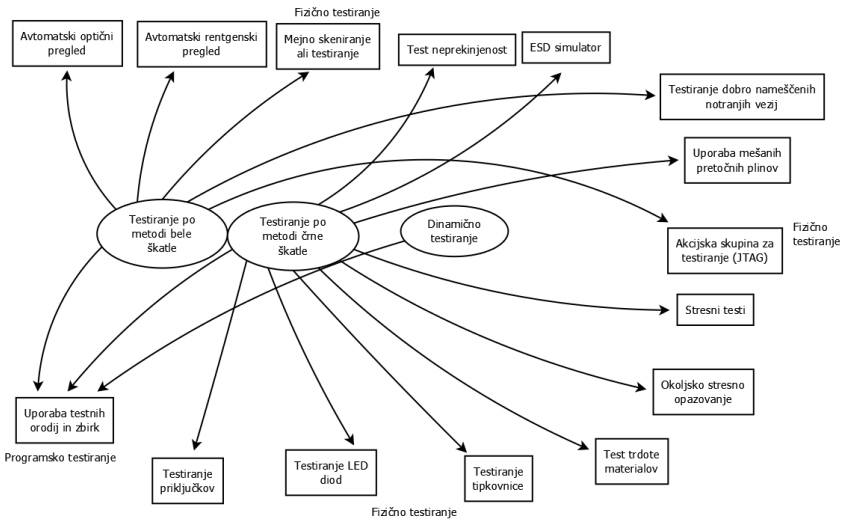
4.2 Testiranje strojne opreme

Za zagotavljanje celovitosti pri delovanju VPN kripto-modula C1S pred končnim lansiranjem izdelka na trg je treba poleg programskega testiranja opraviti tako imenovano testiranje strojne opreme. Testiranje strojne opreme poteka podobno kot ostale vrste testiranj, le s to razliko, da so testiranja osredotočena primarno na fizično delovanje strojne opreme. Kot je razvidno iz slike 1, sta za potrebe VPN kripto-modula C1S primerni metodi testiranja po metodi bele in črne škatle, ki omogočata:

1. Preverjanje delovanja priključkov – preverimo, ali mikro USB in UTP priključki delujejo tako, kot to zagotavlja njihov proizvajalec (Global Sources, n. d.).

2. Testiranje LED diod – s programom ali s pomočjo digitalnega multimetra testiramo delovanje diod.
3. Testiranje tipkovnice – za fizično testiranje pritiskov na tipkovnici se uporabljajo avtomatizirani testni roboti (TRICOR Systems, n. d.).
4. Stresne teste – testiranje v pogojih izven zmogljivosti produkta, pogosto blizu točke zloma (angl. *breaking point*) (Stress testing, 2015).
5. Akcijska skupina za testiranje (JTAG) ali IEEE 1149.1 standard – testiranje pinov na tiskanih vezjih (Altera Corporation, 2007).
6. Uporaba testnih orodij in zbirk – uporaba programov za testiranje strojne opreme.

Slika 1: Metode testiranja strojne opreme



Na sliki 1 je s puščicami ponazorjena primernost uporabe posameznih tipov testiranj, ki niso omenjeni v zgornjih alinejah. Zadnji tip testiranja, ki prav tako pripomore k celovitosti delovanja kripto-modula, predstavlja testiranje kode, nameščene na strojni opremi (angl. *Firmware*). Kot je znano, nam VPN kripto-modul C1S omogoča šifriranje s šifrirnimi standardi AES128/192/256 ter možnostjo dodajanja lastnih šifrirnih algoritmov. To pomeni, da lahko uporabnik kripto-modulu dodaja poljubne šifrirne algoritme, ki nadomestijo AES. Zaradi teh dveh vrst kode na strojni opremi kripto-modula je treba opraviti določena testiranja, ki zagotavljajo, da koda in same komponente delujejo tako, kot od njih pričakujeta proizvajalec in uporabnik. Najboljša možnost testiranja takega tipa opreme je z uporabo testiranja po metodi bele škatle, in sicer z uporabo programskega testiranja, pri katerem uporabljamo uporabo testnih orodij in/ali zbirk s KAT, MMT in MCT testi, ki se uporabljajo predvsem za testiranje šifrirnih algoritmov (Bassham III, 2002).

5 TESTNE METODE ZA EN MODUL

S pomočjo testiranja lahko pravočasno popravimo napake tako na strojni (mehanske oziroma tehnične nepravilnosti) kot na programski (»hrošči«) opremi. Za uspešno izvedbo samega testiranja moramo natančno opredeliti in predvideti testne scenarije. Zaradi obsežnosti naloge in omejenosti s časom smo se osredotočili na pisanje testnih scenarijev za spreminjanje imena naprave oziroma »Hostname«. V okviru projekta smo pripravili 24 testnih scenarijev. Iz tabele 6 je razviden primer enega testnega scenarija.

Tabela 6: Primer enega testnega scenarija

Testni scenarij	Element	Cilj testnega scenarija	Podrobna razlaga	Visokonivojski opis	Pričakovan rezultat
TC_GUI_ HostName_V-01	Hostname	Vnos veljavnega »hostname«	V vnosno polje zapišemo veljavno ime za »hostname« in shranimo spremembe	1. Določi nov »hostname«; omejitve 1 ≤ N ≤ 24, znaki: velike in male črke ASCII ter številke 2. Shrani spremembe	**OK** »Hostname« mora biti spremenjen in shranjen

Ker je testnih scenarijev veliko, je priročno, če testiranje avtomatiziramo. Izvedli smo postopek vizualnega testiranja z orodjem SikuliX. SikuliX je orodje, s katerim avtomatiziramo vse, kar vidimo na zaslonu računalnika. Za identificiranje in upravljanje komponent grafičnega vmesnika se uporablja orodje za prepoznavo slike (Sikuli, n. d.). Preizkusili smo delovanje Robot Framework, ki je generično testno avtomatizirano ogrodje za preskušanje sprejemljivosti ter razvoj na podlagi preskusa sprejemljivosti (Robot Framework, 2014). Ugotovili smo, da je prišlo do razlik med orodjema. Na eni strani je SikuliX, preprost za uporabo, na drugi pa Robot Framework, za katerega je potrebno napredno znanje in izkušnje s področja programiranja.

Pri vseh testih moramo stvari tudi ustrezno beležiti. To lahko uredimo s pomočjo sistema za beleženje hroščev (angl. *Bug tracking system*) v programski opremi. Gre za orodje, ki skrbi za beleženje napak testiranj programske opreme, ki je v procesu razvijanja in nadgrajevanja. Lahko gre za odprt sistem, v katerega poročila o napakah beležijo in poročajo tudi končni uporabniki, ali pa gre za zaprt sistem, ki ga uporabljajo samo razvijalci v fazi razvijanja in testiranja programske opreme. Glavna prednost sistema je centraliziran vpogled na zahteve po razvoju in izboljšavah, kot tudi na stanje napredka in dela na teh zahtevah. Na podlagi tega se lahko generirajo poročila o produktivnosti programerjev pri popravljanju in odpravljanju hroščev (Techopedia, 2016). Testni proces je nekaj, kar se uporablja skozi celotno življenjsko dobo izdelka.

6 UGOTOVITVE IN ZAKLJUČKI

Za izvedbo večmesečnega projekta in ustrezno testiranja VPN kripto-modula C1S je potrebno dobro usklajevanje sodelujočih. Ta se kaže v ustreznem delegiranju nalog in sprotnem izobraževanju tistih, ki testiranja izvajajo in pripravljajo ter urejajo vmesna in končna poročila. Pomembno stično točko celotnega dela na

projektu predstavlja uporaba skupnega spletnega portala, ki omogoča nemoteno komunikacijo med vsemi sodelujočimi in sprotno beleženje dela ter napredka na projektu. Poleg ustrezne izvedbe analize tveganj je za testiranje pomembno poznavanje sorodnih izdelkov ter primernih testnih metod za konkreten izdelek. S poznavanjem in podrobno analizo sorodnih izdelkov je lažje določiti testne scenarije in testne metode. S tem korakom pri testiranju poskrbimo za optimalno izrabo časa in sredstev. Poleg primerjave s sorodnimi izdelki je testerjem omogočen prihranek časa in sredstev s preverjanjem testnih specifikacij, ki jih za vgrajene komponente opravijo proizvajalci. Kot primer vzamemo USB priključke, LED svetila in tipkovnico kripto-modula za navidezno zasebno omrežje, ki so testirana s strani proizvajalca, zaradi česar testiranje teh komponent, kot del testiranja strojne opreme, ni potrebno. Seveda je v teh primerih obvezna izbira zanesljivega in preverljivega proizvajalca posameznih komponent.

Najzahtevnejši del celovitega testiranja predstavlja testiranje programske opreme in šifrirnih algoritmov, posebno tistih, ki jih uporabnik sam namesti na kripto-modul. Testiranje šifrirnih algoritmov, ki spadajo pod kodo, nameščeno na strojni opremi, poteka po standardu FIPS 140-2. To pomeni, da mora kripto-modul zadovoljiti vse potrebe standarda pred lansiranjem na trg. Sledi testiranje programske opreme, ki predstavlja unikaten prispevek posameznih programerjev k delovanju, predvsem uporabniškega vmesnika kripto-modula za navidezno zasebno omrežje. Prav testiranje uporabniškega vmesnika je ena izmed vrst testiranja, ki je lahko avtomatizirano s pomočjo programov npr. SikuliX in Robot Framework. Ugotavljamo, da se s pravilnim postopkom izpeljave avtomatizacije testnih procesov prihranita čas in finančna sredstva, ki bi jih tester oziroma programer porabil ob neavtomatiziranem testnem procesu. Za pravilno delovanje ostale programske opreme, ki je z avtomatiziranim testiranjem ne morem optimalno vključiti v testni proces, je treba uporabiti primerne testne metode. Metodo črne škatle, kadar nas zanimajo le končni rezultati vhodnih in izhodnih podatkov, ali metodo bele škatle, kadar nas zanima celoten cikel potovanja vhodno-izhodnih podatkov.

Ugotavljamo, da je testiranje kripto-modula za navidezno zasebno omrežje kompleksen, vendar nujno potreben proces, ki zagotavlja optimalno delovanje izdelka, kot je VPN kripto-modul C1S. S testiranjem smo odpravili večino napak, kar pomeni, da je na trg lansirani izdelek VPN kripto-modul C1S konkurenčen in zagotavlja izjemno stopnjo varnosti pred grožnjami, prisotnimi v kibernetskem prostoru.

UPORABLJENI VIRI

Altera Corporation. (2007). *IEEE 1149.1 (JTAG) boundary-scan testing for cyclone II devices.* Pridobljeno na http://www.altera.com/literature/hb/cyc2/cyc2_cii51014.pdf

Bassham III, L. E. (2002). *The advanced encryption standard algorithm validation suite (AESAVS).* National Institute of Standards and Technology Information Technology Laboratory Computer Security Division. Pridobljeno na http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf

Bolboaca, A. in Bolboaca A. (6. 3. 2014). *Briefly on architecture, extreme programming and security testing.* Agile Record. Pridobljeno na http://www.agilerecord.com/architecture-extreme-programming-security-testing/

Bordotek. (n. d.). *HC-7825m.* Pridobljeno na http://www.bordotek.net/en/brands-listing/product/57-hc-7825-10-20-100-mb-version.html

British Computer Society Specialist Interest Group in Software Testing [BCS SIGIST]. (2001). *Standard for software component testing*. Pridobljeno na http://www.testingstandards.co.uk/Component%20Testing.pdf

Dimov, I. (20. 6. 2013). *Guiding principles in information security*. Infosec Institute. Pridobljeno na http://resources.infosecinstitute.com/guiding-principles-in-information-security/

Dogša, T. (1993). *Verifikacija in validacija programske opreme*. Maribor: Tehniška fakulteta.

Global Sources. (n. d.). *Micro USB connector manufacturer*. Pridobljeno na http://www.globalsources.com/gsol/I/Micro-USB/p/sm/1066479043.htm#1066479043

Haahr, M. (12. 4. 2015). *Introduction to randomness and random numbers*. Dublin: Random.org. Pridobljeno na https://www.random.org/randomness/

Khan, M. E. in Khan, F. (2012). A comparative study of white box, black box and grey box testing techniques. *International Journal of Advanced Computer Science and Applications, 3*(6), 12–15. Pridobljeno na http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.261.1758&rep=rep1&type=pdf

Kuzem, R. (2011). *Načrtovanje testiranja pri razvoju IS v manjših razvojnih skupinah* (Diplomsko delo). Ljubljana: Fakulteta za računalništvo in informatiko. Pridobljeno na http://eprints.fri.uni-lj.si/1266/1/Kuzem_R._-_diplomsko_delo.pdf

Lončarić, T., Vehovec, A., Kastelic, M., Drofenik, D., Divjak, S., Kavčič, A. et al. (31. 3. 2015). *Upravljanje s programljivimi napravami.* Pridobljeno na http://www.egradiva.net/moduli/programirljive_naprave/01_datoteka.html

Mayers, G. J. (2004). *The art of sotfware testing* (2nd ed.). New Jersey: John Wiley & Sons.

Mesojedec, T., Šporar P., Strojan, K., Valentinčič, T., Bačar, F., Sakovič, G. et al. (2015). *Socialno podjetništvo.* Pridobljeno na http://www.socialni-inovatorji.si/knjiga/socialno-podjetnistvo/44-trzne-raziskave-analiza-trga

Microsoft. (2003). *What is VPN?* Pridobljeno na https://technet.microsoft.com/en-us/library/cc739294(v=ws.10).aspx

Microsoft. (2016). *The STRIDE threat model*. Pridobljeno na https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

National Institute of Standards and Technology. (2001). *Security requirements for cryptographic modules.* Pridobljeno na http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

National Institute of Standards and Technology. (1. 2. 2016). *Standards.* Pridobljeno na http://csrc.nist.gov/groups/STM/cmvp/standards.html

PwC. (2014). *Managing cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015*. Pridobljeno na http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

Robot Framework. (2014). *Robot Framework introduction*. Pridobljeno na http://robotframework.org/#introduction

Senetas. (2013). *Understanding senetas layer 2 encryption: Technical paper*. Pridobljeno na http://www.senetas.com/_uploads/files/Technical-Paper_Understanding_Senetas_Layer_2_Encryption.pdf

Sikuli. (n. d.). *Sikuli script*. Pridobljeno na http://www.sikuli.org/

Slak, L. (2009). *Analiza operativnih tveganj OE banke*. Maribor: Nova KBM. Pridobljeno na http://www.isaca.si/datoteke/Analiza_operativnih_tveganj.ppt

Slovar slovenskega knjižnega jezika. (2014). Ljubljana: Založba ZRC; Znanstveno raziskovalni center SAZU. Pridobljeno na http://www.fran.si/130/sskj-slovar-slovenskega-knjiznega-jezika

Software testing. (2015). V *Wikipedia: The free encyclopedia*. Pridobljeno na https://en.wikipedia.org/wiki/Software_testing

Stress testing. (2015). V *Wikipedia: The free encyclopedia*. Pridobljeno na http://en.wikipedia.org/wiki/Stress_testing

Techopedia. (2016). *Bug tracking*. Pridobljeno na http://www.techopedia.com/definition/25910/bug-tracking

Tiny Hardware Firewall. (n. d.). *Tiny Hardware Firewall VPN client*. Pridobljeno na http://tinyhardwarefirewall.com/

TRICOR Systems. (n. d.). *Automated keyboard test system – 921 xy*. Pridobljeno na http://www.tricor-systems.com/products/switch-testers/switch-tester-921xy.htm

Tutus: Digital Gatekeepers. (2010). *Färist Micro.* Pridobljeno na http://www.tutus.se/products/farist-micro.html

ZyXEL. (2016). *VPN firewall: ZyWALL 1100/310/110*. Pridobljeno na http://www.zyxel.com/products_services/zywall_1100_310_110.shtml?t=p

O avtorjih:

Anže Zaletel, diplomirani varstvoslovec, magistrski študent Fakultete za varnostne vede Univerze v Mariboru.

Jaka Žužek, diplomirani varstvoslovec informacijske varnosti.

Lavra Horvat, diplomantka upravnih ved, magistrska študentka Fakultete za varnostne vede Univerze v Mariboru.

Katja Zupan, diplomirana varstvoslovka, magistrska študentka Fakultete za varnostne vede Univerze v Mariboru.

Sara Železnik, diplomirana varstvoslovka, magistrska študentka Fakultete za varnostne vede Univerze v Mariboru.

Nina Goršič, diplomantka upravnih ved, magistrska študentka Fakultete za varnostne vede Univerze v Mariboru.

Maruša Lipušček, diplomirana varstvoslovka, magistrska študentka Fakultete za varnostne vede Univerze v Mariboru.

VARSTVOSLOVJE,
letn. 18
št. 3
str. 303–324

Naložbene prevare: viktimološki pogled

Mateja Bitenc

Namen prispevka:

Namen prispevka je povečati osveščenost javnosti o obsegu naložbenih prevar, njihovih značilnostih in vplivih na žrtve, o tem, kaj vse vpliva na to, da posameznik postane žrtev, ter na primerih pokazati znake, na podlagi katerih lahko prepoznamo naložbeno prevaro.

Metode:

Prispevek združuje teoretični področji viktimologije ter finančne kriminalitete. Gre za teoretičen prispevek, kjer so bile uporabljene metode deskriptivne in primerjalne analize ter sinteze. Za oblikovanje zaključkov smo uporabili znanstveno metodo sinteze, temelječo na kombinaciji induktivnega in deduktivnega sklepanja (inverzna dedukcija). Pri pregledu viktimoloških raziskav smo poudarek dali raziskavam, ki se ukvarjajo z žrtvami finančne kriminalitete, konkretno žrtvami naložbenih prevar.

Ugotovitve:

Naložbene prevare so problem družbe in problem posameznika. Različne študije kažejo, da je število ljudi, ki so žrtve tovrstnih kaznivih dejanj, iz leta v leto večje. Tovrstna izkušnja se globoko zareže v življenje posameznika in ima na žrtev izredno negativen vpliv – tako v materialnem kot tudi v čustvenem, psihološkem in zdravstvenem pogledu.

V prispevku so predstavljeni najpogostejši tipi naložbenih prevar ter njihove značilnosti, ugotovitve raziskav o žrtvah naložbenih prevar, njihovih lastnostih, življenjskem slogu in okoliščinah, ki pomembno vplivajo na to, da posameznik postane žrtev naložbene prevare. Predstavljen je torej kontekst, znotraj katerega se zgodi naložbena prevara. Prispevek zaključujemo s pregledom nekaterih najočitnejših in najpogostejših znakov, na podlagi katerih lahko posumimo, da gre za naložbeno prevaro in ne za pravo naložbeno priložnost.

Omejitve/uporabnost raziskave:

Viri oziroma raziskave, ki obravnavajo žrtve naložbenih prevar in druge finančne kriminalitete, so v primerjavi s študijami in raziskavami klasične, (»nasilne«) kriminalitete redkejše, saj je pozornost tako stroke kot tudi širše javnosti v večji meri namenjena žrtvam prav slednje, manj pa žrtvam t. i. beloovratniške nenasilne kriminalitete.

Izvirnost/pomembnost prispevka:

Prispevek je pomemben, saj se v zadnjem času predvsem na spletnih straneh in preko drugih prodajnih poti, kot so elektronska pošta, telefonski klici, organizacija brezplačnih prodajnih in informativnih srečanj za potencialne

vlagatelje in podobno, pojavlja vedno več ponudb za vlaganje finančnih sredstev v različne naložbene priložnosti. Za nekaterimi od teh ponudb se skrivajo prevaranti, ki s profesionalnim pristopom in preslepitvenimi taktikami prežijo na potencialne vlagatelje. Prispevek je namenjen širši javnosti in ima namen opozoriti na prisotnost in velik obseg tega pojava ter opisati proces, kako do naložbene prevare sploh pride in kakšne so posledice, s katerimi se soočajo žrtve naložbenih prevar. Prispevek zaključujemo z opozorilom na nekaj najpogostejših (in najočitnejših) znakov, da gre pri finančni naložbi za naložbeno prevaro.

UDK: 343.72

Ključne besede: naložbe, preslepitve, prevare, finančna kriminaliteta, žrtve, oškodovanci

Financial Investment Frauds: Victimological View

Purpose:

The main purpose of the article is to rise attention of the public about the scope of investment frauds, their characteristics and the effects on the victims; to explain the contexts of victims' lives and how they interplay with making someone more or less vulnerable becoming the victim of investment fraud. The goal is also to present some case studies to show the signs of the possible financial fraud.

Design/Methods/Approach:

The article combines two theoretical fields: victimology and financial crime. In the paper, methods of descriptive and comparative analysis and synthesis were used. Scientific method of synthesis based on a combination of inductive and deductive reasoning is used for drawing conclusions. In reviewing victimology researches, the emphasis was on researches dealing with victims of financial crime, specifically the victims of investment fraud.

Findings:

Financial frauds, and more specifically investment frauds, are the problem of the society and the problem of the individual. Financial crimes affect thousands of people every year, yet very little is known about the experiences. Such experience deeply incises into the lives of individuals and has extremely negative impact on their lives due to the victimization - not only in the material sense (material losses) but also highly negative emotional, psychological and health impacts. The article brings the most common types of investment frauds, characteristics of the victims and their contexts of lives which have the major impact on the fact that one became the victim of the investment fraud. Therefore, the context within which the investment scam happens is featured. The article concludes with a review of some of the most obvious and most common signs, on which you can suspect that the opportunity presented is an investment scam and not a real investment opportunity.

Research Limitations/Implications:

The sources and the researches of the victims of investment fraud and other financial crime are rarer because of the fact, that more attention in given by both,

the criminologists and the general public, to the victims of classic („violent“) crime compared to the attention given to the victims of white collar crime.

Originality/Value:

The topic is relevant because of the fact, that recently more and more recruiting actions by fraudsters have taken place on the web sites and via other channels of communication (i.e. spam, cold phone calls, organization of free seminars and sales promotions), all leading the potential victims to making decisions in investing their savings into the financial opportunities, of which some of them may just be financial scams.

Our aim is to inform the public about the scope of these phenomena, to give the outline about the process of leading the investor into the financial fraud (grooming), to present the consequences of the fact that one is become the victim of financial fraud and the impact on his or her life.

UDC: 343.72

Keywords: investments, frauds, scams, financial crimes, victims

1 UVOD

Naložbene prevare so problem družbe in problem posameznika. Različne študije kažejo, da je število ljudi, ki so žrtve tovrstnih kaznivih dejanj, iz leta v leto večje. Tovrstna izkušnja se globoko zareže v življenje posameznika in ima vsaj na nekatere žrtve izredno negativen vpliv – tako v materialnem kot tudi v čustvenem, psihološkem in zdravstvenem pogledu. Meško (1998) ugotavlja, da je odziv žrtev na viktimizacijo zelo različen: nekatere žrtve utrpijo prehodne težave, nelagodje, druge žrtve pa hujše oblike dezorientacije, dolgotrajno trpljenje in resne zdravstvene težave. Psihološka oškodovanost žrtve, ki sledi kriminalni viktimizaciji, je pogosto velika in je odvisna od narave dogodka, sposobnosti soočati se s težavami in možnostmi, ki so na razpolago (Meško, 1998).

Prispevek je namenjen širši javnosti in ima namen opozoriti na prisotnost ter velik obseg naložbenih prevar ter opisati/razložiti proces, kako do naložbene prevare sploh pride in kakšne so posledice, s katerimi se soočajo žrtve naložbenih prevar. Predstavljeni so najpogostejši tipi naložbenih prevar ter njihove značilnosti, ugotovitve raziskav o žrtvah naložbenih prevar, njihovih lastnostih, življenjskem slogu in okoliščinah, ki pomembno vplivajo na to, da posameznik postane žrtev naložbene prevare. Predstavljen je torej kontekst, znotraj katerega se zgodi naložbena prevara. Prispevek nadaljujemo z opozorilom na nekaj najpogostejših (in najočitnejših) znakov, da gre pri finančni naložbi za naložbeno prevaro; te ugotovitve izhajajo iz zbiranja in analiziranja podatkov o naložbenih prevarah in njihovih žrtvah, ki jih je izvedel *Financial Industry Regulatory Authority* (FINRA). Podatki sicer veljajo za ZDA, vendar lahko njihove ugotovitve apliciramo tudi na slovenski finančni trg. Na koncu prispevka pa poskušamo odgovoriti na vprašanje vloge žrtve v kazenskem postopku in poudariti pomen preventivne dejavnosti, ki poskrbi na eni strani za večjo osveščenost javnosti v zvezi s tem pojavom kriminalitete, na drugi strani pa z ustreznim strokovnim pristopom nudi pomoč žrtvam naložbenih prevar pri opolnomočenju po viktimizaciji.

Glavna vprašanja, s katerimi se ukvarja prispevek, so:

- Katere so značilnosti ter okoliščine v življenju posameznika, ki odločilno vplivajo na to, da posameznik postane žrtev naložbene prevare?
- Kakšne so posledice za posameznike, ki so doživeli naložbeno prevaro, kako se soočajo s temi posledicami ter kakšne strategije opolnomočenja po prevari uporabljajo?
- Kateri so najočitnejši in najpogostejši znaki, na podlagi katerih lahko posumimo, da gre za naložbeno prevaro in ne za pravo naložbeno priložnost?

V prispevku je kot znanstvena metoda raziskovanja uporabljena deskriptivna, primerjalna analiza in sinteza strokovne literature. Za oblikovanje zaključkov in predstavitev rezultatov smo uporabili znanstveno metodo sinteze, temelječo na kombinaciji induktivnega in deduktivnega sklepanja. Pri pregledu viktimoloških raziskav smo poudarek dali raziskavam, ki se ukvarjajo z žrtvami finančne kriminalitete, konkretno žrtvami naložbenih prevar.

2 NALOŽBENE PREVARE

Slovar slovenskega knjižnega jezika (2014: 136) prevaro opredeli kot »dejanja, s katerimi kdo z določenim namenom zavede koga v zmoto«. Najpogosteje je glavni motiv pridobitev premoženjske koristi, kar velja za klasične prevare oziroma goljufije[1], pa tudi za prevare, izvedene v virtualnem okolju oziroma internetne prevare (Dimc in Dobovšek, 2012).

Kanduč (2009: 223–224) ugotavlja: »Čeprav je mogoče oznako »prevara« v številnih kontekstih – in brez večjih komunikacijskih zapletov in nesporazumov – nadomestiti z izrazi, kot so »goljufija«, »sleparija« ali »potegavščina« (oziroma »nateg«), se zdi, da je v množici bolj ali manj sorodnih pojmovanj ta izraz dejansko najširši. No, to pa je tudi razlog, da je »prevaro« težko zares natančno opredeliti.«

Keršmanc (2014: 26) se do pojma »prevara« opredeli: »Tako prevara kot goljufija sta pravno kvalificirani obliki preslepitve. Sam pojem preslepitve (kot *modus operandi*) ni tako vrednostno obarvan, kot sta pojma prevara in goljufija. Prav tako je pojem preslepitev širši od pojma prevara in nam omogoča izhodiščno navezavo na preslepitve zunaj pravnega (pod)sistema. Kot najširši pojem preslepitev obsega tudi tiste dejavnosti, ki jih kazenska zakonodaja (še) ni inkriminirala oziroma običajno niso predmet kazenskopravnega pregona. Vsled navedenega je pojem preslepitev najprimernejši za celovito opredelitev preučevanega pojava, medtem ko je (ožji) kazenskopravni pojem *goljufiva* preslepitev uporabljen v kontekstu, ko je preslepitev že prešla v cono kriminalnosti.«

Viktimizacija pomeni oškodovanje; proces, dejanje ali dogodek, ki poškoduje ali oškoduje žrtev. Lahko je kriminalna (kadar je storjena s kaznivim

1 *Kazenski zakonik (KZ-1, 2008) v 211. členu opredeljuje kaznivo dejanje »Goljufije«: »Kdor, zato da bi sebi ali komu drugemu pridobil protipravno premoženjsko korist, spravi koga z lažnivim prikazovanjem ali prikrivanjem dejanskih okoliščin v zmoto ali ga pusti v zmoti in ga s tem zapelje, da ta v škodo svojega ali tujega premoženja kaj stori ali opusti, se kaznuje z zaporom do treh let.« V strokovni javnosti se za opisano ravnanje uporablja termin prevara. Izvršitveno ravnanje pri navedenem kaznivem dejanju je preslepitev, torej lažno prikazovanje ali prikrivanje dejanskih okoliščin, s čimer storilec oškodovanca zapelje v zmoto.*

ravnanjem) ali ne. O viktimizaciji, tako nekriminalni kot tudi kriminalni, pogosto ne vemo dovolj, saj se velik del kriminalne viktimizacije skriva v temnem polju kriminalitete, ki ostaja neprijavljen oziroma neodkrit. S tem izrazom označujemo stanje (p)oškodovanosti, prizadetosti, stanje, v katerem se je znašla žrtev, oziroma rezultat viktimizacije (Peršak, 2015).

Prevare sodijo med nenasilne oblike kriminalitete. Storilci za storitev te oblike kriminalitete največkrat uporabijo telefon, pismo, privlačno publikacijo, brošuro, ki predstavlja in obljublja lepe počitnice, blago, naložbeno priložnost, različne storitve. Primeri prevar so naslednji (United States Department of Justice, 2015): prevare preko telefona (prodaja ničvrednih izdelkov ali storitev), prevare preko pisem, zavarovalniške prevare, prevare v zvezi s pokojninskimi skladi, prevare v zvezi s kreditnimi karticami in čeki, kraja identitete, prevare v zvezi z vrednostnimi papirji in drugimi tipi investicij, bančne prevare, poneverbe, internetne prevare, piramidne in Ponzijeve sheme[2].

Financial Conduct Authority (2016) potencialne vlagatelje opozarja na velike možnosti finančnih prevar, predvsem z vrednostnimi papirji, zemljišči in surovinami (ang. *commodity trading*) na rastočih trgih. Prevara temelji predvsem na dejstvu, da finančni trgi za te vrednostne papirje dejansko obstajajo in so največkrat hitro rastoči, naložbe v njih pa aktualne in potencialno lahko prinesejo velike donose, vendar prevaranti praviloma ne vlagajo v te (realne) finančne trge, temveč jih uporabijo samo za snubljenje potencialnih žrtev oziroma za vabo, na katero se ujamejo vlagatelji. Najpogostejše so prevare:

- *pri trgovanju z emisijskimi kuponi (trgovanje z dovoljenji za izpuste emisij CO2)*: trgovanje s certifikati za izpust emisij CO2 predstavlja priložnost za ustvarjanje dobičkov, predvsem z vidika vedno ostrejše zakonodaje na področju ekologije ter zahtev po omejevanju izpustov toplogrednih plinov v ozračje; obseg trgovanja s tovrstnimi vrednostnimi papirji se zato povečuje, vendar ne obstajajo sekundarni trgi, ne glede na trditve tistih, ki tovrstne investicijske priložnosti nudijo (neukim in neprofesionalnim) vlagateljem;
- *pri vlaganju v t. i. investicijske sheme, ki nudijo hitre in visoke zaslužke, kamor sodijo tudi Ponzijeve in piramidne sheme*: obljubljajo visoke (višje) donose in/ali dividende v primerjavi s tradicionalnimi investicijami, donose pa izplačujejo na podlagi denarnih prilivov novih vlagateljev. Shema se sčasoma zruši, ker novi investitorji in njihovi vložki preprosto ne morejo pokriti izplačil obljubljenih donosov tistim vlagateljem, ki so se shemi (piramidi) pridružili pred njimi;
- *pri investicijah v redke materiale, ki jih uporablja proizvodnja za visoko tehnološke izdelke*: nedvomno obstaja povpraševanje po tovrstnih materialih, vendar jih proizvodna podjetja praviloma odkupujejo od velikih dobaviteljev,

2 *Ponzijeva shema (tudi Ponzijeva piramida) se imenuje po italijanskem priseljencu* Charlesu Ponziju *(1882–1949) v ZDA. Na začetku dvajsetih let 20. stoletja je vlagateljem obljubljal 50-odstotni dobiček v 45 dneh ali 100-odstotni v 90 dneh, češ da pri tem izkorišča razliko med cenami ameriških in italijanskih poštnih kuponov (Ponzijeva shema, 2015). Ponzijeva shema je sistem, po katerem se denar novih vlagateljev v denarni verigi uporablja za poplačilo starih vlagateljev. Propade, ko ni več novih denarnih prilivov in organizator ne zmore več nadzirati sheme. Propade tudi, če si organizator prilasti denar vlagateljev ali se ugotovi, da premoženje, na katerem shema temelji, sploh ne obstaja.*

ki lahko zagotovijo ustrezne količine in izpolnijo ostale pogoje, ne pa od malih vlagateljev; obstaja velika verjetnost, da gre pri tovrstnih naložbenih priložnostih za prevaro, še posebej, če gre za investicijo, ki jo zaradi geografske oddaljenosti investitor v večini primerov ne more preveriti (npr. rudnik v Afriki);

- *investicijske sheme, povezane z naložbami v zemljišča*: prevaranti večje zemljišče (praviloma gre za manj vredno in nezazidljivo, v lepem naravnem okolju) odkupijo, razkosajo na manjše parcele in jih naprej tržijo kot naložbeno priložnost za investitorje; pri prodaji je ključna informacija, da bo v prihodnosti prišlo do spremembe in bo zemljišče postalo zazidljivo ter seveda, da obstaja investitor, ki bo zemljišče (od vseh investitorjev) kupil in ga razvijal naprej v dobičkonosen projekt. Vlagatelji praviloma ostanejo z neuporabnimi parcelami, ki so jih drago plačali, vse ostale informacije, ki so jim bile ob nakupu posredovane, pa se izkažejo za neresnične;
- *investicijske sheme, povezane z naložbami v zemljišča v tujih deželah v povezavi s pridelavo različnih pridelkov (nasadi oziroma plantaže)*: gre za vstop investitorja v naložbo v začetni fazi investicije; vlagatelju se obljublja visoke donose ob prodaji plantaže, praviloma za časovno obdobje petih let. V praksi se velikokrat izkaže, da investicije v zemljišča v tujih deželah sploh niso izvršene in da plantaže ne obstajajo;
- *pri vlaganju v delnice, predvsem pri trgovanju mimo organiziranih finančnih trgov* (t. i. »penny stock«, s katerimi se trguje v »boiler rooms«): gre za delnice, ki ne izpolnjujejo pogojev, da bi lahko kotirale na organiziranih trgih; velikokrat gre za močno precenjene delnice, nič vredne ali celo za neobstoječe delnice, investitorjem pa agresivni prodajalci obljubljajo visoke donose;
- *investicije v neavtorizirano forex trgovanje oziroma trgovanje z različnimi izvedenimi finančnimi instrumenti*: praviloma ne gre za (pravo) trgovanje na finančnih trgih, namenjenih trgovanju s (pravimi) izvedenimi finančnimi instrumenti, temveč prevaranti uporabijo imena (oznake) teh instrumentov zato, da privabijo vlagatelje;
- *investiranje v delnice z omejitvijo družb iz ZDA*: gre za nakup delnic ameriških družb, ki niso dovolj kakovostne, da bi kotirale na organiziranih trgih, zato so označene z omejitvijo, kar pomeni, da kupec za določeno obdobje (največkrat šest mesecev do enega leta) delnic ne more prodati nazaj prodajalcu brez zahteve, da se omejitev na delnici odpravi. Tudi po preteku predpisanega časa je treba odpraviti omejitve delnice, to pa lahko investitor doseže samo preko ameriškega odvetnika. Slednje je povezano z visokimi administrativnimi stroški, kar v praksi pomeni, da znašajo stroški prodaje več, kot je vrednost delnic.

2.1 Naložbene prevare v Sloveniji

V slovenski pozitivno-pravni ureditvi je *sedes materiae*[3] prevare največkrat v kaznivem dejanju »Goljufije« (KZ-1, 2008: 211. čl.). Dejanski stani kriminalitete s tega področja, konkretno naložbene prevare, pa lahko odražajo zakonske stane

3 *Lat.: Mesto v zakonu, ki je odločilno za reševanje nekega vprašanja.*

tudi katerega od naslednjih kaznivih dejanj: »Organiziranje denarnih verig in nedovoljeno prirejanje iger na srečo«[4] (KZ-1, 2008: 212. čl.), »Poslovna goljufija«[5] (KZ-1, 2008: 228. čl.), »Preslepitev pri poslovanju z vrednostnimi papirji«[6] (KZ-1, 2008: 231. čl.) ali »Zloraba trga finančnih instrumentov«[7] (KZ-1, 2008: 239. čl.).

Bernik in Prislanova (2012) ugotavljata, da se (tudi) v kibernetskem prostoru pojavlja vedno več finančne kibernetske kriminalitete. Tako npr. storilci zlorabljajo prestrežene ali s hekanjem pridobljene podatke s kreditnih kartic, uporabljajo metode phishinga, nameščanja škodljive programske opreme in podobno, vse z namenom, da bi z zlorabo pridobljenih podatkov pridobili protipravno premoženjsko korist ali prali denar s pomočjo nedolžnih žrtev. Ne smemo pa spregledati dejstva, da internetno okolje predstavlja zelo primerno okolje za izvajanje najrazličnejših oblik prevar, od Nigerijskih pisem prodaje ponarejenih ali ničvrednih izdelkov, lažnih ženitnih oglasov do promoviranja naložbenih priložnosti. Ta sodobna pot v trenutku doseže veliko število potencialnih žrtev, samo delovanje pa je preprosto in povezano z nizkimi stroški. Bernik in Meško (2011) opozarjata, da je moč formalnega družbenega nadzorstva – prav zaradi elementa zapletenosti in kompleksnosti sodobnih tehnologij ter globalnosti – pri preiskovanju kaznivih dejanj na področju finančne kriminalitete, ki kot sredstvo izvršitve uporablja informacijsko-komunikacijske tehnologije, bistveno manjša kot v primeru vsakodnevne premoženjske in nasilniške kriminalitete.

V svetovnem merilu sodi med najbolj znane in odmevne goljufije finančna piramida Bernarda Madoffa[8], vendar je tudi Slovenija prava Meka za finančne prevarante, ki v naivnih vlagateljih vidijo odlično priložnost za zaslužek.

4 *(1) »Kdor organizira, sodeluje ali pomaga pri organiziranju ali izvajanju denarnih verig, pri katerih udeleženci vplačujejo denarne zneske organizatorjem ali drugim udeležencem, ki so se pred njimi vključili v igro ali dejavnost in pričakujejo plačilo določenih denarnih zneskov od udeležencev, ki naj bi se za njimi vključili v tako igro ali dejavnost, se kaznuje z zaporom do treh let.« (KZ-1, 2008: 212. čl.)*

5 *(1) »Kdor pri opravljanju gospodarske dejavnosti pri sklenitvi ali izvajanju pogodbe ali posla preslepi drugega s prikazovanjem, da bodo obveznosti izpolnjene, ali s prikrivanjem, da obveznosti ne bodo ali ne bodo mogle biti izpolnjene, zaradi delne ali celotne neizpolnitve obveznosti pa si pridobi premoženjsko korist ali nastane za stranko ali koga drugega premoženjska škoda, se kaznuje z zaporom do petih let.« (KZ-1, 2008: 228. čl.)*

6 *(1) »Kdor zaradi trgovanja z delnicami, drugimi vrednostnimi papirji ali drugimi finančnimi instrumenti lažno prikaže premoženjsko stanje, podatke o dobičku ali izgubi ali druge podatke v prospektu, pri objavi letnega poročila ali na drug način, ki pomembno vplivajo na njihovo vrednost, in s tem zapelje eno ali več oseb, da jih kupijo, prodajo ali z njimi na drug način poslujejo, se kaznujejo z denarno kaznijo ali z zaporom do dveh let.« (KZ-1, 2008: 231. čl.)*

7 *(1) »Kdor, zato da bi sebi ali komu drugemu pridobil protipravno premoženjsko korist, s prepovedanim ravnanjem zlorabi trg finančnih instrumentov tako, da:*
1) sklene posel ali izda naročilo za trgovanje, ki udeležencem trga da napačno ali zavajajočo predstavo glede ponudbe, povpraševanja ali cene finančnega instrumenta, ali s tem ena ali več povezanih oseb zagotovijo ceno enega ali več finančnih instrumentov na nenormalni ali umetni ravni,
2) pri sklenitvi posla ali izdaji naročila za trgovanje uporabi fiktivna sredstva ali druge oblike goljufivega ravnanja;
3) razširja napačne ali zavajajoče informacije o finančnih instrumentih, z istim ciljem razširja govorice ter napačne in zavajajoče novice po medijih, medmrežju ali na drug podoben način, se kaznuje z zaporom do treh let.« (KZ-1, 2008: 239. čl.)

8 *Bernard Madoff je v skoraj tridesetih letih vlagatelje, ki so varčevali v njegovem hedge skladu, opeharil za vsaj 65 milijard ameriških dolarjev ter bil zaradi te goljufije obsojen na 150 let zapora (Bernard Madoff, 2016).*

Slovenci smo se opekli z že kar nekaj finančnimi piramidami. V devetdesetih letih prejšnjega stoletja sta bili med najbolj razvpitimi Fair Play in Catch the Cash. V obeh primerih je šlo za prevaro, denarna veriga pa je temeljila na nenehni širitvi števila igralcev, ki so prinašali svež denar. Ta se je stekal na račun ustanovitelja verige, on pa je svoje igralce nagrajeval s sorazmernim deležem nagrade glede na to, kako so širili svoj del verige (Milič, 2015).

Podobne sheme pa nastajajo tudi v sodobnejšem času. Večina je vezana na navidezno trgovanje na valutnih trgih, ponudniki vlagateljem obljubljajo bajne donose, jih k sodelovanju vabijo z zlaganimi poročili o preteklih donosih ter obljubljajo lepe nagrade – provizije, če bodo v sistem pripeljali nove vlagatelje. Eden bolj znanih tovrstnih sistemov pri nas, ki je zacvetel v letu 2008, torej na začetku finančne in gospodarske krize, je bil Finanzas Forex (FFX), za katerega je vlagatelje novačil Nello Marconi, lastnik družbe Remius. Gole (2013) o razpletu v zvezi s to finančno verigo poroča: »Slovenski Madoff so mediji poimenovali Nella Marconija, ki v zaporu preživlja devetletno zaporno kazen. Marconi je namreč prepričal 14 vlagateljev, da so mu s posojilnimi pogodbami zaupali 727.000 evrov, za katerimi je izginila vsaka sled. Marconi je največjo finančno piramido v Sloveniji osnoval prek družbe Remius, ki je v stečaju. Okoli 200 upnikov je v stečaju prijavilo za 9,2 milijona evrov terjatev, stečajna upraviteljica Staška Mrak Jamnik pa jih je priznala za 5,6 milijona evrov.«

Na sodišču je bila pravnomočno končana tudi afera Zdenex. Protagonista, zakonca Marjan in Manica Čare, sta bila obsojena na zaporno kazen, saj sta prek družbe Zdenex med letoma 1995 in 1996 zbirala denar vlagateljev, katerim sta obljubljala štiri- in petodstotne mesečne obresti. Tožilstvo je v postopku ugotovilo, da sta zakonca v lasten žep pospravila 1,1 milijona evrov (Gole, 2013).

Podoben koncept prevar kot denarne verige ali sheme so tudi vabila k vpisu deležev ali delnic različnih velikopoteznih in obetavno zvenečih podjetniških projektov, za katere se pozneje izkaže, da so propadli, pobudniki oziroma organizatorji pa zbrana sredstva tako ali drugače spretno kanalizirajo v svojo korist.

Uradnih podatkov o obsegu naložbenih prevar v Sloveniji ni na voljo. Po podatkih policije (Policija, 2016) je bilo v letu 2015 na področju gospodarske kriminalitete obravnavanih 172 primerov goljufije, kar je za dobrih 25 odstotkov manj kot v letu 2014, ko je policija beležila 272 takšnih primerov. Škoda, povezana z obravnavanimi primeri, je v letu 2015 znašala skoraj 10 milijonov evrov, v letu 2014 pa skoraj 11 milijonov evrov. Velja poudariti, da v to niso vštete samo naložbene prevare, temveč vsa kazniva dejanja goljufije.

Agencija za trg vrednostnih papirjev (ATVP) (n. d.) posreduje v zvezi z naložbenimi prevarami splošne informacije o vlaganju v vrednostne papirje in finančne instrumente v Republiki Sloveniji, prav tako pa izdaja obvestila za javnost o zaznavanju morebitnih naložbenih prevar. Na njenih spletnih straneh lahko slovenski investitorji preberejo tudi obvestila za javnost ESMA (*European Securities and Markets Authority*) in IOSCO (*International Organization of Securities Commissions*). ESMA je neodvisna agencija Evropske unije, ki skrbi za zaščito in stabilnost finančnega sistema Evropske unije, predvsem z vidika zaščite investitorjev in promocije stabilnih in urejenih finančnih trgov v Evropski uniji. Podobno vlogo in cilje ima na mednarodni ravni organizacija IOSCO.

V praksi se za naložbene priložnosti, ki se v nadaljevanju izkažejo kot finančne prevare, največkrat ugotovi, da ponujeni naložbeni produkti v Sloveniji niso registrirani oziroma ponudniki nimajo dovoljenja za trženje produkta v Sloveniji v smislu poslovne registracije, podružnice, licence in/ali registracije pri našem ATVP ali pri sorodni instituciji katere druge države članice EU. Ker je veliko finančnih prevar mednarodnega značaja oziroma niso omejene na neko lokalno okolje, je toliko bolj pomembno mednarodno sodelovanje med institucijami, ki skrbijo za regulacijo finančnih trgov ter obveščanje investitorjev o naložbah brez ustrezne avtorizacije pristojnih organov.

2.2 Viktimizacijske študije s področja naložbenih prevar

Uporaba besednih zvez »problem storilca in žrtve« (MacDonald, 1939), »dvojni okvir zločina« (Von Hentig, 1948) ali bolj splošno »odnos storilca in žrtve« (Schafer, 1968; Schultz, 1968; Von Hentig, 1948) jasno kaže na pomen vloge žrtve pri preučevanju kriminalitete (Sank in Caplan, 2007). Garofalo (1914) je bil eden prvih, ki je pokazal, da žrtev velikokrat pogojuje napad nase, medtem ko je Mendelsohn (Dussich, 2016) oblikoval teorijo, v kateri je opredelil tipologijo žrtev glede na njihov prispevek k viktimiziranosti. Von Hentig (1948) se je na drugi strani ukvarjal s tipologijo žrtev ter jih razdelil v skupine glede na njihove značilnosti, zaradi katerih so posamezniki pogostejše žrtve kriminalitete. Vsem tem teorijam oziroma pogledom je skupno to, da nakazujejo na dejstvo, da določeni posamezniki s svojimi ravnanji, obnašanjem ali zaradi osebnostnih značilnosti pomembno prispevajo k verjetnosti, da bodo postali žrtve kaznivega dejanja.

Čeprav ena izmed opredelitev znanstvene vede viktimologije govori o ukvarjanju s preučevanjem kriminalitete predvsem z vidika žrtve, s poudarkom na zvezi med žrtvijo in storilcem (Meško, 1998), pa Pečar (1984) razširja polje obravnave in vpeljuje pojem induktologije, s katerim opiše vplivanje na kazensko dvojico. Predstavi pomen delovanja v skupini na samo dinamiko izvršitve kaznivih dejanj oziroma na ustvarjanje preddeliktnih situacij. Ugotavlja, da »dvojica (tj. storilec in žrtev, op. a.) ni edina, ki kakorkoli ustvarja posledice. Kazenski par je pogosto to, kar je postal, sam »žrtev« vpletenih ali tretjih oseb, je njihova igrača, ali pa je eden od njiju oziroma kar oba orodje subjekta v ozadju.« (Pečar, 1984: 299).

Viktimizacijske študije so bile tradicionalno ozko usmerjene na klasično (konvencionalno) kriminaliteto med posamezniki, zlasti na premoženjske in uličnе nasilne oblike kriminalitete, ne pa na primer na viktimološke posledice gospodarskega »kriminala močnih« (Walklate, 2012). Empirična viktimologija kaže, da kriminalitetna viktimizacija ni naključno porazdeljena po populaciji (Walklate, 2012), času in prostoru (Kanduč, 2002). Pregled viktimizacijskih študij pokaže, da je tipična najpogostejša žrtev klasične kriminalitete mlad moški nižjega družbenega razreda (Kearon in Godfrey, 2007), nezaposlen, neporočen, z družbenega obrobja (Fattah, 1991). Primerjava žrtev t. i. beloovratniške kriminalitete in klasične kriminalitete (Ganzini, McFarland in Bloom, 1990) pa je pokazala na nekatere faktorje, ki kažejo na večje tveganje za posameznika, da bo izpostavljen kriminaliteti – tako ugotavljajo, da se verjetnost, da bodo posamezniki žrtve klasičnih kaznivih dejanj,

predvsem nasilnih, kot so posilstvo, rop ali napad, prepolovi pri posameznikih, katerih letni prihodki so večji od 15.000 ameriških dolarjev; na drugi strani pa se verjetnost, da posameznik postane žrtev beloovratniške kriminalitete, katere značilnost je predvsem zavajanje in uporaba nenasilja za pridobitev materialne koristi, veča z večanjem premoženja oziroma prihodkov posameznika.

Na podlagi kvantitativne raziskave iz leta 2014 (National Fraud Authority, 2014) o žrtvah naložbenih prevar lahko orišemo značilnosti žrtve naložbene prevare – gre za dva segmenta, ki ju lahko označimo:

- »starejši s premoženjem«, kjer je raziskava pokazala, da obstaja 3,5 krat večja verjetnost za viktimizacijo (najverjetneje bo to moški, star več kot 65 let, z denarnimi sredstvi, ki jih želi vložiti v finančne naložbe, v višini več kot 10.000 angleških funtov) ter
- »zrel in sposoben«, kjer je verjetnost za viktimizacijo 2,5 krat večja kot pri ostali populaciji (v tej skupini bo to najverjetneje moški, višje izobražen, ki se zanima za različne priložnosti).

Raziskava za *Financial Conduct Authority* (Harvey, Kerr, Keeble in McNaughton Nicholls, 2014) pa je pokazala še druge razsežnosti, ki vplivajo na verjetnost, da posameznik postane žrtev naložbene prevare: ne gre zgolj za lastnosti posameznika, ki vplivajo na verjetnost, da bo posameznik žrtev naložbene prevare, temveč lahko na podlagi te raziskave sklepamo na dodatne značilnosti življenjskega sloga posameznikov, ki ključno vplivajo na izpostavljenost – raziskava je opredelila tri faktorje kot ključne:

- finančno stanje posameznika,
- njegove okoliščine glede družine oziroma pomembnih odnosov ter
- psihološko stanje posameznika ob sprejemanju odločitve za pristop k naložbi.

Govorimo lahko o kontekstu, znotraj katerega se zgodi naložbena prevara.

2.3 Kontekst, znotraj katerega se zgodi prevara

Ravnanja žrtev finančnih prevar so velikokrat dojeta kot iracionalna. Podroben vpogled v kontekst okoliščin, znotraj katerih se žrtev odloča, glede na informacije, ki jih ima na voljo, ter način, kako so jim te informacije predstavljene, pa ugotovimo, da je z vidika zornega kota žrtve njeno odločanje racionalno, ne iracionalno. Somerville in Bengtsson (2002) govorita o racionalnem delovanju znotraj konteksta: glede na informacije, ki jih večinoma selektivno in manipulativno žrtvi posreduje storilec prevare, ter glede na ostale okoliščine v trenutku, ko žrtev sprejme odločitev o naložbi, lahko ugotovimo, da je žrtvino ravnanje v tem navidezno logičnem okvirju – navidezno logičnem zato, ker ga kot takšnega predstavi in vzpostavi storilec prevare – v trenutku sprejetja ključne odločitve, da pristopi k naložbi, logično in racionalno.

Ta koncept lahko dodatno poglobimo z vpogledom in razumevanjem mehanizma, ki ga je Seto (2013) poimenoval »snubljenje«. Čeprav je koncept snubljenja poznan predvsem iz raziskav kibernetske kriminalitete, kjer so obravnavane žrtve otroci, pa ugotovitve (O'Connell, 2003; Whittle, Hamilton–

Giachritisis, Beech in Collings, 2013) glede stopenj oziroma faz privabljanja, procesa snubljenja ter taktik, ki jih storilci prevar uporabljajo, da prevarajo žrtve oziroma da jih spodbudijo k določenim ravnanjem, lahko preslikamo tudi na področje finančnih prevar. Storilci naložbenih prevar uporabljajo najrazličnejše preslepitve, s katerimi pri žrtvah ustvarijo vtis, da gre za zaupanja vreden in pošten dogovor med storilcem in žrtvijo. Storilci uporabljajo profesionalno dokumentacijo, svoje potencialne stranke sprejemajo v okoljih, ki dajejo vtis strokovnosti in sofisticiranosti, posle pa predstavljajo v prodajnih tehnikah dobro izučeni in pretkani prodajalci. V procesu snubljenja storilec prevare zvabi žrtve v odnos, v katerem se žrtev emocionalno naveže (poveže) s storilcem. Pri tem storilci za preslepitev uporabijo različne tehnike privabljanja/izrabljanja žrtev, vključno s tem, da s svojimi žrtvami zgradijo odnos, ki temelji na prijateljstvu in zaupanju, ter da vzpostavijo z žrtvijo odnos, v katerem žrtev čuti, da storilcu prevare dolguje (npr. da mora vplačati denar v naložbo, ker se je storilec tako potrudil zanjo) v zameno za odnos, ki ga je storilec prevare pripravljen oblikovati z žrtvijo. Storilci prevar velikokrat svojo žrtev tudi izolirajo od drugih ljudi oziroma od njihove socialne mreže, največkrat tako, da žrtvi dajejo in odvzemajo pozornost glede na to, kako se žrtev »obnaša« in upošteva napotke storilca. Čeprav storilci prevar »prodajajo« žrtvam različne finančne in druge produkte, pa žrtve poročajo o podobnih preslepitvenih metodah ter opisujejo podobne procese, skozi katere jih manipulacijsko »vodijo« storilci prevar. Ne glede na opaženo podobnost, pa je vsaka preslepitev edinstvena: edinstvenost določa odnos storilca prevare do žrtve ter uporaba taktik manipulacije, s katerimi storilec prevare izkorišča življenjske okoliščine posameznika v določenem trenutku.

Ob pomoči teorij »snubljenja« ter »racionalne aktivnosti v kontekstu« lahko utemeljimo tudi racionalnost žrtev, ki izkusijo finančno prevaro večkrat, čeprav so te žrtve (še) večkrat dojete kot iracionalne, torej kot posamezniki, ki vstopajo v proces viktimizacije navkljub opozorilom drugih ljudi na posledice njihovih odločitev. Lyng (2005) govori o teoriji prostovoljnega prevzemanja tveganj, o »delovanju na robu«. Kot »delovanje na robu« označi tiste aktivnosti, ki posamezniku ob izvajanju prinašajo poleg zadovoljstva ob dejstvu, da obvladuje izvajanje te aktivnosti, tudi čustveno intenzivnost, ki jo le-ta doživlja, medtem ko izvaja te aktivnosti. Toda čustvena razsežnost prostovoljno prevzetega tveganja ni samo želja po doživetju intenzivnih čustev, proces vključuje tudi njihov nadzor in ravno občutek nadzora nad intenzivnimi čustvi je tista nefinančna nagrada, ki spodbudi posameznike, da navkljub negativnim preteklim izkušnjam ponovno vstopijo v proces snubljenja in na tak način postanejo večkratne žrtve finančnih prevar.

Poti prepričevanja *(angl. routes to persuasion)* (Langenderfer in Shimp, 2001) igrajo pomembno vlogo v procesu odločanja. Gre za vprašanje, na kakšen način nekoga prepričamo, da si izbere določeno opcijo. Modic (2010) govori o dveh možnostih oziroma poteh:

- *centralno* oziroma neposredno prepričevanje, kjer naj bi sistemski in logični argumenti pripeljali do ugodne reakcije in spodbudili osebo na drugi strani, da globoko razmisli in sprejme optimalno izbiro,
- druga pot pa je t. i. *periferna* oziroma posredna, kjer iščemo bližnjice in emocionalne reakcije, ki naj spodbudijo osebo na drugi strani, da ne razmišlja, ampak se preprosto strinja z nami.

Petty in Cacioppo (1981) periferno pot prepričevanja označita kot način prepričevanja, ki ne temelji na argumentih oziroma kontekstu, ki je pomemben za sprejetje odločitve. Za vplivanje na odločitev tisti, ki želi prepričati, uporablja drugačne mehanizme, ki niso v povezavi z okoliščinami odločitve, npr. prijeten glas, atraktivnost govornika, ustvarjanje občutka kompetentnosti.

2.4 Posledice viktimizacije in opolnomočenje žrtev

Žrtve finančne kriminalitete velikokrat opredelijo svoje doživljanje prevare kot grobo kršitev njihove osebne integritete in zaupanja ter to stanje opišejo kot psihološko »poškodovanje«. Le-to praviloma ni razumljeno kot tako resno stanje kot fizične poškodbe, ki jih žrtve doživijo pri drugih tipih napadov, predvsem pri kriminaliteti, ki je povezana z različnimi stopnjami fizičnega nasilja; prav tako psiholoških »ran« žrtev finančne kriminalitete ne dojemamo v enakem smislu kot psihološko trpljenje in viktimizacijo žrtev spolnih napadov, zato so posledice, ki jih ima finančna kriminaliteta na žrtve, velikokrat nepravilno razumljene in je njihov pomen za posameznika in družbo podcenjen. Žrtve t. i. beloovratniške kriminalitete utrpijo, za razliko od žrtev klasične kriminalitete, ki je povezana s fizičnim nasiljem, »poškodbe«, ki jih velikokrat ne opazimo, ker so večinoma notranje in niso vidne navzven. Ne glede na dejstvo, da so poškodbe žrtev prevar navzven nevidne, pa to še ne pomeni, da žrtve tovrstne kriminalitete ne potrebujejo ustrezne obravnave in pomoči.

Alexander in Seymour (1998) odlično predstavita, kako viktimizacijo doživljajo žrtve prevar, in sicer: kaznivo dejanje s področja finančne kriminalitete pomeni nasilje nad posameznikom. Pomeni, da je zaupanje v lastno presojo ter zaupanje v drugega pri oškodovancu porušeno. Oškodovanec lahko občuti izdajo, še posebej v primerih, ko ga je prevaral nekdo, ki ga je poznal in mu zaupal.

Izguba zaupanja v lastno presojo ter zaupanja v druge pa ni edino, s čimer se morajo soočati žrtve finančne kriminalitete. Finančne prevare velikokrat ogrozijo ali celo porušijo finančno varnost posameznika ter drugih, ki so na kakršen koli način odvisni od njegove finančne varnosti. V tem smislu so še posebej ogroženi starejši, bolni, invalidni oziroma vsi, ki nimajo možnosti nadoknaditi finančno izgubo – ob takšnem dogodku se lahko soočijo še z dodatno travmo ali celo izgubijo svojo samostojnost (Alexander in Seymour, 1998).

Weisburd, Wheeler, Waring in Bode (1991) poročajo o procesu okrevanja in izzivih, s katerimi je soočena žrtev finančne prevare. V prvi vrsti govorijo o samoobtoževanju žrtve, ki je lahko v nekaterih primerih celo večje kot pri žrtvah, ki so doživele viktimizacijo drugih oblik kriminalitete, ter porušenem zaupanju v lastne sposobnosti za sprejemanje odločitev in o težavah pri vzpostavljanju zaupanja do drugih ljudi. Finančna prevara pa nima vpliva samo na oškodovanca, temveč pušča sledi tudi na prijateljih in družini žrtve. Marsikateri posameznik je, ne vedoč, da gre pri naložbi za prevaro, le-to priporočal še svojim sorodnikom in prijateljem ter je v fazi okrevanja, torej v času, ko bi najbolj potreboval podporo in pomoč ter razumevanje bližnjih, soočen tudi z obtožbami vseh tistih, ki jih je brez slabega namena zapeljal v prevaro. V fazi okrevanja žrtev lahko doživi tudi izolacijo, marsikdo pa tudi veliko spremembo v pomembnih odnosih: ločitev,

izgubo prijateljstev, razdor med sorodniki. Žrtve odsotnost zaključka procesa okrevanja po prevari prav tako doživljajo s precejšnjo stopnjo stresa: žrtve morda po prevari nikoli ne bodo soočene s storilcem. V primeru, da se bodo soočile s storilcem, pa obstaja možnost, da bo storilec v kazenskem postopku zaradi kakšnega koli razloga oproščen in žrtve ne bodo doživele niti moralnega zadoščenja.

Žrtve naložbenih prevar kot skupina, ki je doživela (praviloma) nenasilno viktimizacijo, je v svojih odzivih na viktimizacijo podobna žrtvam, ki so doživele nasilno (personalizirano – tj. napad na življenje ali telo, kazniva dejanja zoper spolno nedotakljivost oziroma premoženjsko kaznivo dejanje) viktimizacijo, čeprav včasih posledice nenasilne viktimizacije podcenjujemo in jih obravnavamo z manjšo zavzetostjo, kot posledice nasilne viktimizacije. Meško (1998) v analizi nekaterih razsežnosti nasilne viktimizacije prav tako ugotavlja najrazličnejši spekter odzivov posameznikov na kaznivo dejanje in njegove posledice: od povečanega nezaupanja in občutljivosti, občutkov jeze, sramu, strahu, anksioznosti, do pripisovanja lastne krivde glede (neustreznega) odziva kriminalcu. Na to, kako žrtev dojema svojo vlogo v samem procesu viktimizacije, lahko močno vplivajo tudi člani družine, kazensko pravosodje, družba in drugi, s tem pa žrtvi bodisi olajšajo ali pa otežijo proces reorganizacije in opolnomočenja po stresnem dogodku.

Učinki kriminalitetne viktimizacije so torej raznoliki in nepredvidljivi, dolgotrajnejše pa so navadno čustvene posledice, ki jih veliko žrtev podcenjuje (Dunn, 2007). Muršič (2006) opozarja, da je treba čustvene vidike viktimizacije posebej upoštevati. Med neprijetna čustva, ki predstavljajo odziv na kriminalitetno viktimizacijo, uvrščamo strah oziroma doživljanje ogroženosti, ranljivosti in nemoči, tesnobo, zaskrbljenost, jezo, žrtev pa lahko doživlja tudi sram, občutke ponižanosti ali krivde, obupanost in nizko samospoštovanje. Govorimo o odzivih, ki so rezultat žrtvinega dojemanja, interpretiranja viktimizacijskega dogodka in njegove škodljivosti v povezavi z žrtvinim sistemom vrednot.

Tudi sekundarna viktimizacija zaradi neustreznega formalnega ali neformalnega obravnavanja žrtev je za mnoge žrtve vir dodatne viktimizacije (Wolhuter, Olley in Denham, 2009). Študije so pokazale, da velik delež žrtev ni zadovoljen z ravnanjem policije in njenim odzivanjem na potrebe viktimiziranih (Van Dijk, 1999).

Van Dijk (1999) nadalje ugotavlja, da je vprašanje prijavljanja lastne viktimiziranosti, povezano s kombinacijo moralnih, legalnih, finančnih in praktičnih pomislekov žrtev, predvsem v smislu, ali je ovadba res v interesu žrtev; na to odločitev vplivajo tudi pričakovanja žrtve, kakšen bo odziv institucij ter od značilnosti odnosa med žrtvijo in storilcem (Davies, Francis in Jupp, 2003). Žrtve finančne kriminalitete poročajo, da jih sodelovanje v predkazenskem in kazenskem procesu izpostavlja nelagodju in stresu zaradi različnih razlogov: nepoznavanje kazenskega procesa in njihove vloge ter različnih možnosti podpore, ki so jih v tem procesu lahko deležne, strah pred soočenjem s povzročiteljem prevare, strah pred sodbami in predsodki drugih, njihovimi ravnanji in odnosom, strah pred tem, da bi bili javno izpostavljeni kot oškodovanci v zvezi s kaznivim dejanjem, še posebej v primerih, ko za oškodovanje žrtve niso povedale nikomur.

Vplivi posledic viktimizacije na fizično in duševno zdravje žrtev finančnih prevar niso bili širše raziskani, saj se večina študij osredotoča na žrtve kaznivih dejanj, ki sodijo v skupino nasilne kriminalitete. Študije, ki pa so bile izvedene na žrtvah nenasilne kriminalitete, pa kažejo, da ima doživetje finančne prevare resen vpliv na fizično in duševno zdravje žrtev (Ganzini et al., 1990), saj avtorji poročajo tudi o večji dovzetnosti žrtev za stanja, kot sta depresija in povečanje tveganja za samomor. V Ganzinijevi študiji (v kateri so obravnavali 77 žrtev velikih finančnih prevar, ki so se zgodile v osemdesetih letih prejšnjega stoletja v Oregonu, ZDA), eni redkih študij o vplivu finančnih prevar na psihološko zdravje/stanje žrtev, je bilo ugotovljeno, da je 29 odstotkov anketiranih doživelo resno depresivno epizodo po doživetju prevare v primerjavi z dvema odstotkoma iz kontrolne skupine, pet žrtev je razvilo samomorilska nagnjenja, 45 odstotkov pa je občutilo in kazalo znake tesnobnosti in depresije. Študija je pokazala, da je doživljalo kar 48 odstotkov tistih, ki so doživeli resno depresivno stanje, izrazite znake depresije še šest mesecev kasneje. Avtorji študije so sklepali, da so navedeni simptomi rezultat skupka dogodkov, ki so pri posamezniku povzročili dolgotrajno bolezensko stanje: finančna prevara je sprožitelj nadaljnjih negativnih dogodkov, kot je izguba doma ali težave pri poravnavanju obveznosti, davkov ter vračilu dolga. (Ganzini et al., 1990)

Ena od ključnih nalog viktimologije je oblikovanje mehanizmov za pomoč žrtvam v okviru kazenskega sistema in širše, ki bodo osebno in strukturno ranljive žrtve opolnomočili (Muršič, 2012). Razumevanje pomena in razsežnosti problemov, ki so povezani z ustrezno obravnavo žrtev, je kot najustreznejši pristop k obravnavanju žrtev izpostavilo priznavanje njihovih mednarodno opredeljenih pravic in zavzemanje za njihovo učinkovito uveljavljanje v skladu z načelom enakosti. Sodobne organizacije za pomoč žrtvam niso več zasnovane na konceptu potreb, temveč vse bolj na konceptu pravic (Dunn, 2007), kar vključuje tudi pravico do enake dostopnosti pomoči za žrtve iz vseh družbenih skupin, ne glede na njihov strukturni položaj v družbi. Walklate (2012) opolnomočenje žrtev razume kot razumevanje in upoštevanje strukturne podlage žrtev pri vseh oblikah viktimizacije. Van Dijk (1999) glede opolnomočenja poudari pomen organiziranega sistemskega pristopa k nudenju pomoči žrtvam: opolnomočenje, ki ga podpirajo državne institucije in nevladne organizacije, številnim žrtvam pomaga, da se bolje spoprimejo z viktimizacijsko izkušnjo in njenimi posledicami, si vrnejo zaupanje v državo in v povezano, pravično skupnost.

3 ŽRTVE NALOŽBENIH PREVAR

Žrtve naložbenih prevar imajo po navadi drugačen demografski profil kot ostala populacija. Raziskave kažejo (FINRA), da je skoraj dve tretjini žrtev naložbenih prevar poročenih moških. So izobraženi, optimistični in zaupajo vase, imajo nadpovprečni prihodek in so finančno bolj pismeni kot tisti, ki niso oziroma ne postanejo žrtve naložbenih prevar.

Financial Industry Regulatory Authority (FINRA) je na podlagi zbranih podatkov o žrtvah naložbenih prevar in statističnih analiz ugotovila (podatki veljajo za ZDA) nekaj značilnosti v ravnanju vlagateljev in njihovih lastnosti, ki povečujejo možnost, da posameznik postane žrtev naložbene prevare:

- *Preverjanje naložbe in/ali svetovalca pri regulatorju trga:* FINRA ugotavlja, da več kot 80 % vlagateljev nikoli ne preveri, ali ima njihov svetovalec, broker ali prodajalec ustrezno licenco za delo, ki ga opravlja; enako velja za naložbene priložnosti oziroma finančne produkte, ki jih navedeni prodajajo oziroma svetujejo vlagateljem.
- *Vlaganja v visoko tvegane finančne produkte, ki niso ustrezno registrirani:* 73 % poznanih žrtev naložbenih prevar je imelo ali ima naložbe, ki so povezane z večjimi tveganji, če to primerjamo s (samo) 52 % tistih, ki niso postali žrtve. Raziskave nadalje ugotavljajo, da se žrtve naložbenih prevar dvakrat pogosteje odločajo za naložbe s pričakovanimi nadpovprečnimi donosi v primerjavi s kontrolno skupino.
- *Nezmožnost prepoznati taktike prepričevanja in snubljenja:* eden od petih vlagateljev ne prepozna taktik prepričevanja, snubljenja in ostalin načinov manipuliranja z vlagatelji.
- *Zanašanje na lastno presojo pri odločitvi za naložbo in/ali pri izbiri svetovalca:* primerjava strukture naložbe med skupino znanih žrtev naložbenih prevar in skupino tistih, ki prevare niso doživeli, pokaže, da imajo žrtve naložbenih prevar bistveno večji delež svojih naložb – 70 % v primerjavi z več kot dvakrat manjšim deležem v kontrolni skupini – vloženih v naložbo, ki so si jo sami izbrali na podlagi priporočil prijatelja, sorodnika ali sodelavca. Dodatne značilnosti, na katere je opozorila raziskava, kažejo, da vlagatelji iz prve skupine, tj. skupine žrtev naložbenih prevar, bolj zaupajo lastni presoji, se raje in v večji meri zanašajo na svoje občutke in instinkte, kot pa da bi nasvet poiskali pri profesionalnem svetovalcu. Na drugi strani pa v raziskavi ugotavljajo, da je 50 % večja verjetnost, da bo žrtvi naložbene prevare svetoval oziroma prodal finančno naložbo nekdo, ki ga je priporočil prijatelj ali znanec, v primerjavi s skupino vlagateljev, ki ni doživela naložbene prevare.
- *Doseganje potencialnih vlagateljev:* žrtve naložbenih prevar se v primerjavi s kontrolno skupino veliko raje udeležujejo raznih brezplačnih seminarjev, predstavitev in promocij naložbenih priložnosti ter so bolj odzivni na ponudbe, ki jih od neznancev dobivajo preko elektronske pošte (spam sporočila), hladnih klicev preko telefona ali na ponudbe, ki so predstavljene na internetu.
- *Vpliv negativnega življenjskega dogodka:* posamezniki, ki so pred kratkim doživeli negativni življenjski dogodek (resnejše zdravstvene težave, ločitev in podobno), so za več kot 30 % bolj izpostavljeni tveganju, da postanejo žrtve naložbene prevare v primerjavi z vlagatelji, ki tovrstnemu vplivu niso izpostavljeni.

4 PREPOZNATI NALOŽBENO PREVARO

Ljudje, ki so doživeli finančno prevaro, niso (samo) pasivne žrtve. Raziskava, opravljena za *Financial Conduct Authority* (Harvey et al., 2014) na podlagi podatkov, pridobljenih iz poglobljenih intervjujev z žrtvami naložbenih prevar (raziskava je bila izvedena v Veliki Britaniji), o načinih, ki so jih žrtve poskušale uporabiti ali so

jih uporabile, da bi se zaščitile pred prevaro – večina je iskala načine, kako preveriti, ali gre za pristno naložbo ali prevaro – poroča o tem, da so posamezniki preverjali naložbeno priložnost pri različnih virih in vendar so jih storilci prevar z različnimi mehanizmi prepričali, da so vložili svoja sredstva v finančno naložbo, ki se je v nadaljevanju izkazala za prevaro.

Najmočnejša zaščita pred naložbenimi prevarami je znanje. Analiza značilnosti finančnih prevar (FINRA) pokaže na nekaj znakov, pri katerih lahko posumimo, da gre za naložbeno prevaro:

- *Zagotovljeni visoki donosi:* v svetu financ in investiranja je zelo malo zagotovljenega. Na dolgi rok so visoki donosi povezani z visokim tveganjem, kar pomeni, da lahko vlagatelj izgubi tudi celotno glavnico. Prav sprejemanje višjih stopenj tveganja loči investiranje od varčevanja, kjer so donosi lahko vnaprej znani in zagotovljeni, vendar praviloma niso visoki.
- *(Nerazumljivi) kompleksni finančni produkti:* pametno vlaganje v finančne produkte za posameznega investitorja ne sme biti »visoka znanost«. Velika kompleksnost finančnih produktov ali kompleksna naložbena strategija (še) ne zagotavlja visokih donosov, prav tako visoke provizije nujno ne vodijo do nadpovprečnih donosov ali ne kažejo na odlično naložbeno priložnost.
- *Poslovanje brez pogodb in druge dokumentacije:* k pravi naložbi sodi tudi ustrezna dokumentacija o njej. Če svetovalec le-te ne more ponuditi, ker ne obstaja, in hoče vlagatelja prepričati, da mu zaupa samo na podlagi ustnih obljub, je to lahko dokaz, da za lepimi besedami in obljubami ni ničesar razen – prevare.
- *Poslovanje brez dovoljenj in licenc:* preveriti naložbo in svetovalca, ali imajo ustrezna dovoljenja in licence za delovanje, je pravzaprav zelo enostavno – in vendar večina vlagateljev tega ne stori.
- *Stalna, nespremenljiva donosnost naložbe:* vsaka naložba, ki samo raste in nikoli ne »zaniha navzdol«, niti kot odgovor na (negativne) dogodke v svetu, je sumljiva, saj tudi najbolj konservativne naložbe doživljajo nihanja in spremembo vrednosti.
- *Časovni pritisk in omejenost naložbe:* značilna prodajna tehnika, ki jo uporabljajo prodajalci naložbenih prevar in s katerimi ustvarjajo pritisk na potencialno žrtev, je ustvarjanje pogojev nujnosti za hitro odločitev brez premisleka ali posvetovanja z drugimi viri.

5 RAZPRAVA

Pregled literature in viktimoloških raziskav pokaže, da se viktimologi v precej večji meri ukvarjajo z žrtvami t. i. klasičnih kaznivih dejanj oziroma s področjem splošne kriminalitete, predvsem s preiskovanjem žrtev kaznivih dejanj zoper življenje in telo, spolno nedotakljivost ter nasilja v družini, manj pa z žrtvami premoženjskih kaznivih dejanj. V tem smislu so še slabše zastopane viktimizacijske študije s področja gospodarske kriminalitete, čeprav izvedene študije kažejo, da se žrtve tovrstne kriminalitete v enaki (ali celo večji) meri soočajo s posledicami viktimiziranosti. V čem so si žrtve splošne in gospodarske kriminalitete podobne

in v čem se razlikujejo, bi bilo smiselno poglobljeno raziskati, da bi lažje razumeli tako kontekst, znotraj katerega se zgodi prevara (torej, kateri so tisti pogoji v življenju in lastnostih posameznika, ki pripomorejo k temu oziroma odločilno vplivajo na to, da le-ta postane žrtev), kot tudi procese opolnomočenja po naložbeni prevari, vse z namenom pravilno obravnavati žrtve naložbenih prevar ter jim ponuditi ustrezno pomoč in podporo. Ugotovitve predstavljenih raziskav lahko služijo za načrtovanje pomoči žrtvam finančne kriminalitete in bolj sočutni obravnavi v kazenskem postopku.

Raziskava, ki so jo opravili v Financial Industry Regulatory Authority (FINRA, 2016) (podatki veljajo za ZDA), je pokazala, da je vsak deseti vlagatelj v finančne naložbe izgubil nezanemarljivo visok denarni vložek v naložbeni prevari oziroma zaradi nje. Ne gre prezreti njihove ugotovitve, da pri tem ne gre za neizobražene in neuke vlagatelje, ki jim manjka zdrave pameti in osnovnega znanja o investiranju. Prav nasprotno, raziskave jasno kažejo, da so posamezniki, ki so bolje izobraženi, z nadpovprečnimi dohodki, ki sami upravljajo s premoženjem in iščejo priložnosti za oplemenitenje svojih sredstev, še posebej »privlačni« za prevarante in tudi pogosto – pogosteje kot tisti, ki ne sodijo v to kategorijo – žrtve naložbenih prevar in relativno lahek plen za prevarante.

Kljub vse večji osveščenosti posameznikov in povečani občutljivosti pri zaznavi in preganjanju tovrstnih kaznivih dejanj različne študije kažejo (National Fraud Authority, 2014), da je število ljudi, ki so žrtve tovrstnih kaznivih dejanj iz leta v leto večje. Posamezni, medijsko odmevni primeri (v svetovnem merilu npr. primer Bernard Madoff, pri nas Finanzas Forex, Zdenex ali Remius) lahko povzročijo višjo stopnjo strahu, kot je dejanska stopnja ogroženosti za morebitno viktimizacijo. Young (2007) ugotavlja, da so množični mediji spektakularna mesta izključevanja: v javnost prenesejo zaporedje, pravičnost in vključenost (ozadje novice), pri tem pa namenoma poudarjajo napake, nepravičnosti in izključenost ter te elemente postavijo v ospredje. Slednje lahko zaradi slabega poznavanja področja in pogosto nestrokovnega poročanja medijev še dodatno zastraši javnost, kar pa ne pomaga pri osveščanju in izobraževanju posameznikov za sprejemanje pravih, učinkovitih odločitev v zvezi s finančnimi zadevami ter senzibiliziranje javnosti o tem, kaj je družbeno (ne)sprejemljivo ravnanje na tem področju. Podobno, kot za kibernetsko kriminaliteto ugotavljajo Dimc in Dobovšek (2012: 395) ter Bernik in Meško (2011), velja tudi za finančno kriminaliteto: »… nekatere vrste […] kriminalitete postajajo tako razširjene, da so postale družbeno sprejemljive«. Velja pa tudi obratno – družba zavrne sprejemljivost nekaterih pojavov in jih skozi spremembo kazenske zakonodaje tudi kriminalizira. Primer iz finančnega področja družbeno nesprejemljivih in zato kriminaliziranih praks so piramidne sheme.

Viktimološke raziskave s področja prevar ugotavljajo, da se žrtve prevar sramujejo svoje izkušnje (Schichor et al., 2001), se bojijo kritike družinskih članov in avtoritet (Blanco Hache & Ryder, 2011; Croall, 2009) in velikokrat sploh ne prijavijo kaznivih dejanj organom pregona (Goucher, 2010). Žrtve v raziskavah s tega področja poročajo o izrednem (negativnem) vplivu dogodka na njihovo življenje – tako v materialnem kot tudi v čustvenem, psihološkem in zdravstvenem vidiku (Harvey et al., 2014) ter se v svojem doživljanju viktimiziranosti bistveno ne razlikujejo od žrtev druge vrste (predvsem nasilne) kriminalitete.

Ugotovitve raziskav o »snubljenju« žrtev, ki so bile izvedene na vzorcih otrok in mladostnikov, žrtvah kibernetske kriminalitete (Seto, 2013), lahko apliciramo tudi na žrtve naložbenih prevar, saj storilci, kot kažejo raziskave o samih načinih prepričevanja potencialnih žrtev za vlaganje v različne oblike naložb, uporabljajo podobne taktike in strategije, kot jih je opisal in prepoznal Seto (2013). Ugotovimo, da je proces privabljanja potencialnih žrtev k naložbi zahteven in kompleksen. Prevaranti uporabljajo tehnike »snubljenja«, pri tem pa uporabljajo različne taktike, s katerimi vplivajo na potencialne vlagatelje in z njimi manipulirajo. Najpogosteje uporabljene taktike so: taktika »fantomskega bogastva«, s katero nagovarjajo žrtvina hrepenenja po materialnih dobrinah, taktika »vira kredibilnosti«, pri kateri naložbo povežejo z uglednim podjetjem ali osebo ali državo, ki vzbuja zaupanje in kredibilnost, s taktiko »socialnega konsenza« poskušajo prevaranti potencialnega vlagatelja prepričati, da bo pripadal skupini uspešnih posameznikov, če bo pristopil k naložbi, taktiki »reprocitete« in »redkosti« pa nagovarjata potencialnega vlagatelja o ekskluzivnosti ponudbe, nujnosti hitrega ukrepanja in izkoriščanja ugodne priložnosti.

Proces preslepitve, katerega cilj je oškodovanje vlagateljev, lahko na kratko opišemo v naslednjih korakih: vzpostavitev kontakta, izgradnja prijateljstva in zaupanja, vzpostavljanje občutka v žrtvi, da je »posebej izbrana in da ima poseben privilegij«, da ji je storilec pripravljen ponuditi naložbeno priložnost, do katere nima vsak dostopa. Sledi korak, ko storilec svoji žrtvi prikazuje življenje, ki si ga žrtev želi, in jo spodbuja, da bo s predlagano naložbo prišla do denarnih sredstev, s katerimi bo svoje želje tudi uresničila. Z vsakim stikom med storilcem in žrtvijo se zaupanje poglablja, žrtev pa se v določenem trenutku začne počutiti dolžna, da ustreže storilcu, ker se le-ta tako trudi zanjo. Ko storilec začuti, da je zaupanje žrtve dovolj veliko in da je žrtev pripravljena storiti vse po navodilih storilca, storilec žrtev osami z namenom, da ji lahko sam posreduje samo tiste informacije, s katerimi lahko žrtev usmerja in vodi, kot ustreza storilcu. Če se žrtev temu upira, ga »kaznuje« s tem, da ji odvrne svoje prijateljstvo. Storilec naložbene prevare po potrebi in odvisno od situacije uporablja naštete korake, vse z namenom, da se žrtev ne odvrne od njega ter da brezpogojno in nekritično sledi vsem njegovim predlogom in napotkom za naložbe (Harvey et al., 2014).

Opolnomočenje po prevari zahteva od oškodovanca ponovno vzpostavitev zaupanja v lastno presojo ter zaupanja v druge, (ponovno) izgradnjo finančne varnosti, velikokrat pa tudi ponovno izgradnjo socialnih vezi oziroma socialne mreže. Posameznik torej utrpi oškodovanje ne le na materialnem področju, pač pa tudi psihološkem in socialnem. Zaradi visoke stopnje stresa, ki je povezan z doživljanjem takšnega dogodka, je velikokrat ogroženo tudi zdravje žrtve.

Okrevanje po prevari zahteva torej večplasten in celosten pristop ter v veliko primerih tudi ustrezno strokovno pomoč žrtvam naložbenih prevar. Prepoznanje celotnega procesa, ki ga doživljajo posamezniki, od trenutka, ko vstopijo v vrtinec naložbene prevare, do točke, ko spoznajo, da so bili preslepljeni in se prične proces opolnomočenja po prevari, ponudi odgovore na vprašanje, kako pomagati žrtvi naložbene prevare, da si kar najhitreje in čim bolj celostno opomore po tem dogodku. Obenem pa ta spoznanja ponudijo pomembna izhodišča za preventivno delo v družbi, predvsem s posamezniki, ki sodijo v najranljivejše skupine, kot

so na primer skupina starejših. Preventivno delo pa seveda ni omejeno samo na organe pregona, konkretno preventivno delo policije in Agencije za trg vrednostnih papirjev, temveč so deležniki v teh aktivnostih lahko vsi: od društev, izobraževalnih institucij do najrazličnejših socialnih podpornih mrež.

Študije, ki se ukvarjajo z raziskovanjem izkušenj žrtev z organi pregona, ugotavljajo (Van Dijk,1999), kako pogosto žrtve zaradi neustrezne obravnave doživijo sekundarno viktimizacijo. Da bi ugotovili, kaj konkretno pri delu kriminalistov povzroča ponovno viktimizacijo žrtev, bi bilo treba podrobneje raziskati pričakovanja in izkušnje z obravnavo v predkazenskem (in kazenskem) postopku žrtev naložbenih prevar kot tudi kriminalistov, ki ta kazniva dejanja obravnavajo. Primeri naložbenih prevar so kompleksni ne le po obsegu škode, ki jo povzročijo, in številu žrtev, temveč tudi z vidika, kako je storilec oblikoval in izvedel prevaro; zato je preiskovanje tovrstnih kaznivih dejanj zelo zahtevno in dolgotrajno, praviloma je vpletenih veliko oškodovancev, sama prevara pa največkrat presega nacionalne meje in je potrebno pri obravnavi teh kaznivih dejanj učinkovito mednarodno sodelovanje. Ravno kompleksnost predkazenskega in kazenskega postopka zaradi sofisticiranosti prevare je največkrat razlog, da se posamezne zadeve pravnomočno na sodiščih ne zaključijo tako, kot pričakujejo žrtve teh kaznivih dejanj, hkrati pa osredotočenost na proces in ne na potrebe žrtve v kazenskem postopku povzroči, da žrtev ni (več) obravnavana kot žrtev, temveč postane bolj orodje države za dokazovanje krivde obtoženemu (Meško, 1998).

UPORABLJENI VIRI

Alexander, E. in Seymour, A. (1998). *Rights, roles, and responsibilities: A handbook for faud victims participating in the federal criminal justice system*. Washington: Police Executive Forum.

Agencija za trg vrednostnih papirjev. (n. d.). *Opozorila agencije*. Pridobljeno na http://www.a-tvp.si/default.aspx?id=194

Bernard Madoff. (12. 9. 2016). V *Wikipedia: The free encyclopedia*. Pridobljeno na https://en.wikipedia.org/wiki/Bernard_Madoff

Bernik, I. in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo, 62*(3), 242–252.

Bernik, I. in Prislan, K. (2012). *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem.* Ljubljana: Fakulteta za varnostne vede.

Blanco Hache, A. C. in Ryder, N. (2011). ´Tis the season to (be jolly?) wise-up to online fraudsters. Criminal on the web lurking to scam shoppers this Cristmas: Critical analysis of the United Kingdom's legislative provisions and policies to tackle online fraud. *Information and Communications Technology Law, 20*(1), 35–56.

Croall, H. (2009). White collar crime, consumers and victimisation. *Crime, Law and Social Change*, *51*(1), 127–146.

Davies, P., Francis, P. in Jupp, V. (ur.). (2003). *Victimology: Theory, Research and Policy*. New York: Palgrave Macmillan.

Dimc, M. in Dobovšek, B. (2012). *Kriminaliteta v informacijski družbi.* Ljubljana: Fakulteta za varnostne vede.

Dunn, P. (2007). Matching service delivery to need. V S. Walklate (ur.), *Handbook of victims and victimology* (str. 255–281). Devon: Willan.

Dussich, J. P. J. (2016). *Victimology – past, present and future.* Pridobljeno na http://www.unafei.or.jp/english/pdf/RS_No70/No70_12VE_Dussich.pdf

Fattah, E. A. (1991). *Understanding criminal victimisation.* Scarborough: Prentice Hall.

Financial Conduct Authority. (2016). *Over 55s at heightened risk of fraud, says FCA.* Pridobljeno na https://www.fca.org.uk/news/press-releases/over-55s-heightened-risk-fraud-says-fca

Financial Industry Regulatory Authority [FINRA]. (2016). *FINRA risk meter.* Pridobljeno na http://apps.finra.org/meters/1/riskmeter.aspx

Ganzini, L., McFarland, B. in Bloom, J. (1990). Victims of fraud: Comparing victims of white collar and violent crime. *Bull Am Acad Psychiatry Law*, *18*(1), 55–63.

Garofalo, R. (1914). *Criminology.* Boston: Little, Brown.

Gole, N. (21. 1. 2013). Slovenci prevarani v finančnih verigah. *Delo.* Pridobljeno na http://www.delo.si/gospodarstvo/finance/slovenci-prevarani-v-denarnih-verigah.html

Goucher, W. (2010). Becoming a cybercrime victim. *Computer Fraud and Security*, (10), 16–18.

Harvey, S., Kerr, J., Keeble, J. in McNaughton Nicholls, C. (2014). *Understanding victims of financial crime: A qualitative study with people affected by investment fraud.* NatCen za Financial Conduct Authority. Pridobljeno na http://www.fca.org.uk/static/documents/research/qual-study-understanding-victims-investment-fraud.pdf

Kazenski zakonik [KZ-1]. (2008, 2009, 2011, 2015, 2016). *Uradni list RS,* (55/08, 66/08, 39/09, 91/11, 54/15, 38/16).

Kanduč, Z. (2002). Žrtve, viktimizacije in viktimološke perspektive v optiki tranzicije iz moderne v po(zno)moderno družbo. V Z. Kanduč (ur.), *Žrtve, viktimizacije in viktimološke perspektive* (str. 125–245). Ljubljana: Institut za kriminologijo pri Pravni fakulteti.

Kanduč, Z. (2009). Prevare, prevarantstvo in prevaranti: preliminarna kriminološka analiza. *Revija za kriminalistiko in kriminologijo, 60*(3), 223–224.

Kearon, T. in Godfrey, B. S. (2007). *Handbook of victims and victimology.* London; New York: Routledge, Cavendish.

Keršmanc, C. (2014). *Prevare na meji in onkraj pregona.* Ljubljana: GV založba.

Langenderfer, J. in Shimp, T. A. (2001). Costumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psyhology and marketing*, *18*(7), 763–783.

Lyng, S. (2005). Edgework and the risk-taking experience. V S. Lyng (ur.), *Edgework: The sociology of risk-taking* (str. 17–49). New York: Routledge, Cavendish.

MacDonald, R. (1939). *Crime as a business.* Palo Alto: Stanford University Press.

Meško, G. (1998) Nekatere razsežnosti nasilne viktimizacije. *Teorija in praksa*, *35*(6), 1076–1088.

Milič, M. (20. 10. 2015). Kako iz 100 evrov v letu dni narediti 300 evrov – finančne piramide in prevare! *Mladi in denar.* Pridobljeno na http://www.mladi-denar.si/8837195?cctest&

Modic, D. (2010). Nigerijska prevarantska pisma. V A. Završnik (ur.), *Kriminaliteta in tehnologija: Kako računalniki spreminjajo nadzor in zasebnost ter kriminaliteto in kazenski pregon?* (str. 37–47). Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.

Muršič, M. (2006). K večji varnosti s (kritično) kriminologijo emocij. *Varstvoslovje*, *10*(1), 21–31.

Muršič, M. (2012). Prekiniti krog nasilja. V M. Muršič (ur.), *(O)krog nasilja v družbi in šoli* (str. 7–42). Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.

National Fraud Authority. (2014). *National Fraud Authority annual report and accounts 2013 to 2014.* Pridobljeno na https://www.gov.uk/government/publications/national-fraud-authority-annual-report-and-accounts-2013-to-2014

O'Connell, R. (2003). *A typology of child cybersexploitation and online grooming practices.* Lancashire: University of Central Lancashire.

Pečar, J. (1984). »Induktologija« – znanje o vplivanju na kazensko dvojico. *Revija za kriminalistiko in kriminologijo, 35*(4), 299–311.

Peršak, N. (2015). Viktimologija. V A. Šelih in K. Filipčič (ur.), *Kriminologija* (str. 126–181). Ljubljana: IUS SOFTWARE, Inštitut za kriminologijo pri Pravni fakulteti.

Petty, R. E. in Cacioppo, J. T. (1981). *Attitudes and persuasion: Classic and contemporary approaches.* Dubuque: Brown.

Policija. (2016). *Letno poročilo o delu policije za leto 2015.* Ljubljana: MNZ RS. Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2015_popravljeno.pdf

Ponzijeva shema. (7. 7. 2015). V *Wikipedija: prosta enciklopedija.* Pridobljeno na https://sl.wikipedia.org/wiki/Ponzijeva_shema

Sank, D. in Caplan, D. I. (2007). *To be a victim: Encounters with crime and injustice.* New York: Springer.

Schafer, S. (1968). *The victim and his criminal: A study in functional responsibility.* New York: Random House.

Schultz, L. (1968). The victim-offender relationship. *Crime and Delinquency, 14*(2), 135–141.

Schichor, D. (2001). Victims of inverstment fraud. V H. N. Pontell in D. Schichor (ur.), *Contemporary issues in crime and criminal justice: Essay in honour of Gilbert Geis* (str. 27–29). Upper Saddle River: Prentice Hall.

Seto, M. C. (2013). *Internet sex offenders.* Washington: American Psyhological Association.

Slovar slovenskega knjižnega jezika: SSKJ 2. (2014). Ljubljana: Cankarjeva založba.

Somerville, P. in Bengtsson, B. (2002). Constructionism, realism and housing Theory. *Housing, Theory & Society, 19*(3/4), 121–136.

United States Department of Justice. (2015). *Financial fraud crime victims.* Pridobljeno na https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud

Van Dijk, J. J. M. (1999). Introducing victimology. V R. G. Van Kaam, J. J. M. Van Dijk in J. Wemmers (ur.), *Caring for crime victims* (str. 15–19). New York; Monsey: Criminal Justice Press.

Von Hentig, H. (1948). *The criminal and his victim.* New Haven: Yale University Press.

Walklate, S. (2012). *Hanbook of victims and victimology*. New York; London: Routledge, Cavendish.
Weisburd, D., Wheeler, S. Waring, E. in Bode, N. (1991). *Crimes of the middle classes: White collar offenders in the federal courts.* New Haven: Yale University Press.
Whittle, H. C., Hamilton-Giachristis, C., Beech, A. in Collings, G. (2013). A review of young people's vulnerabilities to online grooming. *Aggression and Violent Behavior, 18*(1), 135–146.
Wolhunter, L., Olley, N. in Denham, D. (2009). *Victimology: Victimisation and victims' rights.* London; New York: Routlege, Cavendish.
Young, J. (2007). *The vertigo of late modernity.* London: Sage.

O avtorici:

Mateja Bitenc, doktorska študentka Fakultete za varnostne vede Univerze v Mariboru. Zaposlena kot kriminalistična inšpektorica specialistka na Oddelku gospodarske kriminalitete Policijske uprave Ljubljana. Njena področja zanimanja so finančna kriminaliteta, viktimologija beloovratniške kriminalitete, naložbene prevare, pranje denarja. E-pošta: mateja.bitenc@policija.si

VARSTVOSLOVJE,
letn. 18
št. 3
str. 325–348

Obveščevalno-varnostni sistem Republike Slovenije: reorganizacija in sistemske rešitve

Jaroš Britovšek, Aleš Čretnik

Namen prispevka:

Namen prispevka je predstaviti modele reorganizacije in izboljšave dela obveščevalnih in varnostnih služb majhnih držav, ki se soočajo z omejenimi finančnimi in kadrovskimi resursi. Analiza prispevka temelji na primeru obveščevalno-varnostnega sistema Republike Slovenije (RS).

Metode:

Z analizo primarnih in sekundarnih virov so bile analizirane in identificirane pomanjkljivosti obveščevalno-varnostnega sistema Republike Slovenije ter s primerjalno analizo obveščevalnih in varnostnih služb tujih držav razvite ustrezne rešitve.

Ugotovitve:

Razviti in predstavljeni so trije možni modeli reorganiziranja obveščevalno-varnostnega sistema RS, ki se med seboj razlikujejo glede na obsežnost posegov. Prav tako so v prispevku predstavljene sistemske rešitve na področju nadzora, zaposlovanja in izobraževanja uslužbencev obveščevalnih in varnostnih služb, ki jih lahko odgovorni implementirajo ne glede na to, ali se država odloči za reorganizacijo ali ne.

Omejitve/uporabnost raziskave:

Tajna narava delovanja obveščevalnih in varnostnih služb nudi omejen dostop do popolnih podatkov, kar posledično omejuje raziskovanje na tem področju.

Praktična uporabnost:

Ugotovitve oz. rešitve, ki so predstavljene v prispevku se lahko nanašajo na praktično implikacijo reorganizacije in izboljšave dela obveščevalnih in varnostnih služb Republike Slovenije.

Izvirnost/pomembnost prispevka:

Prispevek opredeli obveščevalne in varnostne naloge ter odgovarja na vprašanja in dileme v zvezi z reorganizacijo in izboljšavami dela obveščevalnih in varnostnih služb Republike Slovenije, same ugotovitve pa so namenjene tako politični, strokovni kot tudi širši javnosti.

UDK: 355.401(497.4)

Ključne besede: obveščevalne naloge, varnostne naloge, obveščevalnovarnostne naloge, zaščitne naloge, reorganizacija

Intelligence and Security System of the Republic of Slovenia: Reorganisation and Systemic Solutions

Purpose:

The purpose of the article is to present models for the reorganisation and improvement of the intelligence and security services of smaller countries, which often struggle with a lack of financial and human resources. The analysis is based specifically on the intelligence and security system of the Republic of Slovenia (RS).

Design/Methods/Approach:

Shortcomings in the current intelligence and security system of the Republic of Slovenia were identified through analysis of primary and secondary sources. Viable solutions to address identified shortcomings were developed and presented after comparative analysis of selected foreign intelligence and security services.

Findings:

Proposals for reorganisation encompass three possible models for reforming the intelligence and security system of the Republic of Slovenia, which differ according to the extent of the changes needed. The article also presents systemic solutions regarding the accountability, employment and education of intelligence and security service staff. The systemic solutions are distinct from, and can be implemented regardless of, the proposed reorganizational models.

Research Limitations:

The secret nature of intelligence and security services is a limiting factor in accessing complete data, which consequently limits the research capabilities in this field.

Practical Implications:

The findings and solutions presented in this article could have a practical implication on the reorganisation and improvement of the effectiveness of intelligence and security system of the Republic of Slovenia.

Originality/Value:

This article defines intelligence and security tasks, and also provides answers to questions and issues regarding the reorganisation and improvement of the intelligence and security services in the Republic of Slovenia. Findings and conclusions are meant for political, professional and wider public audiences.

UDC: 355.401(497.4)

Keywords: intelligence tasks, security tasks, security intelligence tasks, protective measures tasks, reorganisation

1 UVOD

V zadnjem letu smo bili priča razmeroma negativni medijski izpostavljenosti slovenskih obveščevalnih in varnostnih organizacij (Jančič, 2015; Kajzar in Červek, 2015). Pri tem velja spomniti, da obveščevalne afere ali napake spremljajo slovenske obveščevalno-varnostne službe že vse od njihovega začetka (Kapitanovič, 2015). Namen prispevka ni polemiziranje o posameznih dogodkih ali incidentih, v katere so bile vpletene obveščevalne in varnostne službe, temveč predstaviti modele reorganizacij in predloge izboljšav dela obveščevalnih in varnostnih služb majhnih držav, ki se soočajo z omejenimi finančnimi in kadrovskimi resursi. Med te majhne države spada tudi Republika Slovenija (RS), katere obveščevalno-varnostni sistem je predmet analize prispevka.

Države se po navadi odločajo za reforme svojih obveščevalnih in varnostnih sistemov, ko pride do večjih obveščevalnih napak, odtekanja tajnih podatkov v javnost ali vpletenosti služb v politične afere. Pritisk javnosti in medijev na politične strukture občasno zadostuje, da se lotijo določenih reform, vendar gre pri tem lahko prepogosto za prehitre in nepremišljene poteze. Reorganizacija in/ali reforma organizacij in institucij predstavlja poseben izziv za vsako državo, saj imajo le-te namreč tendenco po ohranitvi, kar pa lahko pripelje do njihove disfunkcionalnosti. Institucije lahko namreč ohranjajo lastno stabilnost, pri tem pa nehajo služiti namenu, za katerega so bile vzpostavljene ali pa so se okoliščine spremenile in potrebe po instituciji ne obstajajo več. Z drugimi besedami, institucije se vzpostavljajo zato, da zadovoljijo določenim okoliščinam, vendar ko se okoliščine spremenijo, se jim institucije ne znajo prilagoditi. Eden od razlogov, da prihaja do tega, je kognitivni, kjer ljudje razvijejo mentalne modele o tem, kako svet deluje in kljubujejo spremembam, ne glede na dokaze. Drugi razlog je interesni, kjer določene skupine posameznikov razvijejo interes v statusu quo in se upirajo kakršnimkoli spremembam (Fukuyama, 2014). Določena državna organizacija lahko torej postane ali postaja disfunkcionalna zaradi intelektualne rigidnosti ter moči posameznikov, ki preprečujejo spremembe. Stalni pregled, analiza ter ocena institucij so potrebne, da se lahko ugotavlja, ali določena institucija potrebuje reforme, reorganizacijo ali celo ukinitev.

Razmišljanja o reorganizaciji obveščevalno-varnostnega sistema RS niso nova. Že Purg (1995) je pisal o predlogu združene obveščevalne službe (Slovenska obveščevalna agencija), ki bi bila notranje organizacijsko razdeljena na različna področja. Podobno je o združeni obveščevalni službi (Državna informativna služba) razmišljal Anžič (1996). Po njegovem mnenju bi bili uslužbenci znotraj službe specializirani za vojaško in civilno področje. Tako Purg (1995) kot Anžič (1996) sta predvidevala izločitev varnostnih nalog[1] iz obveščevalnih služb, ki bi po njunem mnenju morale biti organizirane znotraj Ministrstva za notranje zadeve (MNZ). Kljub temu je Anžič (1996) menil, da bi bile ob MNZ varnostne naloge lahko organizirane tudi znotraj Ministrstva za obrambo (MO). Potrebo po reorganizaciji oz. reformi obveščevalnih in varnostnih služb sta izpostavila tudi nekdanja vodilna v Slovenski obveščevalno-varnostni agenciji (SOVA) in Obveščevalno varnostni službi (OVS). Nekdanji direktor SOVA I. Podbregar je v

1 *Razlike med obveščevalnimi in varnostnimi nalogami bodo podrobneje razložene v nadaljevanju.*

zvezi z združitvijo obveščevalnih in varnostnih služb dejal, da po strokovni plati ta ne bi bila sporna in da bi bilo bolj koordinirano sodelovanje boljše, med drugim zaradi kadrovskih in finančnih omejitev. Prednosti je videl predvsem v večji sinergiji delovanja na tem področju, slabost pa v koncentraciji moči (Delić, 2012). Med drugim je tudi trdil, da bi obveščevalne in varnostne službe lahko združili in obdržali le tretjino trenutnih zmogljivosti (Podbregar, 2011). O potrebah po reorganizaciji, predvsem profesionalizaciji in kadrovski modernizaciji je govoril tudi nekdanji direktor OVS in SOVA D. Črnčec. Črnčec je med drugim govoril o preveliki zaprtosti in nujnosti prilagajanja obveščevalnih in varnostnih služb spremembam in novim izzivom. Omenil je tudi pomanjkanje pravno-formalnih okvirjev za definiranje ekstremističnih skupin in s tem učinkovito ukrepanje zoper njih (Glücks, 2013). Med drugim je tudi ponujal rešitev, po kateri RS potrebuje novo neodvisno institucijo oz. pooblaščenca za nadzor nad delovanjem obveščevalnih in varnostnih služb (Črnčec, 2010).

Prispevek zasleduje tezo, da morajo majhne države, kot je Slovenija, glede na grožnje in finančne ter kadrovske omejitve slediti modelom organiziranosti obveščevalno-varnostnega sistema, ki omogočajo učinkovito in ekonomično opravljanje tako obveščevalnih kot tudi varnostnih nalog. V prispevku bodo najprej predstavljene obveščevalne in varnostne naloge, temu pa bo sledila analiza obveščevalno-varnostnega sistema RS. Na podlagi analize bodo identificirane pomanjkljivosti in dileme ter predstavljeni predlogi. Predlogi so razdeljeni na dva širša sklopa, in sicer na reorganizacijo in na sistemske rešitve obveščevalno-varnostnega sistema RS. Reorganizacija obveščevalno-varnostnega sistema RS mora zasledovati cilj izboljšanja organizacije za dosego optimalnega opravljanja obveščevalnih in varnostnih nalog. Pri tem se je treba, če je le mogoče, izogniti podvajanju nalog ter stremeti k združevanju procesov in delov posameznih organizacij, ki opravljajo podobne ali celo enake naloge. Prav tako je treba zmanjšati oziroma preprečiti neproduktivno tekmovanje posameznih organizacij za kadrovske in finančne resurse. Sistemske rešitve se nanašajo na področje nadzora obveščevalnih in varnostnih služb RS ter zaposlovanja in izobraževanja uslužbencev teh služb. Cilj implementacije sistemskih rešitev mora biti izboljšanje preglednosti, profesionalnosti in učinkovitosti delovanja obveščevalnih in varnostnih služb RS.

2 OBVEŠČEVALNE IN VARNOSTNE NALOGE

Obstoj obveščevalnih in varnostnih organizacij ne sme biti samemu sebi namen in mora biti venomer odvisen od potreb države, pri čemer obveščevalno-varnostne organizacije nudijo podporo državi oz. vodilnim v državi (odločevalcem) pri doseganju nacionalnovarnostnih ciljev ter zaščiti nacionalnih interesov. To podporo nudijo z zaznavanjem, identificiranjem, spremljanjem ter ocenjevanjem tveganj in groženj, ki lahko izhajajo iz tujine ali znotraj države.

Resolucija o strategiji nacionalne varnosti RS (ReSNV-1, 2010) opredeljuje glavne vire tveganj in ogrožanj nacionalne varnosti RS. Resolucija jih deli na globalne, nadnacionalne ter nacionalne vire. Med globalne vire uvršča podnebne spremembe, finančna, gospodarska in socialna tveganja ter krizna žarišča.

Med nadnacionalne vire uvršča terorizem, nedovoljene dejavnosti na področju konvencionalnega orožja, orožij za množično uničevanje in jedrske tehnologije, organiziran kriminal, nezakonite migracije, kibernetske grožnje in zlorabo informacijskih tehnologij in sistemov, dejavnost tujih obveščevalnih služb in vojaške grožnje. Kot nacionalne vire ogrožanja pa uvršča ogrožanje javne varnosti, naravne in druge nesreče, omejenost naravnih virov ter degradacijo življenjskega okolja, zdravstveno-epidemiološke grožnje ter določene dejavnike negotovosti. Obveščevalne in varnostne službe zbirajo in ocenjujejo podatke[2] o tveganjih in grožnjah ter sprejemajo ukrepe za preprečitev, zmanjšanje ali celo odpravo le-teh[3]. Obveščevalne službe so osredotočene predvsem na globalne in nadnacionalne vire, medtem ko varnostne službe svoje aktivnosti osredotočajo na nacionalne ter v določenem delu tudi na nadnacionalne vire tveganj in groženj. Kadar imajo države obveščevalno in varnostno službo združeno v eno organizacijo, govorimo o obveščevalno-varnostni službi.

Za pomoč pri analizi in izpeljavi predlogov obveščevalnih in varnostnih sistemov so v nadaljevanju opredeljene naloge značilne na obveščevalno-varnostnem področju. Te naloge so postavljene tudi v kontekst ogrožanj, ki so navedena v omenjeni Resoluciji (ReSNV-1, 2010). Tradicionalno se v RS govori in piše o obveščevalni, protiobveščevalni in varnostni dejavnosti (Anžič, 1997; Črnčec, 2009; Podbregar, 2012; Purg, 1995) ali nalogah (Zakon o obrambi, 2004). Na tem področju je potreben korak naprej in na podlagi analize in izkušenj je mogoče identificirati naslednje naloge znotraj obveščevalno-varnostnega sistema: obveščevalne naloge, vojaške obveščevalne naloge, varnostne naloge (vojaške in civilne), ki jih je mogoče deliti na obveščevalnovarnostne in zaščitne naloge.

Obveščevalne naloge so širši pojem in predstavljajo zbiranje, analiziranje in ocenjevanje podatkov o razmerah in virih ogrožanja, ki izhajajo iz tujine. Obveščevalne naloge zagotavljajo podporo odločevalcem pri sprejemanju odločitev na zunanjem, obrambnem, vojaškem, varnostnem in tudi ekonomskem področju. Postavljeno v kontekst ReSNV-1 (2010) obveščevalne naloge obsegajo zbiranje in analizo podatkov o političnih, ekonomskih, varnostnih in vojaških razmerah v tujini, območjih kriznih žarišč oz. kjer država zasleduje nacionalni interes. Obveščevalne naloge obsegajo tudi zbiranje o tujih obveščevalnih službah, terorističnih, ekstremističnih in vojaških grožnjah. Naloge lahko obsegajo tudi zbiranje podatkov o migracijah, ilegalni trgovini z radiološkim, kemičnim in

2 *Zahodni predvsem angleško govoreči svet oz. njihova terminologija govori o obveščevalnih disciplinah zbiranja podatkov, kot so: OSINT (angl. Open Source Intelligence), ki pomeni zbiranje obveščevalnih podatkov iz različnih javno dostopnih virov (medijev, različnih evidenc, znanstvenih publikacij itd.); HUMINT (angl. Human Intelligence), ki pomeni zbiranje obveščevalnih podatkov preko človeških virov (vohunov, agentov, insajderjev, prebežnikov, informantov, diplomatov, poslovnežev, popotnikov itd.); SIGINT (angl. Signal Intelligence), ki pomeni prestrezanje in zbiranje obveščevalnih podatkov, ki poteka po elektronskih komunikacijah (radio, radar, omrežja, optika itd.); IMINT (angl. Imagery Inteligence), ki pomeni zbiranje slikovnih obveščevalnih podatkov s kopnega, iz zraka ali vesolja (fotografija, infrardeča tehnologija, ultravijolična tehnologija itd.) (Wyss, 2011).*

3 *Na tem mestu je treba poudariti, da podatke o tveganjih in grožnjah zbirajo in ocenjujejo tudi nekateri drugi organi v državi (npr. o zdravstveno-epidemioloških grožnjah zbirata in ocenjujeta podatke ter sprejemata ukrepe Ministrstvo, pristojno za zdravje, in Inštitut za varovanje zdravja RS ter območni zavodi za zdravstveno varstvo, v določenem delu pa tudi Civilna zaščita, Uprava RS za zaščito in reševanje ter drugi), ki pa niso posebej izpostavljeni, saj niso predmet tega prispevka.*

biološkim orožjem ter organizirani kriminaliteti, v primeru, da predstavlja vir finančnih ali drugih sredstev za prej omenjene aktivnosti. Vojaške obveščevalne naloge so ožji pojem in se nanašajo na zbiranje in analiziranje podatkov, ki so primarno pomembni za vojaške poveljnike in poveljstva vojaških enot oz. so pomembni za izvajanje nalog, ki jih opravljajo oborožene sile. V kontekstu ReSNV-1 (2010) gre za zbiranje podatkov o vojaških grožnjah in o razmerah na kriznih žariščih ter drugih območjih, kjer delujejo vojaške enote. Zaradi spremenjenega varnostnega okolja in kompleksnosti varnostnih tveganj (npr. mednarodne operacije in misije [MOM] ter krizna žarišča), vojaške enote zbirajo tudi podatke, ki so zanimive za civilne obveščevalne in varnostne službe.

Varnostne naloge delimo na obveščevalnovarnostne in zaščitne naloge. Obveščevalnovarnostne naloge[4] obsegajo preiskovanje, zbiranje, analiziranje in ocenjevanje podatkov o posameznikih in organizacijah, ki z vohunjenjem, sabotažami, subverzivnim delovanjem, organiziranim kriminalom ter z nasilnim ekstremizmom in terorizmom ogrožajo varnost države. V kontekstu ReSNV-1 (2010) predstavljajo zbiranje podatkov o delovanju tujih obveščevalnih služb, terorističnih in ekstremističnih grožnjah, migrantih, ilegalni trgovini z radiološkim, kemičnim in biološkim orožjem, ter organiziranem kriminalu, v primeru, da predstavlja vir finančnih ali drugih sredstev za prej omenjene aktivnosti. Zaščitne naloge sestavljajo predvsem varnostni ukrepi, katerih končni cilj je nevtralizacija ali zmanjšanje groženj in tveganj. Obstaja več klasifikacij varnostnih ukrepov, na splošno pa se jih deli na organizacijske (zakonodaja, pravila ravnanja s tajnimi podatki, usposabljanja, varnostna preverjanja oseb ...), fizične (varnostniki, ograja, protivlomna vrata ...) ter tehnične ukrepe (videonadzor, alarmni sistemi, kriptografija, komunikacijska varnost ...). Protiteroristične in protiobveščevalne naloge se opravljajo s kombinacijo obveščevalnovarnostnih nalog (zbiranje podatkov o obveščevalnih službah in terorističnih skupinah) ter zaščitnih nalog (Herman, 1996).

3 ANALIZA OBVEŠČEVALNO-VARNOSTNEGA SISTEMA RS

Slovenski obveščevalni-varnostni sistem je bil formiran in njegov delokrog določen na osnovi vedenj/znanj, ki so jih snovalci imeli v devetdesetih letih prejšnjega stoletja. Od takrat so se grožnje nenehno spreminjale in postajale vedno bolj nekonvencionalne. Tradicionalna vojaška grožnja RS je postala skoraj zanemarljiva, na površje pa so prišle nekonvencionalne oz. asimetrične grožnje, kot so npr. terorizem, ilegalne migracije in kibernetske grožnje. Obstaja verjetnost, da so se obveščevalne in varnostne službe RS do neke mere prilagodile novim grožnjam v okviru trenutnih zakonskih in organizacijskih omejitev, kar pa jim nujno ne omogoča celovitega pristopa k novim varnostnim izzivom, kot so npr.

4 *Izraz obveščevalnovarnostne naloge smo izpeljali iz angl. termina »Security intelligence«, ki pomeni obveščevalne naloge primarno usmerjene v grožnje znotraj države (Herman, 1996). Pri tem je treba razlikovati pojma obveščevalnovarnostno in obveščevalno-varnostno (s stičnim vezajem). Pri besedni zvezi obveščevalnovarnostne naloge gre za podredno zloženko s poudarkom na besedi varnostne, medtem ko pri besedni zvezi obveščevalno-varnostne naloge za priredno zloženko, kjer gre za enakovredno izvajanje obveščevalnih in varnostnih nalog (prirejeno po Toporišič, 2006).*

potencialne avtohtone ekstremistične in teroristične organizacije. Posledično je mogoče sklepati, da so potrebne tako organizacijske in s tem tudi zakonske spremembe obveščevalno-varnostnega sistema RS.

Obveščevalno-varnostni sistem RS[5] trenutno sestavljajo SOVA, Kriminalistična policija, OVS ter organi in enote Slovenske vojske (SV). SOVA izhaja iz nekdanje republiške Službe državne varnosti (SDV), ki je primarno opravljala varnostne naloge, razdeljene na protiobveščevalni oddelek in oddelek za notranje zadeve (Trampuš, 2007). SDV je bila leta 1991 preimenovana v Varnostno-informativno službo (VIS) pod MNZ, leta 1993 pa je postala samostojna vladna služba. Z odlokom vlade se VIS leta 1993 preimenuje v SOVA (Černe, 2011). Leta 1999 dobi tudi svoj zakon (z novelo iz leta 2006), kjer se primarno varnostne naloge dokončno zamenjajo s primarno obveščevalnimi nalogami (Zakon o Slovenski obveščevalno-varnostni agenciji [ZSOVA], 2006).

Kljub sodelovanju med SOVA in Policijo je slednja začela razvijati lastne zmogljivosti zbiranja podatkov znotraj Uprave kriminalistične policije. Prej je SOVA Policiji nudila tehnično pomoč pri zbiranju podatkov, vendar je Ustavno sodišče leta 2005 odločilo[6], da SOVA v kazenskem postopku te pomoči ne sme nuditi. Uprava kriminalistične policije je vzpostavila tudi Center za kriminalistično obveščevalno dejavnost, zadolžen predvsem za analitično obdelavo podatkov (Dvoršek in Frangež, 2011). Kriminalistična policija ima znotraj svoje organizacije tudi Sektor za posebne naloge in Sektor za organizirano kriminaliteto, znotraj katerega je organiziran Oddelek za terorizem in ekstremno nasilje (Policija, n. d.).

Na obrambnem področju je OVS nastal iz nekdanjega Varnostnega organa Ministrstva za obrambo (VOMO) in je danes organiziran kot služba na nivoju direktorata znotraj MO. Pred preoblikovanjem v OVS je bil VOMO usmerjen predvsem v varnostne naloge, pozneje pa je dobil tudi obveščevalne naloge. Tako SOVA kot OVS sta zadolžena za spremljanje razmer v tujini, kjer naj bi bila OVS zadolžena za obrambno/vojaško, SOVA pa civilno področje (Černe, 2011). V praksi pa je zaradi obsežnosti groženj (predvsem groženj iz tujine) (glej ReSNV-1, 2010) takšno razmejitev težko doseči[7].

OVS tako opravlja obveščevalne in vojaške obveščevalne naloge, vendar se nekatere vojaške obveščevalne naloge dejansko ne izvajajo v OVS, ampak v Slovenski vojski (Obveščevalni in varnostni organi t. i. J/G/S-2 ter obveščevalno-izvidniške enote). Z eno od reorganizacij OVS so bili leta 2000 uslužbenci OVS skupaj z nalogami spremljanja mednarodnih komunikacij prerazporejeni iz OVS v SV, kjer danes deluje Enota za elektronsko bojevanje (EEB) (Mihačič, 2012). Pri tem naj bi SV na strateškem nivoju sodelovala z OVS (Rode, Derviz in Henigman, 2009), v preteklosti pa so bili tudi številni poskusi integracije obeh organov (Lesjak, 2013).

5 *Slovenski obveščevalno-varnostni sistem izhaja iz varnostne in ne toliko iz obveščevalne tradicije. V Socialistični federativni republiki Jugoslaviji (SFRJ) sta varnostne naloge opravljali Služba državne varnosti (SDV) in Kontraobveščevalna služba (KOS) (Garb, 2007), ki pa ju slovenska javnost predvsem zaradi takratne frazeologije pozna kot obveščevalni službi.*

6 *Ustavna odločba številka Up-412/03-21 z dne 8. 12. 2005 (Ustavno sodišče RS, 2005).*

7 *V primeru vodenja človeških virov se lahko npr. zgodi, da dve obveščevalni organizaciji nevede vodita isti vir. To pa lahko pripelje do napačnih sklepov, kjer napačno mislimo, da se je neka informacija potrdila, ker je druga služba poročala isto, pri tem pa je šlo za isti vir.*

OVS opravlja tudi varnostne naloge, kot so spremljanje dejavnosti tujih vojaških obveščevalnih služb, preiskovanje kaznivih dejanj, nudenje rešitev na področju fizičnega in tehničnega varovanja ter varnostna preverjanja uslužbencev MO. Nekatere varnostne naloge na vojaškem področju poleg OVS opravljajo tudi obveščevalni in varnostni organi SV (J/G/S-2) ter Vojaška policija (Ravnak, 2012).

Obveščevalno-varnostni sistem RS ima za majhno državo veliko število organizacij z razmeroma podobnimi obveščevalnimi in varnostnimi nalogami. Slednje lahko prispeva k neučinkovitim opravljanjem nalog ter tudi neproduktivnim tekmovanjem posameznih služb za finančne in kadrovske resurse. Poleg tega obstaja tudi določeno tveganje, da lahko kljub širokemu obveščevalno-varnostnemu sistemu prihaja do zanemarjanja in zmešnjave na področjih, kot sta npr. spremljanje in preprečevanje ekstremizma in terorizma na teritoriju RS[8].

SOVA lahko zbira podatke o skupinah in osebah, ki s svojo dejavnostjo iz tujine ali v povezavi s tujino ogrožajo, ali pa bi lahko ogrozile nacionalno varnost. Slednja razmeroma dobro pokriva spremljanje delovanja tujih obveščevalnih in mednarodnih terorističnih organizacij. Pojavi pa se vprašanje, kdo spremlja ekstremistične ali teroristične organizacije, ki izhajajo iz države. Če ne obstajajo indici o načrtovanju ali naklepih po izvršitvi kaznivega dejanja, lahko policija sicer zbira podatke o teh skupinah, vendar z manj vsiljivimi metodami[9]. M. Fank, takratni pomočnik direktorja Uprave kriminalistične policije, je na vprašanje novinarja, koliko je ekstremističnih skupin in posameznikov v RS, dejal, da je to težko opredeliti, saj policija posameznih združevanj ne more nadzirati, če te ne prestopijo meje zakonitosti (Rečnik, 2013). Kot že rečeno, pa mora SOVA, če bi želela zbirati podatke o ekstremističnih skupinah, najprej poiskati povezavo s tujino (ZSOVA, 2006). Poleg tega se pojavlja tudi vprašanje zakonitosti uporabe podatkov SOVE v sodnih in/ali predkazenskih postopkih.

Ob migrantsko-begunski krizi, ki je jeseni 2015 zajela Evropo in RS, bi naj učinkovit obveščevalno-varnostni sistem predčasno opozoril na pojav ter posledično sprožil priprave na varnostne, politične, diplomatske in druge ukrepe za omejitev in obvladovanje krize. Vlada RS je sicer trdila, da je krizo pričakala pripravljena, vendar ji opozicija in del javnosti očitata ravno nasprotno (B. T. in Al. Ma., 2015). Na MO sicer obstaja Nacionalni center za krizno upravljanje (NCKU)[10], vendar je njegova vloga opredeljena zelo ozko, in sicer zagotavlja prostorske, tehnične, informacijske in telekomunikacijske pogoje za delo Vlade RS v skladu z zakonom ob izrednem in vojnem stanju ter ob pojavih ali dogodkih oziroma krizah v državi oziroma v regionalnem ali strateškem okolju, ki lahko pomembno ogrozijo nacionalno varnost (Uredba o organizaciji in delovanju Nacionalnega

8 *Znan je primer državljana RS ter spreobrnjenca in islamista Roka Žavbija, ki se je od leta 2013 pa do 2014 boril v Siriji. Žavbi je bil 2016 sicer aretiran v RS, vendar na podlagi tiralice italijanske policije zaradi suma kaznivega dejanja novačenja z namenom terorizma (Lončar, 2016).*

9 *Policija ima sicer zaradi prisotnosti po vsej državi dobro informacijsko oz. obveščevalno mrežo, ki deluje na razmeroma nevsiljivih principih zbiranja podatkov, kot je npr. koncept »Policijsko delo v skupnosti« (Jeram, 2013).*

10 *Pozitiven korak v smislu koordinacije in pregleda nad zbiranjem in analizo podatkov je bila vzpostavitev medresorske analitične skupine v času migrantsko-begunske krize znotraj NCKU (Vlada RS, 2015).*

centra za krizno upravljanje, 2006). Z drugimi besedami, NCKU zagotavlja samo prostore in komunikacije v izrednem in vojnem stanju, kar pa po vsej verjetnosti ne zadovoljuje potreb Vlade RS v današnjih varnostnih izzivih in grožnjah. Prav tako je nerealno pričakovati, da bi bila Vlada RS v vojnem stanju na MO, ki bi verjetno predstavljal enega primarnih ciljev nasprotnikovih sil.

Nadzor nad obveščevalno-varnostnimi organizacijami v RS se opravlja na več nivojih. Glavni nadzorniki so: Varuh človekovih pravic, Vrhovno sodišče, Komisija za nadzor obveščevalnih in varnostnih služb, Vlada RS, Računsko sodišče in Proračunska inšpekcija, javnost in Informacijski pooblaščenec (Sotlar, 2012). Iz zakonodajnega vidika je nadzor razmeroma dobro urejen, vendar obstajajo nekatere praktične težave. V pogovoru na oddaji RTV Slovenije je član Komisije za nadzor obveščevalnih in varnostnih služb RS dejal, da se komisija sooča z nezadostno strokovno podporo pri nadzoru obveščevalnih in varnostnih služb, kar bistveno otežuje delo poslancev in komisije (Prisluškovanje: Studio ob 17h, 2015). Pomanjkanje strokovne podpore lahko bistveno ovira učinkovit nadzor nad obveščevalno-varnostnimi službami RS.

Tako SOVA kot OVS veljata za izjemno zaprti organizaciji, na kar kažejo že njune razmeroma skope spletne strani, v medijih pa se pojavljajta samo v kontekstu političnih afer. Spletna stran OVS vsebuje le kontaktne podatke in ime direktorja (Ministrstvo za obrambo RS, 2015), medtem ko ima spletna stran SOVA nekoliko več vsebine, a še vedno razmeroma splošne podatke o delu organizacije. Na njihovi spletni strani pod zavihkom Sporočila za javnost najdemo stavek »Trenutno ni aktualnih sporočil za javnost« (Slovenska obveščevalno-varnostna agencija [SOVA], 2015). Slednje kaže na pomanjkljivo komunikacijo obveščevalnih in varnostnih služb RS z javnostjo.

Omejevanje zaposlovanja, ki ga je bila zaradi zakonskih in finančnih razlogov deležna državna uprava, je najverjetneje pripeljalo tudi do kadrovske podhranjenosti obveščevalnih in varnostnih služb RS. Trenutno splošno podhranjenost varnostnih struktur potrjujejo tudi ugotovitve Komisije za nadzor obveščevalnih in varnostnih služb, navedene v Sklepu seje Vlade RS z 20. 4. 2016 (Urad vlade RS za komuniciranje, 2016), ki Vladi RS priporoča, da prouči vse možnosti za povečanje finančnih sredstev za nadgradnjo vseh varnostnih struktur. Posledice krize so vodile v zmanjšanje števila zaposlenih in višanja povprečne starosti uslužbencev v teh službah. Dodatno težavo predstavlja nepregledno zaposlovanje v obveščevalnih in varnostnih službah RS. Delovno razmerje v SOVA (ZSOVA, 2006) in OVS (Uredba o obveščevalno-varnostni službi Ministrstva za obrambo [Uredba OVS], 1999) se namreč lahko sklene brez objave delovnega mesta oz. razpisa, kar ima mogoče določen smisel, vendar pa hkrati predstavlja tudi priložnost za zlorabe – klientelistično in politično zaposlovanje (Na Morsu izigravali predpise?, 2008).

4 PREDLOGI REORGANIZACIJE OBVEŠČEVALNO-VARNOSTNEGA SISTEMA RS

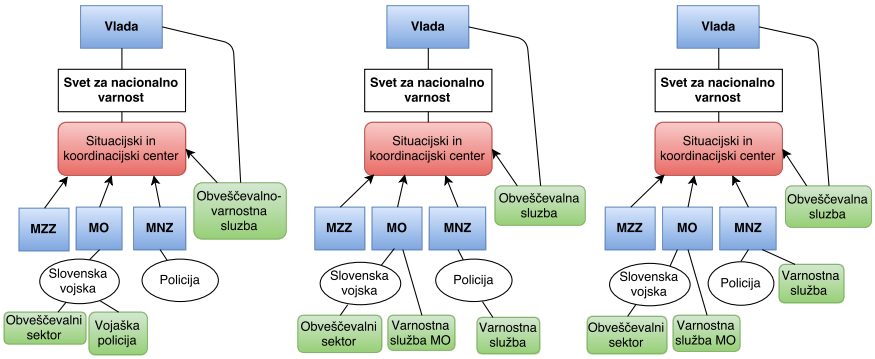
V nadaljevanju so predstavljeni trije modeli reorganiziranja obveščevalno-varnostnega sistema RS, ki se med seboj razlikujejo glede na

obsežnost posegov v trenutno organiziranost. Predstavljene reorganizacije oz. modeli sledijo ciljem doseganja ustreznega razmerja med finančnimi in kadrovskimi resursi ter učinkovitostjo opravljanja obveščevalno-varnostnih nalog, ki so bile predstavljene in opredeljene na začetku prispevka. Modeli reorganizacij so bili izbrani na podlagi načela ekonomičnosti, torej upoštevanja finančnih in kadrovskih omejitev, s katerimi se soočajo majhne države, kot je RS, in združevanja nalog (obveščevalnih in varnostnih), ki so si po vsebini podobne in se v praksi lahko pogosto tudi prekrivajo. Za pomoč pri razvoju modelov so bili uporabljeni primeri tujih obveščevalno-varnostnih sistemov, ki stremijo k ekonomičnemu in združevalnemu principu izvajanja obveščevalnih in varnostnih nalog: (1) združena obveščevalno-varnostna služba (Švica); ena obveščevalna in ena varnostna služba (Danska); ena obveščevalna in dve varnostni službi (civilno in vojaško področje) (Nemčija).

Vsi trije modeli (glej model 1, 2 in 3) predvidevajo preoblikovanje trenutnega NCKU v Koordinacijski in situacijski center ter pomembnejšo vlogo varnostnih nalog znotraj obveščevalno-varnostnega sistema RS. Situacijski in koordinacijski center (v nadaljevanju Center) bi bil ustanovljen iz trenutnega NCKU[11], ki bi deloval kot operativni del ter podpora Svetu za nacionalno varnost. Center bi deloval na konceptu dežurstva (24/7), popolnjevali pa bi ga pripadniki SV, uslužbenci MO, MZZ, MNZ ter obveščevalnih in varnostnih služb. Združeval bi človeške vire dežurnih, kriznih, operativnih in situacijskih centrov vključno z analitiki/častniki za povezavo[12] z MO, MZZ, MNZ in drugih ministrstev. Center bi deloval po konceptu NATO Centra za združevanje obveščevalnih podatkov (NATO Intelligence Fusion Centre – NIFC) (Čretnik, 2010), ki pa bi bil poleg izdelave ocen groženj in analiz zadolžen tudi za koordinacijo aktivnosti in ukrepov državnih organov v primeru naravnih nesreč ali poslabšanih varnostnih razmer v državi ali na kriznem območju, kjer se nahajajo in delujejo predstavniki RS. Z drugimi besedami, Center bi predstavljal komunikacijsko, informacijsko ter koordinacijsko središče obveščevalno-varnostnega sistema RS, ki bi odločevalcem zagotavljal pravočasne podatke in ocene v zvezi z tveganji in grožnjami RS ter njenim pripadnikom/državljanom v tujini, hkrati pa bi nudil in koordiniral aktivnosti za omejitev in/ali popolno odpravo groženj/tveganj ter njihovih posledic.

11 *Pri tem ne bi šlo za ukinitev nalog, ki jih trenutno opravlja NCKU, saj bi okrepljeni Center obdržal tudi naloge, ki jih je imel do sedaj – zagotavljal prostorske, tehnične, informacijske in telekomunikacijske pogoje za delo Vlade RS.*

12 *Gre za pooblaščenega predstavnika za vzdrževanje zveze med matično organizacijo in Centrom z namenom, da se zagotovi neoviran pretok podatkov in da procesi potekajo nemoteno, hkrati pa so ti predstavniki tudi pooblaščeni s strani vodij matičnih organizacij, da lahko sprejemajo s pooblastilom določene odločitve.*



Shema 1: Predlogi modelov reorganizacije obveščevalno - varnostnega sistema RS.

Vsi modeli (glej model 1, 2 in 3) predvidevajo okrepitev Obveščevalnega sektorja SV znotraj Generalštaba SV. Obveščevalni sektor SV bi v celoti prevzel vojaške obveščevalne naloge (spremljanje vojaških groženj, razmer na MOM, bojiščih ter kriznih žariščih) in bi s svojimi ocenami in ugotovitvami redno podpiral enote, poveljnike in poveljstva SV, ter ostale organe Ministrstva za obrambo. Za optimalno opravljanje nalog bi Obveščevalni sektor SV moral okrepiti analitični del ter izkoristiti obveščevalne zmogljivosti, ki jih premore SV. Obveščevalni sektor SV bi s svojimi ugotovitvami in ocenami podpiral in sodeloval z Obveščevalno-varnostno službo (model 1) ali Obveščevalno službo (model 2 in 3). Podobno rešitev najdemo v Švici, kjer so vojaški obveščevalni organi organizirani v Vojaško obveščevalno službo (J2) (nem. Militärischer Nachrichtendienst [FGG 2]) znotraj Združenega vojaškega štaba Švicarske vojske (The Swiss Armed Forces, n. d.).

Model 1 predvideva združitev obveščevalnih in varnostnih nalog s civilnega in obrambnega področja v enotno Obveščevalno-varnostno službo, in sicer po zgledu Švice, ki je leta 2010 združila del policije s Strateško obveščevalno službo in ustanovila Zvezno obveščevalno službo NDB (nem. Nachrichtendienst des Bundes), katere naloge so zbiranje podatkov o zunanjih in notranjih grožnjah (Swiss Federal Archives, n. d.). Policija bi bila s tem osredotočena na klasične oblike kriminalitete in organizirano kriminaliteto, medtem ko bi Obveščevalno-varnostna služba zbirala podatke v zvezi z ogrožanjem nacionalne varnosti tako v tujini kot tudi doma (tuje obveščevalne službe, ekstremistične in teroristične skupine). Kadar bi šlo za pregon kaznivih dejanj v zvezi z ogrožanjem nacionalne varnosti, pa bi morala sodelovati s policijo. Čeprav obstaja več rešitev organizacijske uvrstitve službe znotraj sistema, bi bila najbolj optimalna postavitev pod Vlado RS, kot je sedaj SOVA, saj bi bila naloga službe nuditi podporo zunanji (MZZ), obrambni (MO) in varnostni (MNZ) politiki.

Model 2 in 3 predvidevata združitev obveščevalnih nalog (zbiranjem in analiziranjem podatkov o razmerah v tujini) v enotno Obveščevalno službo. Ker gre pri obveščevalnih nalogah za podporo tako zunanji (MZZ) kakor tudi obrambni politiki (MO), bi bilo optimalno, da je služba organizirana pod Vlado RS. Podobno rešitev pozna Nemčija, kjer je Zvezna obveščevalna služba BND (nem. Bundesnachrichtendienst) podrejena predsedniku vlade oz. kanclerju (Bundesnachrichtendienst [BND], n. d. A). Nemčija je med drugim leta 2007

ukinila vojaško obveščevalno službo imenovano Center za obveščevalno dejavnost Zvezne vojske in ga združila z Zvezno obveščevalno službo BND (Carstens in Löwenstein, 2007).

Model 2 predvideva prenos civilnih varnostnih nalog pod policijo oz. bi lahko bil znotraj policije ustanovljena organizacijska enota za nacionalno varnost (npr. Varnostna služba), ki bi opravljala in združevala obveščevalnovarnostne naloge (protiteroristične in protiobveščevalne naloge). Takšno oz. podobno rešitev poznata Danska in ZDA. Na Danskem deluje Policijska obveščevalna služba PET (dan. Politiets Efterretningstjeneste), ki opravlja protiteroristične in protiobveščevalne naloge, in je organizirana znotraj policije, vendar odgovarja neposredno ministru za pravosodje (Politiets Efterretningstjeneste [PET], n. d. A). V Združenih državah Amerike (ZDA) je znotraj Zveznega preiskovalnega urada FBI (angl. Federal Bureau of Investigation) organiziran Nacionalnovarnostni sektor, ki vključuje Oddelek za protiobveščevalne naloge in Oddelek za protiteroristične naloge (Federal Bureau of Investigation [FBI], n. d. B). Po drugi strani model 3 predvideva, da bi civilne varnostne naloge opravljala nova Varnostna služba znotraj MNZ. Podobno rešitev pozna Nemčija, kje je varnostna služba imenovana Zvezna služba za zaščito ustave (nem. Bundesamt für Verfassungsschutz [BfV]) organizirana znotraj ministrstva, zadolženega za notranje zadeve. Služba zbira in analizira podatke o posameznikih in skupinah, ki ogrožajo nacionalno varnost oz. demokratično ustavno ureditev Nemčije (politični in verski ekstremizmi ter obveščevalne službe) vendar nima policijskih pooblastil, kot so npr. aretacije (Federal Minstry of the Interior, 2016).

Model 1 predvideva, da bi varnostne naloge na vojaškem področju opravljala Vojaška policija, ki pa bi bila omejena predvsem na zaščitne naloge. Takšno rešitev najdemo v Švici, kjer varnostne naloge (protiobveščevalne zaščitne naloge) na vojaškem področju opravlja Vojaška policija (Schweizer Armee, n. d.). Po drugi strani model 2 in 3 predvidevata, da bi varnostne naloge na obrambnem in vojaškem področju opravljala Varnostna služba MO, ki bi imela svoje izpostave v SV. Podobno rešitev najdemo v Nemčiji, kjer na ministrstvu, pristojnem za obrambo, deluje varnostna služba MAD (nem. Militaerischer Abschirmdienst), ki opravlja varnostne naloge na obrambnem in vojaškem področju (Die Dienststellen der Streitkräftebasis, n. d.). Varnostna služba MO ima svoje prednosti, saj bi pokrivala tako vojaški kot tudi civilni del MO, medtem ko bi Vojaška policija, ki je organizirana znotraj SV, pokrivala samo vojaško osebje, s čimer bi lahko prišlo do zanemarjanja civilnega dela MO oz. bi ta del morala pokriti Obveščevalno-varnostna služba ali Policija (model 1).

Cilj obveščevalnovarnostnih nalog ni vedno kazenski pregon, ampak izboljšanje varnosti z obveščanjem odgovornih, ki lahko sprejmejo različne ukrepe, kot so sprememba politike, zakonodaje, in/ali uvedba ustreznih varnostnih ukrepov (zaščitne naloge). Kot primer lahko navedemo spremljanje tujih obveščevalnih služb, kjer pogosto ne pride do kazenske ovadbe (npr. zaradi diplomatske imunitete tujih obveščevalcev), ampak je cilj predvsem omejitev in/ali obvladovanje delovanja teh služb. Prav tako lahko zbrani podatki in analize o ekstremizmu ne vodijo nujno v kazenski pregon, lahko pa pripomorejo k racionalnejšim pristopom odgovornih pri reševanju problema ekstremizma in

radikalizacije (npr. preprečevanje radikalizacije posameznikov v zaporih, uvedba programov deradikalizacije ...). Zaščitne naloge se znotraj državne uprave izvajajo v različnih oblikah, odvisne pa so od stopnje in vrste ogroženosti. Ker pa gre pri varnostnih incidentih pogosto za neupoštevanje že vzpostavljenih zaščitnih ukrepov, bi morala služba, ki opravlja varnostne naloge, imeti pooblastila, ki bi jim omogočala boljši nadzor nad doslednim izvajanjem in implementacijo zaščitnih ukrepov. Reorganizacija predvideva tudi integracijo Urada za varovanje tajnih podatkov (UVTP) v Obveščevalno-varnostno službo (glej model 1), Policijo (glej model 2) ali Varnostno službo MNZ (glej model 3), ki bi za vse javne uslužbence, ki imajo potrebo po dostopu do nacionalnih in NATO/EU tajnih podatkov, opravljal varnostna preverjanja ter jim izdajal varnostna potrdila za dostop do tajnih podatkov.

Predstavljeni modeli niso mišljeni kot popolne in edine rešitve, saj sami po sebi ne rešujejo nekaterih dilem na področju dela obveščevalno-varnostnih služb, kot so optimalna organizacijska umeščenost, razmerje med civilnimi in vojaškimi obveščevalnimi nalogami ter razmerja med »policijskimi« in »obveščevalnimi« pooblastili. Dileme v smislu nadzora pri postavitvi obveščevalno-varnostne službe (model 1) ali Obveščevalne službe (model 2 in 3) neposredno pod Vlado RS je omenjal že Črnčec (2010), ki je ugotavljal, da imajo lahko resorne službe RS močnejši strokovni nadzor nad svojim delom kot pa vladna služba. To pa predvsem zaradi tega, ker je resorna služba umeščena na ministrstvo, ki strokovni nadzor opravlja s svojimi drugimi organi (npr. inšpektorat in revizijska služba).

V zvezi z enotno obveščevalno službo obstajajo tudi argumenti proti združevanju, kot so ločitev vojaških in civilnih obveščevalnih nalog ter pozitiven izkupiček tekmovanja posameznih služb za naklonjenost politične elite in s tem resursov (Anžič, 1996). Prvi argument se sicer lahko omeji s predlogom, da bi vojaške obveščevalne naloge dejansko ostale znotraj SV, medtem ko bi Obveščevalni sektor SV sodeloval z enotno obveščevalno službo podobno kot to počne sedaj z OVS. Prav tako se zaradi spremenjenih in prepletenih oblik ogrožanj v praksi dejansko ne more postaviti jasne ločnice med vojaškimi in civilnimi obveščevalnimi nalogami. Drugi argument se lahko demantira zaradi negativnih posledic, ki jih lahko ima neproduktivno tekmovanje ali celo sovražni odnos med notranjimi organizacijskimi enotami.[13] Poleg tega je cilj obveščevalno-varnostnega sistema, da obveščevalne službe vlagajo napore in tekmujejo z obveščevalnimi službami tujih držav ali terorističnih skupin in ne med seboj.

Na problematiko mešanja t. i. »policijskih« in »obveščevalnih« pooblastil je opozarjal že Anžič (2010), ki je ostro nasprotoval združevanju »policijskih« in »obveščevalnih« pooblastil v eni organizacijski enoti. Parlamentarna skupščina Sveta Evrope (Parliamentary Assembly, 1999) je med drugim priporočila državam

13 *Za primer lahko pogledamo zasebno družbo Sears, ki jo je njen direktor Eddie Lampert leta 2008 reorganiziral na podlagi principa tekmovalnosti notranjih oddelkov. Ideja je bila, da bi se spodbudilo tekmovanje med oddelki, namesto tega pa je prišlo do sovražnosti. Oddelki so začeli tekmovati za naklonjenost vodstva, zanimali so se samo za svoj uspeh in zanemarjali uspešno poslovanje celotne družbe. Lojalnost oddelku je prevladala nad lojalnostjo družbi. Namesto, da bi oddelki med seboj sodelovali in tekmovali s konkurenčnimi družbami, je njihovo tekmovanje vodilo v propad celotne družbe. Lampert se namreč ni zavedal, da smo ljudje nagnjeni k sodelovanju pri doseganju skupnih ciljev in smo lahko takrat celo bolj produktivni (Cummins, 2006).*

članicam, da naj notranje varnostne službe ne bi imele »policijskih pooblastil«, kot so vodenje kriminalističnih preiskav, aretacije in pridržanje oseb. Prav tako te službe naj ne bi bile uporabljene za boj proti organizirani kriminaliteti, razen v posebnih okoliščinah, kadar organizirana kriminaliteta predstavlja grožnjo nacionalni varnosti. Po drugi strani je Završnik (2013) ugotavljal, da prihaja do vedno bolj zabrisane meje med delom organov pregona in obveščevalno-varnostnih služb. To velja še posebej na področju protiterorizma, kjer so države začele iskati rešitve, kako bi lahko zbrane podatke obveščevalno-varnostnih služb uporabile kot dokazno gradivo v sodnih postopkih. Rešitev takšnih dilem se lahko išče v omejenih pooblastilih obveščevalno-varnostnih služb, ki bi bile omejene le na zbiranje in analizo podatkov, in bi na področju protiterorističnih in protiobveščevalnih nalog morale sodelovati z organi pregona. Vsakršni posegi v imenu nacionalne varnosti pa morajo glede na Evropsko sodišče za človekove pravice[14] zadostiti naslednjim trem pogojem: ukrepi morajo imeti podlago v domačem pravu; zakonodaja mora biti dostopna in jasna prizadetim osebam ter posledice za posameznika morajo biti predvidljive.

5 SISTEMSKE IZBOLJŠAVE OBVEŠČEVALNIH IN VARNOSTNIH SLUŽB RS

V nadaljevanju so predstavljeni sistemski predlogi na področju izboljšave delovanja obveščevalnih in varnostnih služb RS. Gre za rešitve anomalij, ki bi morale biti odpravljene ne glede na to, ali sistem ostane tak, kot je, ali pa se odločevalci odločijo za enega od treh modelov. Pri nadzoru je izpostavljeno izobraževanje nadzornikov in s tem izboljšanje učinkovitosti samega nadzora. Učinkovit nadzor se lahko krepi tudi z večjo odprtostjo služb in krepitvijo zaupanja in razumevanja med obveščevalno-varnostnimi službami ter javnostjo. Izboljšave so potrebne tudi v zvezi z zaposlovanjem ter usposabljanjem uslužbencev obveščevalnih in varnostnih služb, in sicer je treba identificirati kadrovske potrebe, vzpostaviti kriterije za selekcijo kandidatov, čemur pa mora slediti ustrezno osnovno in specializirano izobraževanje uslužbencev.

Delo Komisije za nadzor obveščevalnih in varnostnih služb v RS bi se izboljšalo z okrepitvijo strokovne podpore, na kar je opozarjal že Črnčec (2010). Komisija je namreč pogosto odvisna od poznavanja in interesa posameznega poslanca, ki pa seveda lahko variira, zato bi bilo dobro razmisliti o stalni strokovni podpori tej komisiji. Strokovnjaki bi poleg strokovne podpore pri nadzoru pomagali pri iskanju dobrih izkušenj (dobre prakse) iz primerov tujih držav in služb ter predlagali nove pobude in spremembe na področju obveščevalno-varnostnega sistema. Nadzorna telesa naj bi poleg pravilnosti in zakonitosti nadzirala tudi učinkovitost in uspešnost dela obveščevalnih in varnostnih služb. Slednje bi se moralo redno ocenjevati s strani neodvisnih teles, prav tako naj bi nadzorna telesa obveščevalnih in varnostnih služb redno sodelovala s tujimi podobnimi organi ter s tem identificirala in delila dobre prakse delovanja (Born in Wills, 2012).

14 *Glej npr. naslednje sodbe Evropskega sodišča za človekove pravice (2008, 2009, 2010): Kennedy proti Združenem kraljestvu, št. 26839/05, z dne 18. 5. 2010; Iordachi in drugi proti Moldaviji, št. 25198/02, z dne 10. 2. 2009; ter Liberty in drugi proti Združeno kraljestvo, št. 58243/00, z dne 1. 7. 2008.*

Tu govorimo o dodatni krepitvi strokovnosti in učinkovitosti obveščevalnih in varnostnih organizacij z zgodovinskim spominom organizacije in učenjem novih praks, ki se zagotavlja z implementacijo menedžmenta znanja v obveščevalnih in varnostnih strukturah (Britovšek in Čretnik, 2012).

Obveščevalno-varnostne službe RS morajo izboljšati komunikacijo z javnostjo. V zvezi s tem je povezan tudi problem pretiranega oz. prekomernega označevanja tajnosti podatkov, s katerim se soočajo obveščevalne in varnostne službe po vsem svetu (Jones, 2014). V tujini imajo nekatere službe svoje predstavnike za stike z javnostjo, veliko komunikacije pa poteka preko njihovih spletnih strani. Švicarska Zvezna obveščevalna služba (Verteidigung, Bevölkerungsschutz und Sport, n. d. A) ima npr. svojo spletno stran, kjer so predstavljene osnovne informacije o službi, njene naloge in umestitev ter sporočila za javnost (npr. spremembe zakonodaje in kaj to pomeni za javnost). Služba izdaja tudi letna poročila in posebna poročila, ki so dostopna javnosti (Verteidigung, Bevölkerungsschutz und Sport, n. d. B). Podobne spletne strani in za javnost dostopna poročila imajo tudi varnostne službe Danske (PET, n. d. B) in Nemčije (Bundesamt für Verfassungsschutz [BfV], n. d. C). Zaupanje javnosti je pomembno pri delu obveščevalnih in varnostnih služb, to pa se lahko okrepi z vzpostavitvijo ekipe za odnose z javnostmi ter za upravljanje spletne strani, kjer bi služba lahko komunicirala z javnostmi, predstavljala svoje naloge in novosti ter objavljala letna in posebna poročila.

Problem prekomernega označevanja tajnosti podatkov je zaradi narave dela obveščevalnih in varnostnih služb težko rešljiv v praksi. Lahko pa bi delo obveščevalnih in varnostnih služb a priori – že zaradi uporabe tajnega komunikacijskega sistema – označevali z določeno stopnjo tajnosti, vendar bi pooblaščena stalna komisija imela ob zahtevku javnosti ter določenih pogojih možnosti umakniti stopnjo tajnosti in s tem obveščati javnost. Druga možnost je določitev jasnih kriterijev, kdaj je določen podatek tajen in kdaj ne. Trenutno v RS obstaja zelo splošen opis določanja tajnosti podatkov, ki se nanaša na to, kako hudo razkritje podatka škoduje organu ali državi (Zakon o tajnih podatkih, 2006). Slednje pomeni, da se mora avtor sam odločiti, na osnovi ne povsem jasnih kriterijev, v kakšni meri razkritje podatka škoduje organu ali državi. Slednje pa na koncu pripelje do prekomernega označevanja tajnosti podatkov. Na težave arbitrarnega določanja tajnosti podatkov je že ob sprejemanju zakonodaje opozarjal Pečar (2001), ki je dejal, da se predpisi na tem področju pretežno ukvarjajo z obravnavanjem in ne toliko s samim nastajanjem tajnih podatkov.

Obveščevalno-varnostni sistem potrebuje spremembe na področju zaposlovanja oseb v obveščevalnih in varnostnih službah RS. V zvezi z zaposlovanjem so predstavljeni primeri ZDA, Velike Britanije in Nemčije. Njihove službe na svojih spletnih straneh objavljajo delovna mesta, s čimer lahko dobimo razmeroma dober vpogled v strukturo in pogoje za zasedbo delovnih mest.[15] Prav tako imajo omenjene službe na svojih straneh predstavljene svoje izobraževalne institucije. Dejansko stanje na področju zaposlovanja in izobraževanja zaposlenih v takšnih sistemih je sicer težko oceniti, kljub temu pa je možno izpostaviti dobre prakse ter možne izboljšave za obveščevalno-varnostni sistem RS. Na spletni

15 *Za primer kompetenc oz. pogojev, ki naj bi jih za delo na analitičnem področju imel kandidat, glej Zver (2015).*

strani ameriške Centralne obveščevalne agencije (Central Intelligence Agency, n. d) lahko vidimo vrste delovnih mest, pogoje in tudi razpis prostih delovnih mest. Podobne informacije so tudi na spletnih straneh Nemške obveščevalne službe (BND, n. d. B) in obveščevalne službe Velike Britanije (Secret Intelligence Service [MI6], n. d.). Pogoji in delovna mesta so razmeroma podrobno opisana, področja dela pa se na splošno delijo na: analitično delo, operativno delo, lingviste, znanost in tehnologijo ter podporo (finance, kadrovanje, pravna podpora, informacijska podpora, logistika, administracija, varovanje). Vse omenjene obveščevalne službe imajo tudi svoje izobraževalne institucije, ki skrbijo za redno testiranje in usposabljanje njihovih uslužbencev. Te institucije nudijo splošno in specializirano usposabljanje (jezikovne šole, informatika). Podoben sistem zaposlovanja in izobraževanja v omenjenih državah imajo tudi njihove varnostne službe. V ZDA ima Zvezni preiskovalni urad (FBI, n. d. A) na spletni strani objavljena delovna mesta, skupaj s pogoji. Podobno velja za varnostni službi Velike Britanije (Security Service [MI5], n. d. A) in Nemčije (BfV, n. d. B). Na splošno se razpisi za delovna mesta delijo na obveščevalno delo, lingviste, tehnologijo in znanost, podporo ter specializirana znanja, kot so npr. psihologi.

Finančna kriza in posledični vladni varčevalni ukrepi v RS so zaradi zamrznitve zaposlovanj in upokojevanj najverjetneje pripeljali do zmanjšanja in postaranja deleža aktivnih uslužbencev v obveščevalnih in varnostnih službah. V okviru zaposlovalne politike je treba imeti jasno opredeljene opise del, ki jih morajo kandidati izpolnjevati za določeno delovno mesto. Kandidati bi morali pred zaposlitvijo preiti vsaj skozi delno fazo testiranja. Na ta način se lahko pregledno selekcionira najboljše med prijavljenimi kandidati. Da bi se izognili nepravilnostim pri zaposlovanju, bi bilo mogoče razmisliti o ukinitvi zaposlovanja brez razpisov v obveščevalnih in varnostnih službah. Obstaja pa seveda nevarnost, da bi šlo pri razpisih za tako imenovane »prirejene razpise«, kjer delodajalec razpiše pogoje, ki ustrezajo točno določenemu kandidatu in ne delovnemu mestu (Aščić, 2013). Zato bi bilo dobro razmisliti o testiranjih kandidatov in organu, ki bi skrbel za preglednost zaposlitev v službah (Voh Boštic, 2015). Poleg tega je treba izbranim uslužbencem postaviti in zagotoviti smiselno in jasno karierno pot. Če bi šlo za določeno specialistično storitev, ki ima lahko tudi omejen rok trajanja, bi bila lahko izvedena pogodbena zaposlitev (npr. izobraževanja uslužbencev, svetovanje na določenem področju, testiranja sistemov, prevajalci ...).

V RS se kaže tudi potreba po izobraževalni ustanovi za uslužbence obveščevalnih in varnostnih struktur. Nekatere službe imajo tudi svoje izobraževalne ustanove, ki skrbijo za izobraževanje in usposabljanje svojih uslužbencev. ZDA poznajo FBI akademijo (FBI, n. d. C), Britanci imajo svojo MI5 akademijo (MI5, n. d. B) ter Nemci BfV akademijo (BfV, n. d. A). Da takšne akademije niso omejene le na večje države, kaže primer sosednje Hrvaške, ki ima znotraj Urada za nacionalno varnost organizirano svojo Obveščevalno akademijo (Sigurnosno-obavještajna agencija, 2015). Obveščevalno-varnostne strukture v RS trenutno nimajo posebne lastne institucije, preko katere bi organizirano zbirali znanje in veščine ter izvajali izobraževanja in usposabljanje uslužbencev. Možna rešitev bi bila ustanovitev institucije v smislu npr. Obveščevalno-varnostna akademija, ki bi bila zadolžena za redno usposabljanje uslužbencev ter bi

delovala kot povezava s civilnimi izobraževalnimi institucijami in zasebnimi gospodarskimi družbami.

Razvoj informacijskih tehnologij in s tem povezanih groženj narekuje potrebo po posodobitvi Obveščevalnih in varnostnih služb RS tudi na tem področju. Treba je razmisliti o kadrovskih in organizacijskih zmogljivostih obveščevalnih in varnostnih služb RS na področju spremljanja in varovanja komunikacij. Krčenje finančnih resursov in pomanjkanje ustreznega kadra zmanjšuje kibernetske obrambne zmogljivosti RS. Pojavijo se dileme, ali bi bilo treba več napora vlagati v izobraževanje trenutnih uslužbencev ali v zaposlovanje novih uslužbencev na omenjenem področju. Kot primer države, ki je, kljub majhnosti, začela v letu 2016 intenzivno iskati kadre na področju kibernetike, lahko navedemo Dansko (Rychla, 2016). Ker pa je potreba po takšnih kadrih visoka tudi v zasebnem sektorju, ki lahko kadrom ponudi tudi razmeroma višjo plačo, bi veljalo razmisliti tudi o pogodbenih možnostih sodelovanja zasebnih informacijskih družb pri krepitvi kibernetskih zmogljivosti RS[16] (usposabljanje ali delo na konkretnih projektih). Ne nazadnje se pojavlja vprašanje, ali bi bilo treba razmišljati o združevanju resursov tudi na tem področju.

6 ZAKLJUČEK

Prispevek je zasledoval tezo, da morajo majhne države, kot je Slovenija, glede na grožnje in finančne ter kadrovske omejitve slediti modelom organiziranosti obveščevalno-varnostnega sistema, ki omogočajo učinkovito in ekonomično opravljanje tako obveščevalnih kot tudi varnostnih nalog. Za potrditev teze so bile najprej identificirane in opredeljene obveščevalno-varnostne naloge, ki so bile podlaga za nadaljnji razvoj modelov reorganizacije. Opredelili smo obveščevalne in vojaške obveščevalne naloge, ki so usmerjene izven države, ter varnostne naloge (obveščevalnovarnostne in zaščitne naloge), ki se načeloma opravljajo znotraj države. Identificirani in predstavljeni so bili trije možni modeli reorganiziranja obveščevalno-varnostnega sistema RS, ki se med seboj razlikujejo glede na obsežnost posegov. Poleg tega so bile predstavljene tudi sistemske rešitve na področju nadzora, zaposlovanja in izobraževanja. Največji izziv ostaja sama pripravljenost in odločitev za reorganizacijo, ki pa je odvisna predvsem od politične volje ter drugih interesov.

V zvezi z reorganizacijo bi najmanj posegov zahteval model 1, ki predvideva združitev obveščevalnih in varnostnih nalog v enotni obveščevalno-varnostni službi. Na ta način bi bili finančni in kadrovski resursi za zbiranje in analiziranje podatkov o zunanjih in notranjih grožnjah zbrani na enem mestu. Koncentracija podatkov v eni službi bi lahko izboljšala učinkovitost, vendar se je treba zavedati, da obstajajo razlike v naravi obveščevalnih in varnostnih nalog[17]. Prihaja lahko tudi do nejasnosti glede vloge Vojaške policije in zanemarjanja varnostnih nalog

16 *Država si npr. zaradi plačnega sistema ne more privoščiti velikega števila vrhunskih kadrov na informacijskem področju (Voh Boštic, 2016). S podobnimi težavami se soočajo tudi druge države. V ZDA je npr. pri vdoru v pametni telefon terorističnega napadalca pomagala zasebna informacijska družba (Gjorgievska, 2016).*

17 *Za razliko od obveščevalnih so varnostne naloge po svoji naravi dela bližje delu represivnim organom.*

v civilnem delu MO. Zato bi optimalno izvajanje obveščevalnih in varnostnih nalog v RS predstavljal model 3, kjer so obveščevalne naloge združene v enotni Obveščevalni službi, varnostne naloge bi na civilnem področju opravljala Varnostna služba MNZ, na obrambnem/vojaškem pa Varnostna služba MO. Takšna reorganizacija pa bi pomenila razmeroma velike zakonodajne in strukturne posege v trenutni obveščevalno-varnostni sistem RS. Ker bi lahko pretirano ali prehitro poseganje lahko nehote zmotilo izvajanje nalog, ki se trenutno opravljajo učinkovito, bi bilo mogoče sprva dobro razmisliti o manjših posegih, kot je model 2. Slednji predvideva združitev obveščevalnih nalog v enotno Obveščevalno službo. Varnostne naloge na civilnem področju bi nadalje opravljala policija, varnostne naloge na obrambnem in vojaškem področju pa bi opravljala Varnostna služba MO. Pri tem se je treba zavedati, da varnostne naloge niso omejene samo na teritorij države, ampak se lahko izvajajo tudi v tujini (npr. protiobveščevalna in protiteroristična zaščita diplomatskih predstavništev in oboroženih sil v tujini). Vsi modeli reorganizacij predvidevajo prenos in okrepitev vojaških obveščevalnih nalog v SV ter preoblikovanje trenutnega NCKU v Koordinacijski in situacijski center pod vlado RS oz. Svet za nacionalno varnost, ki bi skrbel za izmenjavo informacij in koordinacijo dela obveščevalnih in varnostnih služb. Ostale naloge, ki jih je prej opravljal NCKU, se prav tako prenesejo v novi Koordinacijski in situacijski center.

Predstavljeni modeli vsekakor niso mišljeni kot popolne rešitve, saj modeli sami po sebi ne rešujejo, niti ne morejo reševati številnih dilem, ki se pojavljajo na področju obveščevalno-varnostnih sistemov. Organizacijska umeščenost se lahko, npr., izkaže kot neprimerna šele po nekaj letih delovanja. Obstajajo tudi nekatere dileme glede združevanja civilnih in vojaških obveščevalnih nalog. Prav tako ostaja dilema ustreznega razmerja med t. i. »policijskimi« in »obveščevalnimi« pooblastili. Neustrezno razumevanje teh razmerij lahko po eni strani povzroča preveliko moč služb in s tem zlorabo pooblastil, po drugi strani pa lahko ustvari komunikacijsko blokado, podvajanje nalog ter posledično neučinkovitost dela služb.

Največji izziv vsakršne reorganizacije vsekakor predstavlja vzpostavitev politične volje in interesa za izvedbo potrebnih sprememb. Takrat se lahko začne tudi podrobneje analizirati potrebne spremembe na zakonodajnem področju. Eden prvih korakov bi bila opredelitev in prepoved delovanja in združevanja v ekstremističnih skupinah, ki ogrožajo demokratično in ustavno ureditev RS v Kazenskem zakoniku RS (2008). Pri tem je seveda treba biti previden, saj se lahko površna dikcija zlorabi za pregon delovanja sicer legitimnih političnih skupin. Nadaljnji koraki v spremembah zakonodaje in pooblastil bi bili odvisni od tega, za kateri model reorganizacije bi se odgovorni odločili, zagotovo pa bi bil pozitiven korak sprejetje krovnega zakona o obveščevalnih in varnostnih službah, kjer bi med drugim bile opredeljene naloge, grožnje, metode zbiranja podatkov ter posamezne organizacije in njihova področja. Slednje bi neposredno vplivalo na potrebe po spremembi ali umiku Zakona o SOVA (2006) in spremembi Zakona o obrambi (2004), iz katerega bi bilo treba izvzeti organizacijo, ki opravlja obveščevalne in varnostne naloge. Sprememba Zakona o obrambi (2004) bi predstavljala največji izziv, saj vsakršna sprememba zahteva privolitev dvotretjinske večine vseh

poslancev Državnega zbora RS. Posegi v ostalo zakonodajo, kot so npr. Zakon o organiziranosti in delu v policiji (2013), Zakon o nalogah in pooblastilih policije (2013) ter Zakona o tajnih podatkih (2006), so nadalje odvisni od izbora modela reorganizacije. Vprašanja in dileme glede pooblastil bi bilo treba reševati, če in ko se država odloči za reorganizacijo obveščevalnih in varnostnih služb. Glede pooblastil se lahko poraja več vprašanj in dilem, kot so združevanja ali širjenje pooblastil (npr. uporaba poligrafa, pooblastila v zvezi z varnostnim preverjanjem oseb, uporaba obveščevalnih podatkov v predkazenskih in/ali kazenskih postopkih ...). Slednje bi potrebovalo podrobnejšo analizo in ni del tega prispevka.

Po drugi strani se lahko sistemske rešitve izvedejo tudi brez večjih organizacijskih posegov. Prva rešitev, ki se nanaša na nadzor dela obveščevalnih in varnostnih služb, predvideva uvedbo strokovne podpore Komisiji za nadzor obveščevalnih in varnostnih služb. Podpora bi izboljšala tako delo Komisije kot tudi delo obveščevalnih in varnostnih služb. Na področju zaposlovanja je bila predlagana uvedba preglednega zaposlovanja na podlagi znanih kriterijev in testiranj kandidatov. Predlagana je tudi ustanovitev posebnega telesa, organa ali akademije, ki bi skrbela za usposabljanje uslužbencev in sodelovanje z zunanjimi izobraževalnimi institucijami in bi izboljšala strokovnost dela zaposlenih v obveščevalnih in varnostnih službah. Pri tem se porajajo tudi vprašanja in dileme, ki pa niso obravnavane v tem prispevku, in sicer v zvezi z imenovanjem vodilnih v obveščevalnih in varnostnih službah ter postavljanju strokovnih in jasnih kriterijev (znanje in izkušnje na obveščevalnem in varnostnem področju), ki bi jih kandidat moral izpolnjevati.

Učinkoviti obveščevalno-varnostni sistemi ostajajo hrbtenica in živčevje stabilnih in uspešnih nacionalnovarnostnih sistemov držav, zato mora biti prilagajanje sistemov novim grožnjam in razmeram stalna prioriteta nacionalnovarnostne politike. Predstavljeni predlogi reorganizacij in sistemskih rešitev sledijo temu načelu, saj nudijo ekonomične rešitve za optimalno delovanje obveščevalno-varnostnega sistema majhnih držav, ki se soočajo z omejenimi finančnimi in kadrovskimi resursi, med katere spada tudi RS. Prepletenost in pojav novih groženj ter nova področja, kot je kibernetika, so dovolj pomemben razlog, da RS začne razmišljati o reformi in modernizaciji svojega obveščevalno-varnostnega sistema.

UPORABLJENI VIRI

Anžič, A. (1996). *Vloga varnostnih služb v sodobnih parlamentarnih sistemih – nadzorstvo*. Ljubljana: Enotnost.

Anžič, A. (1997). *Varnostni sistem Republike Slovenije*. Ljubljana: Uradni list Republike Slovenije.

Anžič, A. (2010). Parlamentarni nadzor obveščevalnih dejavnosti in policijskih prikritih ukrepov –Slovenija med teorijo in prakso. *Bilten Slovenske vojske*, *12*(3), 143–161. Pridobljeno na http://www.slovenskavojska.si/fileadmin/slovenska_vojska/pdf/bilten_sv/bilten_sv_12_3.pdf

Aščić, J. (8. 12. 2013). Do službe v javnem sektorju prek zvez in poznanstev? *MMC RTV SLO*. Pridobljeno na http://www.rtvslo.si/slovenija/do-sluzbe-v-javnem-sektorju-prek-zvez-in-poznanstev/324535

B. T. in Al. Ma. (5. 11. 2015). SMC: Slovenija se je odzvala dobro. SDS: Nepripravljenost se ponavlja. *MMC RTV SLO.* Pridobljeno na https://www.rtvslo.si/begunska-kriza/smc-slovenija-se-je-odzvala-dobro-sds-nepripravljenost-se-ponavlja/377940

Born, H. in Wills, A. (2012). *Overseeing intelligence services – a toolkit*. Geneva: DCAF.

Britovšek, J. in Čretnik, A. (2012). Implementacija menedžmenta znanja v obveščevalnih in varnostnih strukturah. V T. Pavšič Mrevllje (ur.), *Zbornik prispevkov: 13. slovenski dnevi varstvoslovja*. Ljubljana: Fakulteta za varnostne vede. Pridobljeno na http://www.fvv.um.si/DV2012/zbornik/varnostno_obvescevalna_dejavnost/Cretnik_Britovsek.pdf

Bundesamt für Verfassungsschutz. [BfV]. (n. d. A). *Akademie für Verfassungsschutz*. Pridobljeno na http://www.verfassungsschutz.de/de/das-bfv/akademie-fuer-verfassungsschutz

Bundesamt für Verfassungsschutz [BfV]. (n. d. B). *Das BfV als Arbeitgeber*. Pridobljeno na http://www.verfassungsschutz.de/de/das-bfv/karriere

Bundesamt für Verfassungsschutz [BfV]. (n. d. C). *Öffentlichkeitsarbeit.* Pridobljeno na http://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit

Bundesnachrichtendienst [BND]. (n. d. A). *History of the Bundesnachrichtendienst*. Pridobljeno na http://www.bnd.bund.de/EN/About_us/History/Historical_Review/Historical_Review_node.html

Bundesnachrichtendienst [BND]. (n. d. B). *Karriere*. Pridobljeno na http://www.bnd.bund.de/DE/Karriere/karriere_node.html

Carstens, P. in Löwenstein, S. (28. 6. 2007). Der BND und das Militär Willkommene Amtshilfe, geneidete Kompetenz. *Frankfurter Allgemeine Zeitung*. Pridobljeno na http://www.faz.net/aktuell/politik/inland/der-bnd-und-das-militaer-willkommene-amtshilfe-geneidete-kompetenz-1437717.html

Central Intelligence Agency. (n. d.). *Career opportunities*. Pridobljeno na https://www.cia.gov/careers/opportunities

Cummins, D. (16. 2. 2016). This is what happens when you take Ayn Rand seriously. *Pbs*. Pridobljeno na http://www.pbs.org/newshour/making-sense/column-this-is-what-happens-when-you-take-ayn-rand-seriously/

Černe, G. (2011). *Pravni okviri delovanja varnostnih in obveščevalnih služb od osamosvojitve dalje* (Magistrsko delo). Ljubljana: Fakulteta za družbene vede.

Čretnik, A. (2010). Združevalni centri v procesu izmenjave podatkov – problem ali rešitev? *Bilten Slovenske vojske*, *12*(1). 21–33. Pridobljeno na http://www.slovenskavojska.si/fileadmin/slovenska_vojska/pdf/bilten_sv/bilten_sv_10_1.pdf

Črnčec, D. (2009). *Obveščevalna dejavnost v informacijski dobi*. Ljubljana: Defensor.

Črnčec, D. (2010). Sodobni izzivi nadzora nad obveščevalnimi službami. *Bilten Slovenske vojske*, *12*(3), 143–161. Pridobljeno na http://www.slovenskavojska.si/fileadmin/slovenska_vojska/pdf/bilten_sv/bilten_sv_12_3.pdf

Delić, A. (20. 2. 2012). V drobovju oblasti pomembni premiki: Sova in OVS. *Delo*. Pridobljeno na http://www.delo.si/clanek/196526

Die Dienststellen der Streitkräftebasis. (n. d.). *Militärischen Abschirmdienst* [MAD]. Pridobljeno na http://www.kommando.streitkraeftebasis.de/portal/a/kdoskb/weitdstst/mad

Dvoršek, A. in Frangež, D. (2011). Pomen strateške (kriminalistične) analitike za kriminalistično obveščevalno dejavnost. V T. Pavšič Mrevlje (ur.), *Smernice sodobnega vartvoslovja: zbornik prispevkov: 11. slovenski dnevi varstvoslovja*. Ljubljana: Fakulteta za varnostne vede. Pridobljeno na http://www.fvv.um.si/DV2010/zbornik/kriminalisticne_in_forenzicne_preiskave/Dvorsek_Frangez.pdf

Evropsko sodišče za človekove pravice. (2008). Sodba Evropskega sodišča za človekove pravice številka 58243/00 z dne 1. 7. 2008.

Evropsko sodišče za človekove pravice. (2009). Sodba Evropskega sodišča za človekove pravice številka 25198/02 z dne 10. 2. 2009.

Evropsko sodišče za človekove pravice. (2010). Sodba Evropskega sodišča za človekove pravice številka 26839/05 z dne 18. 5. 2010.

Federal Bureau of Investigation [FBI]. (n. d. A). *Explore careers*. Pridobljeno na https://www.fbijobs.gov/explore-careers

Federal Bureau of Investigation [FBI]. (n. d. B). *National security branch*. Pridobljeno na https://www.fbi.gov/about-us/nsb

Federal Bureau of Investigation [FBI]. (n. d. C). *Training*. Pridobljeno na https://www.fbi.gov/about-us/training/training

Federal Minstry of the Interior. (2016). *Federal Office for the Protection of the Constitution*. Pridobljeno na http://www.bmi.bund.de/EN/Topics/Security/Protection-of-the-Constitution/protection-of-the-constitution_node.html

Fukuyama, F. (2014). America in decay: The sources of political dysfunction. *Foreign Affairs*, *93*(5), 763–775.

Garb, G. (2007). *Oblike tajnega delovanja obveščevalno-varnostnih služb Republike Slovenije* (Magistrstko delo). Ljubljana: Fakulteta za družbene vede.

Gjorgievska, A. (30. 3. 2016). Sun Corp. Soars on ties to company that helped FBI crack iPhone. *Bloomberg*. Pridobljeno na http://www.bloomberg.com/news/articles/2016-03-30/sun-corp-soars-on-ties-to-company-that-helped-fbi-crack-iphone

Glücks, N. (27. 1. 2013). Damir Črnčec, direktor Sove: Na Sovi vsi še niso pretrgali praks SDV. *Reporter*. Pridobljeno na http://www.reporter.si/iz-tiskane-izdaje/damir-%C4%8Drn%C4%8Dec-direktor-sove-na-sovi-vsi-%C5%A1e-niso-pretrgali-praks-sdv/14125

Herman, M. (1996). *Intelligence power in peace and war*. Cambridge: University Press.

Jančič, P. (23. 3. 2015). Vebrove težave s protiobveščevalci in obveščevalci. *Delo.* Pridobljeno na http://www.delo.si/novice/politika/vebrove-tezave-s-protiobvescevalci-in-obvescevalci.html

Jeram, G. (2013). *Policijsko delo v skupnosti v Republiki Sloveniji – analiza procesov od osamosvojitve dalje* (Magistrsko delo). Ljubljana: Fakulteta za varnostne vede.

Jones, N. (20. 3. 2014). The menace of overclassification. *The National Security Archive*. Pridobljeno na https://nsarchive.wordpress.com/2014/03/20/the-menace-of-overclassification/

Kajzar, R. in Červek, R. (7. 9. 2015). Sovo ujeli pri vohunjenju za avstrijskim veleposlaništvom v Sloveniji. *Delo*. Pridobljeno na http://www.delo.si/novice/slovenija/sovo-ujeli-pri-vohunjenju-za-avstrijskim-veleposlanistvom-v-sloveniji.html

Kapitanovič, P. (26. 7. 2015). Vsi lapsusi slovenskih obveščevalcev. *Delo*. Pridobljeno na http://www.delo.si/novice/politika/vsi-lapsusi-slovenskih-obvescevalcev.html

Kazenski zakonik. (2008, 2009, 2011, 2015, 2016). *Uradni list RS*, (55/08, 66/08, 39/09, 91/11, 54/15, 38/16).

Lesjak, D. (2013). *Integracija procesov OVS MORS in VOPVD* (Zaključna naloga). Maribor: Poveljniško štabna šola.

Lončar, A. (9. 5. 2016). Sodišče zavrnilo pritožbo Žavbija, osumljenec terorizma ostaja v priporu. *Siol.net.* Pridobljeno na http://siol.net/novice/slovenija/kdo-je-rok-zavbi-teroristicni-osumljenec-ki-ga-zeli-italija-416827?image=1

Mihačič, S. (2012). *Elektronsko bojevanje v SV – samostojna disciplina ali kot del elektronskega izvidovanja* (Zaključna naloga). Maribor: Šola za častnike.

Ministrstvo za obrambo RS. (2015). *Obveščevalno varnostna služba*. Pridobljeno na http://www.mo.gov.si/si/o_ministrstvu/organizacija/obvescevalno_varnostna_sluzba/

Na Morsu izigravali predpise? (17. 9. 2008). *24ur.com.* Pridobljeno na http://www.24ur.com/novice/slovenija/na-morsu-izigravali-predpise.html

Parliamentary Assembly. (1999). *Control of internal security services in Council of Europe member state* (Recommendation 1402). Pridobljeno na http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16689&lang=en

Pečar, J. (2001). Javnost ali tajnost državnih podatkov. *Revija za kriminalistiko in kriminologijo, 52*(1), 3–10.

Podbregar, I. (2011). Pred reinženiringom nacionalnovarnostnega sistema – priložnosti za Slovensko vojsko. *Bilten Slovenske vojske*, *13*(2), 15–26. Pridobljeno na http://www.slovenskavojska.si/fileadmin/slovenska_vojska/pdf/vojaski_izzivi/svi_13_2.pdf

Podbregar, I. (ur.). (2012). *Obveščevalno-varnostna dejavnost: procesi, metode, nadzor*. Ljubljana: Fakulteta za varnostne vede.

Policija. (n. d.). *Uprava kriminalistične policije – organiziranost.* Pridobljeno na http://www.policija.si/index.php/o-policiji/organiziranost/171

Politiets Efterretningstjeneste [PET]. (n. d. A). *About PET*. Pridobljeno na https://www.pet.dk/English/About%20PET.aspx

Politiets Efterretningstjeneste [PET]. (n. d. B). *Publications*. Pridobljeno na https://www.pet.dk/English/Publications.aspx

Prisluškovanje: Studio ob 17h. (6. 10. 2015). *RTV SLO.* Pridobljeno na http://4d.rtvslo.si/arhiv/studio-ob-17h/174363728

Purg, A. (1995). *Obveščevalne službe*. Ljubljana: Enotnost.

Ravnak, R. (2012). *Varnostna zagotovitev vojaških aktivnosti in načrtovanje varnostne zagotovitve* (Zaključna naloga). Maribor: Šola za častnike.

Rečnik, G. (27. 3. 2013). Slovenija je oaza za shode neonacistov. *RTV SLO, Val 202.* Pridobljeno na http://val202.rtvslo.si/2013/03/zulj-skrajne-skupine-ki-sirijo-nestrpnost/

Resolucija o strategiji nacionalne varnosti Republike Slovenije [ReSNV-1]. (2010). *Uradni list RS*, (27/10).

Rode, A., Derviz, D. in Henigman, Ž. (2009). Vojaška obveščevalno-varnostna dejavnost v podpori delovanja Slovenske vojske v operacijah kriznega odzivanja. *Bilten Slovenske vojske*, *11*(2), 55–68.

Rychla, L. (16. 3. 2016). Danish intelligence agency to start 'hacker academy' to fight cyber warfare. *Cph Post Online*. Pridobljeno na http://cphpost.dk/news/danish-intelligence-agency-to-start-hacker-academy.html

Schweizer Armee. (n. d.). *Militärische Sicherheit (Mil Sich)*. Pridobljeno na http://www.vtg.admin.ch/internet/vtg/de/home/schweizerarmee/organisation/fsta/milit.html

Secret Intelligence Service [MI6]. (n. d.). *Explore life at SIS*. Pridobljeno na https://www.sis.gov.uk/explore-life-at-sis.html

Securtiy Service [MI5]. (n. d. A). *Careers*. Pridobljeno na https://careers.mi5.gov.uk/

Securtiy Service [MI5]. (n. d. B). *Working at MI5*. Pridobljeno na https://careers.mi5.gov.uk/working-at-mi5

Sigurnosno-obavještajna agencija. (2015). *Ured za nacionalnu sigurnost*. Pridobljeno na https://www.soa.hr/hr/povijest/uns/

Slovenska obveščevalno-varnostna agencija [SOVA]. (2015). *Sporočila za javnost*. Pridobljeno na http://www.sova.gov.si/si/medijsko_sredisce/sporocila_za_javnost/

Sotlar, A. (2012). Nadzor nad delovanjem obveščevalno-varnostne dejavnosti. V I. Podbregar (ur.), *Obveščevalno-varnostna dejavnost: procesi, metode, nadzor* (str. 437–488). Ljubljana: Fakulteta za varnostne vede.

Swiss Federal Archives. (n. d.). *Political police and state security in Switzerland*. Pridobljeno na https://www.bar.admin.ch/bar/en/home/research/searching/topics/nachrichtendienste--spione--landesverraeter-und-staatsschutz-in-/die-politische-polizei-und-der-staatsschutz-in-der-schweiz-.html

The Swiss Armed Forces. (n. d.). *Military Intelligence Service (J2).* Pridobljeno na http://www.vtg.admin.ch/internet/vtg/en/home/schweizerarmee/organisation/fsta.html

Toporišič, J. (2006). *Besedjeslovne razprave.* Ljubljana: Založba ZRC.

Trampuš, J. (17. 6. 2007). »Če enkrat delaš za tujo obveščevalno službo, delaš zanjo zmeraj. S tega vlaka ni mogoče izstopiti.« – mag. Zoran Krunić, strokovnjak za varnostna vprašanja. *Mladina*. Pridobljeno na http://www.mladina.si/93442/ce-enkrat-delas-za-tujo-obvescevalno-sluzbo-delas-zanjo-zmeraj-s-tega-vlaka-ni-mogoce-izstopiti/

Urad vlade RS za komuniciranje. (20. 4. 2016). *Sporočilo za javnost – 85. redna seja Vlade RS*. Pridobljeno na http://www.vlada.si/fileadmin/dokumenti/si/Sporocila_za_javnost/2016/sevl85-16.pdf

Uredba o obveščevalno-varnostni službi Ministrstva za obrambo [Uredba OVS]. (1999). *Uradni list RS*, (63/99).

Uredba o organizaciji in delovanju Nacionalnega centra za krizno upravljanje. (2006). *Uradni list RS*, (9/06).

Ustavno sodišče RS. (2005). Odločba Ustavnega sodišča RS številka Up-412/03-21 z dne 8. 12. 2005.

Verteidigung, Bevölkerungsschutz und Sport. (n. d. A). *Nachrichtendienst des Bundes*. Pridobljeno na http://www.vbs.admin.ch/internet/vbs/de/home/departement/organisation/ndb.html

Verteidigung, Bevölkerungsschutz und Sport. (n. d. B). *Publikationen*. Pridobljeno na http://www.vbs.admin.ch/internet/vbs/de/home/documentation/publication.html

Vlada RS. (23. 10. 2015). *Vzpostavitev delovanja medresorske analitične skupine, ki deluje v okviru Nacionalnega centra za krizno upravljanje*. Pridobljeno na http://www.vlada.si/medijsko_sredisce/sporocila_za_javnost/sporocilo_za_javnost/article/vzpostavitev_delovanja_medresorske_analiticne_skupine_ki_deluje_v_okviru_nacionalnega_centra_za_k/

Voh Boštic, A. (13. 1. 2015). Kako bo minister Koprivnikar preprečil politično zaposlovanje v javni upravi. *Podčrto*. Pridobljeno na https://podcrto.si/kako-bo-minister-koprivnikar-preprecil-politicno-zaposlovanje-v-javni-upravi/

Voh Boštic, A. (29. 2. 2016). Absurdna plačna lestvica pri zaposlovanju informatikov stane državo milijone evrov. *Podčrto*. Priodbljeno na https://podcrto.si/absurdna-placna-lestvica-pri-zaposlovanju-informatikov-stane-drzavo-mlijone-evrov/

Wyss, M. (2011). *Zivile Nachrichtendienstsysteme im europäischen Umfeld der Schweiz*. Zürich: Center for Security Studies.

Zakon o nalogah in pooblastilih policije. (2013, 2015). *Uradni list RS*, (15/13, 23/15).

Zakon o obrambi. (2004, 2015). *Uradni list RS*, (103/04, 95/15).

Zakon o organiziranosti in delu v policiji. (2013, 2014, 2015). *Uradni list RS*, (15/13, 11/14, 86/15).

Zakon o Slovenski obveščevalno-varnostni agenciji [ZSOVA]. (2006). *Uradni list RS*, (81/06).

Zakon o tajnih podatkih. (2006). *Uradni list RS*, (50/06).

Završnik, A. (2013). Blurring the Line between Law Enforcement and Intelligence: Sharpening the gaze of surveillance? *Journal of Contemporary European Research*, *9*(1), 181–202

Zver, D. (2015). *Kompetence analitika v obveščevalnih in varnostnih službah* (Magistrsko delo). Ljubljana: Fakulteta za varnostne vede.

O avtorjih:

Jaroš Britovšek, univerzitetni diplomirani politolog Fakultete za družbene vede Univerze v Ljubljani, doktorski študent Fakultete za varnostne vede Univerze v Mariboru, zaposlen na Ministrstvu za obrambo Republike Slovenije. E-pošta: jaros.britovsek@mors.si

Aleš Čretnik, univerzitetni diplomirani politolog Fakultete za družbene vede Univerze v Ljubljani in magister obveščevalnih in varnostnih ved Univerze Salford v Manchestru (Velika Britanija), zaposlen na Ministrstvu za obrambo Republike Slovenije. E-pošta: ales.cretnik@mors.si

Varnost na športnih in drugih javnih prireditvah: poročilo o okrogli mizi

V okviru 17. konference Dnevi varstvoslovja, ki jo je 8. in 9. 6. 2016 v Kranjski Gori organizirala Fakulteta za varnostne vede Univerze v Mariboru, je potekala tudi okrogla miza z naslovom *Varnost na športnih in drugih javnih prireditvah*. Na okrogli mizi so sodelovali dr. Branko Lobnikar s Fakultete za varnostne vede, ki je bil moderator, mag. Mile Nunič, strokovnjak s področja policijske dejavnosti za zagotavljanje javnega reda in miru ter za javna zbiranja, Marjan Jakše, vodja komisije za varnost pri organizacijskem komiteju Vitranca in Planice, dveh izmed naših največjih športnih dogodkov, ter Milan Vačovnik, svetovalec uprave za varnost zasebnovarnostnega podjetja Varnost Maribor, ki ima bogate izkušnje z zagotavljanjem varnosti na največjih športnih in drugih prireditvah.

Iztočnice za razpravo so bile podane že v zborniku povzetkov konference, nekatere pa je na začetku okrogle mize predstavil tudi moderator. Zagotavljanje varnosti na športnih prireditvah postaja vedno bolj pomembna tema. Lobnikar je izpostavil, da stroški za zagotavljanje varnosti, še posebej pri velikih športnih dogodkih, naraščajo. Kot primer je predstavil podatke o stroških organizacije olimpijskih iger. Leta 2004 so olimpijske igre v Atenah predstavljale mejnik pri vrtoglavih stroških za zagotavljanje varnosti. Pred olimpijskimi igrami so v Grčiji začeli veljati obsežni vojaški varnostni ukrepi, s katerimi naj bi podprli varnostne ukrepe na igrah. 35 grških vojaških ladij in na ducate patruljnih čolnov je nadzorovalo Egejsko morje in obale olimpijskih objektov. V olimpijsko mesto so prispele enote Nata, ki so s pomočjo posebnih radarskih letal nadzorovale zračni prostor. Pri varovanju olimpijskih iger je pomagalo tudi okoli 20 ladij iz stalne sredozemske flote Nata. Za varnost je skrbelo skupaj več kot 70.000 pripadnikov varnostnih sil. Stroški za varovanje so presegli milijardo evrov in so bili višji kot kadarkoli v zgodovini olimpijskih iger. Na zimskih olimpijskih igrah v Vancouvru 2010 je za varnost med drugimi skrbelo več kot 15.000 varnostnikov, stroški za varnost pa so znašali 940 milijonov ameriških dolarjev. Varovanje olimpijskih iger 2012 v Londonu je stalo 650 milijonov evrov, za varnost pa je skrbelo 24.000 ljudi. Stroški zimskih olimpijskih iger v Sočiju leta 2014 so presegli mejo 50 milijard ameriških dolarjev, pri čemer je velik del odpadel prav na zagotavljanje varnosti. Pred začetkom iger je Rusija v Sočiju sprožila največjo varnostno akcijo v zgodovini olimpijskih iger. Pri zagotavljanju varnosti je sodelovalo več kot 30.000 policistov, ki so imeli nalogo omejevati dostop do prizorišč. »Vsa prizorišča so pod nadzorom, sprožen je tudi sistem nadzora iz vesolja,« je takrat povedal minister za izredne razmere Vladimir Pučkov. Za varnost na ulicah Ria de Janeira naj bi v času poletnih olimpijskih iger leta 2016 skrbelo približno 47.000 policistov in 38.000 vojakov, stroški za varnost pa naj bi bili dvakrat večji kot v Londonu 2012.[1]

1 *V času avgustovskih olimpijskih iger v Riu de Janeiru je za varnost na športnih prizoriščih skrbelo kar 85.000 policistov in vojakov, kar je dvakrat več kot v primerjavi z olimpijskimi igrami pred štirimi leti v Londonu. Zvezna vlada je za varnost namenila 890 milijonov dolarjev. Stroški celotnih olimpijskih iger pa so ocenjeni na 11,5 milijard ameriških dolarjev.*

Samo ta dejstva povedo, da športni dogodki velikega obsega še zdaleč niso le srečevanje športnikov, ki se merijo v tem, kdo je višji, močnejši, hitrejši in boljši. Tudi nasilje v športu je vedno bolj pereča tema.

Športne prireditve in javna zbiranja so področje, ki je v zadnjem času doživelo veliko sistemskih sprememb. Na predlog moderatorja je Mile Nunič podal svoj pogled na obravnavano tematiko. Dejal je, da je šport (kot ena od oblik javnega zbiranja) v zadnjem času tudi posel, za tiste, ki zagotavljajo red, pa izjemen strošek. Nedvomno so se tega zavedali tudi tisti, ki so leta 2001 pripravljali novi zakon o javnem zbiranju. Pri tem so morali upoštevati omejitve iz 42. člena Ustave RS, kjer je opredeljena pravica do mirnega zbiranja in do javnih zborovanj. Pri tem je razpravljavec poudaril, da ne gre za katerokoli zbiranje, temveč izključno za mirno zbiranje. Čeprav kar nekaj javnih prireditev in javnih shodov mine popolnoma mirno in neopazno, je res, da se javnost in tisti, ki se ukvarjajo z zagotavljanjem reda na javnem zbiranju, osredotočijo na tista javna zbiranja, kjer prihaja do izgredov, nemirov in drugih kršitev. Da bi zagotovili red v okviru javnega zbiranja, so leta 2001 pripravili Zakon o javnih zbiranjih, ki je bil objavljen leta 2002 in stopil v veljavo leta 2003. Pri pripravi zakona so izhajali iz predpostavke, da se problematika nasilja pojavlja zgolj na nekaterih javnih zbiranjih. Zlasti gre za športne prireditve, predvsem so to nogometne tekme. Nunič je izpostavil osrednjo vlogo organizatorja, ki je z vodjo javnega zbiranja in rediteljsko službo odgovoren za zagotavljanje reda. Nikakor ni primarna naloga države, državnih organov, policije ali katerih drugih, da skrbijo za red na prireditvenem prostoru. To je naloga organizatorja. Izjema je zgolj na državnih proslavah, kjer zakon to primarno nalogo daje policiji. V vseh ostalih primerih pa so naslednji akterji ključni za zagotavljanje reda in miru na javnih zbiranjih – organizator, vodja in rediteljska služba. Nunič pravi, da lahko o rediteljski službi sicer razpravljamo, ali je bolje vključevati laike/neprofesionalce ali rediteljsko službo sestavimo iz vrst varnostnikov, vendar ne glede na to, kdo opravlja rediteljsko službo, mora zagotoviti red. Z nekaterimi podzakonskimi akti so v skladu z evropsko konvencijo o preprečevanju nasilja na športnih prireditvah na nogometnih tekmah normativno uredili vse kriterije in vse tisto, kar je treba zagotoviti kot neki nadstandard na športnih prireditvah. Nunič je izpostavil problem, da spremembe zakonodaje običajno sledijo tragičnim dogodkom, kot sta bila na primer v diskoteki Lipa in baru Roxly v Ljubljani.

Mile Nunič je poudaril, da tudi, če organizator zagotovi vse ukrepe, od upravne enote prejme dovoljenje in upošteva vse predloge policije, še vedno ni zagotovila, da bo zbiranje potekalo mirno. Nekateri menijo, da lahko z represivnimi ukrepi uredimo določene zadeve v družbi, in zato smo pred tem, da dobimo poseben zakon, ki bo veljal zgolj na športnih prireditvah. Nekatere države to prakso že poznajo. V Sloveniji smo pri pripravi nove policijske zakonodaje en del tega umestili v nov zakon o nalogah in pooblastilih policije, ko so policisti dobili dve novi pooblastili: prepoved udeležbe na športnih prireditvah (62. člen ZNPPol) in prekinitev potovanja na športno prireditev (63. člen ZNPPol). Gre za pooblastili za zagotavljanje varnosti in reda ter preprečevanja nasilja na športnih prireditvah. Tako lahko policisti nasilnim skupinam preprečijo dostop do športne prireditve, tistim navijačem, ki so bili v preteklosti že kaznovani zaradi kršitev

na tekmah, pa lahko začasno (za eno leto) prepovejo ogled športne prireditve. Pri tem je treba še enkrat poudariti, da je za red in varnost na športnih prireditvah odgovoren organizator športne prireditve. Policisti posredujejo šele takrat, ko sta z dogajanjem na športni prireditvi ogrožena javni red in mir ter organizator varnosti ni več zmožen zagotavljati. V letu 2015 je bilo pet takšnih primerov. Zakon je omogočil, da če rediteljsko službo na športni prireditvi opravljajo varnostniki, lahko od policije pridobijo podatke o osebah, ki jim je prepovedan vstop na športne prireditve, in tem osebam vstop na to prireditev tudi preprečijo. Ta ukrep je usmerjen bolj v huligane in povzročitelje neredov, pa vendar imamo občutek, da tisti, ki skrbijo za vstop na prireditev, vselej ne ugotavljajo, ali je nekomu prepovedan vstop na prireditev. Pomembno je omeniti tudi to, da Zakon o javnih zbiranjih določa, da se mora organizator s policijo dogovoriti, na kakšen način bo ta sodelovala pri zagotavljanju varnosti na tistih javnih zbiranjih, kjer se pričakujejo neredi. Po tem, ko je bil spremenjen pravilnik za izvajanje zakona o javnih zbiranjih, je policija stroške za zagotavljanje varnosti na javnih prireditvah začela zaračunavati organizatorju, saj je to pridobitna dejavnost, zakaj bi imela država s tem stroške. Zavedati se moramo, da je to resnično velika obremenitev za policijo. V letu 2015 je policija sodelovala pri 3.800 varovanjih javnih prireditev. Razumeti je treba, da policija ni stražar na prireditvenem prostoru, zato mora organizator plačati policiji, če ta skrbi za red.

V nadaljevanju je besedo povzel Marjan Jakše, ki je odgovoren za zagotavljanje varnosti na dveh največjih športnih prireditvah v Sloveniji: Vitranc in Planica. Z vidika zagotavljanja varnosti je tudi mirno srečanje, kot sta smučanje ali poleti v smučarskih skokih, resen zalogaj. Jakše meni, da je zakon lahko pisati, precej težje ga je izvajati v praksi. Prav zaradi tega je pomembno, kakšen je odnos organizatorjev do javnih prireditev. Organizator naj bi bil vesten, odgovoren in zelo konstruktiven. A žal na velikih javnih prireditvah takšnega organizatorja ne pozna. Ti so slabi, neodgovorni in za nameček povzročajo nesorazmerno več stroškov, kot so bili z normalno dejavnostjo teh akterjev predvideni. Veliko določb v zakonu o javnem zbiranju je tistih, ki neposredno določajo, kaj organizator mora narediti pri izvedbi same javne prireditve. Kako izvajati te določbe, pa je delo organizatorja. Ti dve prireditvi, Vitranc in Planica, ki jih imajo na Gorenjskem, ter Zlata lisica na Štajerskem, so klasičen primer, kako prireditev izpeljati na tako obširnem področju, predvsem pa na specifičnem področju terena. Jakše je opozoril na nekatere organizacijske probleme, ki se nanašajo predvsem na finančni zalogaj varovanja takih prireditev. Poudaril je, da se finančni zalogaj za varnost povečuje, še posebej v povezavi s stopnjo ogroženosti javne prireditve. Ta ogroženost pa je tudi posledica dogajanj v družbi. Tudi nova dognanja glede terorizma povzročajo, da mora organizator na tej sferi narediti in posodobiti določene varnostne elemente ob vstopu na prireditveni prostor ter znotraj prireditvenega prostora. Organizator ne sme dovoliti, da organizacijo varovanja vodijo posamezniki, ki niso odgovorni in ki lahko povzročijo večje eskalacije na javnih prireditvah. Nikakor ne smemo dovoliti, pravi Jakše, da organizator na podlagi večjega finančnega zalogaja popusti pri zagotavljanju varnosti. Pri vseh teh organizacijskih odborih, kjer je sodeloval tudi sam, ob koncu prireditve naredijo analizo, s katero so do sedaj vedno ugotovili, da vložen denar in trud, ki so ga vložili v posamezno prireditev,

ni bil zaman. Za Planico 2016 je povedal, da je uspela v vseh sferah. Uspela je prireditev, uspeli so tekmovalci, vreme, bila je neizmerna evforija ljudi in športno navijanje. Vse to se je poklopilo in skoraj ne verjame, da se bo še kdaj. Naredili so že analizo, s katero so ugotovili ogromno dobre prakse, ki so jo dali v varnostni načrt že z lanskoletne prireditve. Kar naenkrat pa so se soočili z novimi dejstvi in okoliščinami, pri katerih vedo, da bo treba investirati še več denarja, hkrati pa ohraniti novosti v Planici: večje število obiskovalcev, struktura obiskovalcev, zagotoviti manj alkohola ter posledično zmanjšati negativne pojave na javni prireditvi.

Subjekti, ki sodelujejo pri varovanju prireditev, so reditelji, varnostniki in organizatorji. Reditelji in varnostniki delujejo po načrtu varnostne službe, to je načrt organizatorja, ter policija, ki dela po svojem načrtu. Zelo pomembno je, da je usklajevanje teh treh dobro, strokovno, predvsem pa pravi čas. Ustna obravnava zagotavljanja in izdajanja njihove odločbe za javno prireditev je zelo primeren čas, da se na celostni obravnavi ugotovi, kaj še manjka, kateri so tisti elementi, ki bi še več doprinesli pri zagotavljanju varnosti. Pri organizaciji Planice so šli še nekoliko dlje, saj se že pred samo ustno obravnavo dobijo z varnostniki in reditelji. Analizirali so moč prireditelja in funkcijo varnostne službe. Prišli so do zaključkov, da pozitivne strani izhajajo iz prireditelјev in obiskovalcev. Tako se lahko bolje poistovetijo s samim obiskovalcem, večjo profesionalnost pa dosežejo s tem, da reditelje z obeh prireditev (Planica in Vitranc) tudi izobražujejo. Že več let imajo delovno skupino, ki pa jo pomlajujejo. Jakšič pravi, da je 120–130 ljudi težko stalno izobraževati. A med njimi je od 20 do 25 % upokojenih policistov, s katerimi se še bolj približajo poslanstvu. Sodelovanje vseh treh subjektov je zagotovilo, da bo prireditev uspela, kljub temu, da so lahko prisotne nepredvidljive situacije.

Lobnikar je povzel, da je že zelo dolgo od takrat, ko so javni red in mir na nogometnih tekmah zagotavljali policisti. Sedaj je že celo desetletje od takrat, ko je to področje prevzela varnostna služba. Ko govorimo o zagotavljanju varnosti z vidika zasebnovarnostnih podjetij, se mnogokrat ne zavedamo kompleksnosti in posebnosti tega položaja, ki ga imajo tovrstna gospodarska podjetja pri izvajanju tako pomembne dejavnosti. Zato verjame, da je Milan Vačovnik iz Varnosti Maribor, ki zagotavlja varnost na nogometnih tekmah v Mariboru, zelo primeren sogovornik, da predstavi zelo pomemben zasebnovarnostni vidik.

Vačovnik je povedal, da je neka javna prireditev, ki se zgodi v mestu, šok za mesto. Za nekatere ljudi predstavlja prireditev situacijo, na katero niso bili pripravljeni. Namreč treba se je zavedati, da imamo dve strani: ena stran je zelo zainteresirana za športno prireditev, druga stran pa ne. Ta nezainteresirana stran je za to prireditev zelo rizična, saj se prireditve bojijo, jih moti, zato se posledično umikajo iz mesta. Pomembno je, da se postavi neko ravnotežje med temi, ki si prireditve želijo in ki jim je to v interesu, ter med tistimi, ki jih to moti in se tega bojijo.

Vačovnik je poudaril, da se moramo zavedati, da ne govorimo le o prireditvi sami, temveč o sklopu nekega življenja v mestu, lokalni skupnosti, ki se dogaja pred to prireditvijo in ki se bo dogajala po prireditvi. Zasebnovarnostna podjetja so gospodarska družba, ki so v javnem in gospodarskem interesu. Ta gospodarska družba ne živi le za to, da izvaja varovanje na prireditvi, temveč živi za to, da

izvaja zelo veliko različnih oblik varovanja. Zasebno varovanje se je od leta 1994 zakonsko trikrat spremenilo, vsak zakon pa je imel vsaj tri dopolnitve. Poleg tega ima zasebno varovanje več kot 20 podzakonskih aktov, kar nam prikazuje, da je to zelo regulirano področje. Za izvajanje dela imajo 8 licenc; in ena od njih je za varovanje na javnih zbiranjih. Če nekdo želi izvajati to storitev, mora gospodarska družba dati dovoljenje, poleg tega pa se morajo varnostniki usposabljati, da dobijo poklic varnostnik izvajalec varovanja na javnem zbiranju.

Ko se pogleda samo ta storitev, ki se izvaja na prireditvenem prostoru, se moramo zavedati, da druge varnostne storitve, ki se izvajajo v mestu, zaradi tega ne smejo trpeti. A nekateri naročniki se takrat počutijo ogrožene (bencinski servisi, finančne ustanove), saj ob takšnem dogodku pride v mesto večja skupina ljudi, in vsi drugi njihovi naročniki se (lahko) počutijo ogrožene. Njihova funkcija (funkcija zasebnovarnostne službe) je, da vsem naročnikom predvidijo ukrepe, s katerimi zmanjšajo ta občutek ogroženosti. Po drugi strani pa tudi oni sami ne morejo varno izvajati nekaterih drugih storitev, ki jih drugače izvajajo nemoteno. Ne morejo polniti bankomatov, ne morejo prevažati denarja tako kot v normalnih razmerah, ne morejo nositi denarja v nočne trezorje in podobno. Zato ne smemo gledati samo na prireditev znotraj prireditvenega prostora, ampak moramo gledati na varnost v lokalni skupnosti v celoti. Namreč vsem njihovim naročnikom morajo nuditi višjo stopnjo varnosti, plus višjo stopnjo varnosti na tej prireditvi. Za razliko od ostalih subjektov, ki izvajajo varnost na prireditvah, so za njih vsi obiskovalci tudi potencialni naročniki ali obstoječi naročniki, ki jih morajo obravnavati zelo previdno in profesionalno. Poleg tega pa so njihovi zaposleni najbolj ogroženi, saj so na vhodih in imajo stik s posamezniki. Izvajajo tudi površinske preglede, opozarjajo ljudi, ki se gibajo na teh prostorih, izvajajo ukrepe in so prisotni na vseh ograjah.

Vačovnik je povedal, da se moramo zavedati, da njihovi zaposleni na javni prireditvi predstavljajo blagovno znamko. Oni niso etiketirani kot varnostna služba, temveč so etiketirani kot blagovna znamka izvajalca. Če bo prišlo do konflikta njihovega izvajalca, se ne bo govorilo, da je bil problem v varnostni službi, ampak da je bil problem pri podjetju, ki je izvajalo varnost. In to je tisto, kar ima lahko posledice tudi naslednji dan po javni prireditvi. Ta večplastnost zagotavljanja varnosti na javni prireditvi je za njih zelo velikega pomena in velik izziv. Vlaganje v kakovost, vlaganje v usposabljanje, vlaganje v usposobljenost varnostnikov je zelo zahtevno.

Razpravo je povzel Nunič. Zaveda se, da neko okolje živi za neko javno prireditev. Silvestrovanje na prostem ali neke druge tradicionalne prireditve, s katerimi živi okolje, so tudi javna prireditev. A pomembno je, da si postavimo vprašanje, kje organizator skrbi za varnost? Nikjer drugje kot le na prireditvenem prostoru. Izven prireditvenega prostora nima nobenih pristojnosti. Tam jih ima policija. Če je športna prireditev v dvorani, če se dogajajo kršitve s strani navijačev na poti, tam rediteljska služba nima pristojnosti. Rediteljska služba na javnem zbiranju ima samo eno nalogo: da skrbi za red. Blagovna znamka gor ali dol. To je njena temeljna naloga. Tako kot je naloga policije, da zagotovi red, z vsem spoštovanjem pravil tistega, ki je v postopku. A kombinacija rediteljske in varnostne službe se v praksi ni pokazala za dobro. V nekaterih primerih so

nekateri reditelji bolje odreagirali na kršitve kot pa varnostniki. Ključno je, kdaj odreagirati na neki dogodek in kdaj pričeti s postopkom.

Lobnikar se je strinjal z Nuničem, a popolnoma razume tudi Vačovnika, ki ga je vprašal, kakšna je njihova osebna izkušnja oziroma izkušnja podjetja glede rediteljev. Vačovnik je povedal, da so inšpektorji po več inšpekcijskih nadzorih na nogometnih tekmah podali mnenje in napisali, da reditelji izvajajo slab pregled na vstopnih točkah, za to je posledično več pirotehnike na prireditvenem prostoru (igrišču). Razlog je v tem, da reditelji nimajo pooblastil pregleda vrhnjih oblačil, temveč samo za pregled prtljage. Usposobljenost in opremljenost rediteljev je nižja kot varnostnikov; rediteljska služba nima nobenega programa usposabljanja in opremljanja. Do problemov je prihajalo takrat, ko je prihajalo do incidentov. Varnostnik, ki ima pooblastila, lahko pridrži osebo, reditelj pa tega pooblastila nima. Zelo jih skrbi, saj se v zadnjem času povečuje število rediteljev na račun varnostnikov. Problem so izpostavili tudi glede preverjanja istovetnosti akreditacij, saj tudi teh pooblastil reditelji nimajo. In ne nazadnje je predlog inšpekcijske službe, da se regulira ta dejavnost rediteljske službe.

Saša Kuhar

Vodenje v policiji: poročilo o okrogli mizi

V sklopu 17. konference Dnevi varstvoslovja je bila 8. 6. 2016 v Kranjski Gori izvedena okrogla miza z naslovom »Vodenje v policiji«. Razpravo je vodil izr. prof. dr. Branko Lobnikar s Fakultete za varnostne vede Univerze v Mariboru, kot razpravljavci pa so sodelovali predstavniki treh organizacijskih nivojev slovenske policije. Vidike nacionalnega nivoja je predstavila mag. Tatjana Bobnar, namestnica generalnega direktorja policije; stališča regionalnega nivoja je zastopal Janez Ogulin, direktor Policijske uprave [PU] Novo mesto; lokalni nivo pa je predstavljal komandir Policijske postaje [PP] Murska Sobota Tomislav Habulin.

Namen razprave je bil preko predstavljenih stališč in izkušenj policijskih vodij ugotoviti aktualne izzive vodenja sodobnih policijskih organizacij. Vprašanje o primernih načinih vodenja se pojavlja predvsem v zadnjem desetletju, ko prihaja do transformacije tradicionalnega (birokratskega) modela policijske dejavnosti v sodobni pristop, ki zahteva večnivojske spremembe. Slovenska policija si namreč v zadnjih letih aktivno prizadeva za uvedbo novih pristopov k zagotavljanju varnosti in preprečevanju kriminalitete. Ta prizadevanja se kažejo v obliki uvajanja različnih preventivnih aktivnosti, demokratičnega in decentraliziranega vodenja, izboljševanja učinkovitosti reševanja problemov ter uresničevanja v skupnost usmerjenega policijskega dela.

Policijski vodje se v kontekstu sodobnih varnostnih razmer soočajo z uvajanjem sprememb na treh ravneh: na ravni vodij, ravni zaposlenih in organizacijski ravni. V tem kontekstu je najprej potrebna sprememba filozofije, znanja, vrednot in vedenja vodij, od katerih je odvisen uspeh uvajanja novih policijskih strategij in posledično uspeh pri uvajanju sprememb na ravni zaposlenih. Pri tem se pojavlja vprašanje, kako organizirati sistem usposabljanja, da bi bilo uvajanje sprememb pri policijskih vodjih najbolj uspešno in da bi se odpravila skepticizem ter tradicionalna mentaliteta, ki nasprotujeta sodobni strategiji policijske dejavnosti. Pri prilagajanju policijske organizacije so potrebne tudi organizacijske spremembe, v smislu prehoda od avtoritativnosti, konformnosti, konzervativnosti in tajnosti, ki zaznamujejo tradicionalni model, k pripadnosti, diskreciji, inovativnosti, zaupanju, javnosti in transparentnosti policijskega dela. Za uvedbo nove paradigme je treba poskrbeti za integriteto, opolnomočenje in osebno zavzetost policistov. Odgovornost za to leži ravno na policijskih vodjih, saj so ti nosilci oz. agenti uvajanja sprememb.

Moderator je pojasnil, da je izhodiščna teza okrogle mize zavedanje, da policijska organizacija, ki je po naravi hierarhična institucija, ne more delovati zgolj po principu stroge hierarhije, ampak na podlagi kompetentnega upravljanja, na znanju utemeljeni dejavnosti in legitimnosti. V razpravi so se dotaknili treh vsebin: internih organizacijskih izzivov policije, kompetenc policijskih vodij in načrtov za prihodnost pri uresničevanju cilja povečanja osebne zavzetosti policistov.

1 ORGANIZACIJSKI IZZIVI

Razpravo je odprla mag. Bobnar, ki je potrdila aktualnost teme, sploh v kontekstu migracij in sindikalnih dejavnosti, ki sta v zadnjem letu zaznamovali delo slovenske policije. Zelo pomembno je namreč, da so v stresnih situacijah vodje empatični, razumevajoči in sposobni voditi z vzgledom. Biti dober in uspešen vodja v (slovenski) policiji je zelo zahtevna naloga, razlog pa je v doseganju ravnovesja med vodstvenimi in strokovnimi stališči, saj večina policijskih vodij izhaja iz operative, od njih pa se zahteva hitra transformacija v kompetentnega šefa. Policija ima velika pooblastila, pri svojem delu pa posega v temeljne človekove pravice, zato sta pravilen pristop k vodenju in skrb za dobre odnose z zaposlenimi in državljani izjemnega pomena. Slednjega se slovenska policija sicer dobro zaveda. Razpravljavka je kot primer sistemskega pristopa na tem področju izpostavila Odbor za etiko in integriteto ter Center za raziskovanje in socialne veščine v slovenski policiji, kjer se izvajajo aktivnosti za krepitev etike, integritete, opolnomočenosti in krepitve dobrih odnosov v policiji. Hierarhično poveljevanje je sicer na prvem mestu, ampak ne na račun skrbi za zaposlene. V vodstvu policije se zavedajo, da policijsko delo vpliva na osebno življenje in da je vse več pritiskov na zaposlene z vidika stalne pripravljenosti in dosegljivosti. K temu je prispevala tudi uvedba novih tehnologij, ki so sicer zelo uporabne, vendar so za nekatere policiste in vodje povzročile konstantno, še večjo vpetost v delo. Trenutno se veliko poudarka namenja zagotavljanju enakih možnosti, odpravljanju diskriminacije, zagotavljanju psihološke pomoči zaposlenim in razvoju kompetenc za učinkovito izvajanje policijskega dela v skupnostih. Posebno pomembni področji pri vodenju sta upravljanje s konflikti in mediacija. V policiji se stalno pojavljajo problemi in konflikti, kar pravzaprav ni težava, kadar se vodje teh problemov tudi zavedajo in jih priznavajo. Najbolj problematično je, kadar šefi teh problemov ne priznavajo in se z njimi ne soočajo. Vodje se morajo ves čas izpopolnjevati in zavedati, da niso superiorni, vsemogočni in vsevedni, predvsem pa morajo paziti, da se ne zastrupijo z lastno močjo. Žal se to dogaja tudi v policiji, vendar so se za enkrat mediacije in posredovanja med konflikti izkazala za učinkovita pristopa. Trenutni problem predstavljajo predvsem negativni odnosi med zaposlenimi, v smislu konstantnega socialnega nadzora in obrekovanja, ki ustvarjata destruktivno delovno okolje in posledično vplivata tudi na storilnost policijskih vodij.

Dr. Lobnikarja je v kontekstu razprave o organizacijskih izzivih zanimalo, kako strateški nivo vodij v slovenski policiji doživlja odnose z javnostjo, politiko in drugimi institucijami nadzora.

Namestnica generalnega direktorja je pojasnila, da je za policijske vodje vsak dan težak, saj morajo biti neodvisni in ne smejo dopustiti vpliva politike na svoje delo. Zagotavljati neodvisnost in nepristranskost je sicer težko, saj je policija najbolj nadziran organ. Nadzor se izvaja preko javnosti, politike, ministrstva, Komisije za nadzor obveščevalnih in varnostnih služb, nevladnih organizacij in drugih nadzornih institucij (npr. Varuh človekovih pravic, Informacijski pooblaščenec). Kot neodvisna institucija je policija pod strogim in konstantnim nadzorom, ki prihaja z vseh strani. Pogosto se zato postavlja vprašanje, ali bi bilo treba nadzor nad policijo kako drugače sistemsko urediti.

Z opisanimi stališči se je strinjal direktor PU NM Janez Ogulin, ki je v odgovoru na vprašanje, kako sistem vodenja, regulacije in motiviranja kadrov poteka na regionalni ravni, pojasnil, da tudi policijske uprave občutijo te pritiske. Problem se pojavlja predvsem pri usklajevanju kadrovskega in delovnega področja. Na eni strani je vse več omejitev pri zaposlovanju, na drugi pa je kljub pomanjkanju kadra treba delo izvajati enako kakovostno. Vodenje po načelu hierarhične moči ni rešitev, ko se soočamo z vprašanjem motiviranja kadrov in spodbujanja zaposlenih k uresničevanju temeljnega poslanstva policije. Po njegovem mnenju je policija sicer na dobri poti opolnomočenja policistov, vendar je še vedno nekaj problemov, ki jih je treba razrešiti. Pereče vprašanje, s katerim se sooča pri delu, je, kako vodjem na nižjih ravneh zagotoviti ustrezno znanje in veščine, da bodo ti sposobni učinkovito reševati vodstvene probleme in da bodo ne nazadnje sposobni svoje znanje prenesti na podrejene. Policistom je treba razumno in nazorno predati naloge, vendar so te naloge vse bolj zahtevne. Pogosto za ustrezen in sistematičen pristop preprosto zmanjka časa. To se je pokazalo v nedavni migrantski krizi – izobraževanje se je ustavilo, kar je ustvarilo velike vrzeli, ki jih bo treba nadomestiti. Sočasno se zakonodaja stalno posodablja, razumevanje novih predpisov pa je treba prenesti na vse zaposlene, ki jih izvajajo v praksi. Ta pravila se morajo namreč izvajati enotno, zato je usposabljanje zelo pomembno. Zunanji opazovalci pogosto ne razumejo obsega in kompleksnosti policijske dejavnosti, menijo, da je zapis v zakonodaji dovolj za razumevanje novih pravil. Pa vendar temu ni tako, saj je treba razlago najprej poenotiti in nato usposobiti vse policiste za skladno izvedbo v praksi. Razlaga in medsebojna komunikacija je na PU zelo pomembna, ne nazadnje tudi sam prenos vseh zahtev in obrazložitev na nižjo raven – na PP. Ogulin je poudaril, da je treba tudi na področju policijskega dela v skupnosti uvesti močnejše spremembe. V 90. letih so bile skupnosti bolj povezane kot danes, zato je treba policiste bolj spodbujati k aktivni in zavzeti udeležbi v tej strategiji. Njen namen je delovati proaktivno in probleme reševati skupaj s prebivalci skupnosti. Odgovornost vodij pa je policiste prepričati, da so vsi, še tako banalni (lokalni) problemi, pomembni. Vsak problem je problem preveč in takšno mentaliteto bi morali posvojiti vsi policisti, vendar ta cilj za enkrat še ni povsem dosežen. Glavni izziv na regionalni ravni je pri policistih vzbuditi občutek odgovornosti, da bodo samoiniciativno in kakovostno izvajali naloge na lokalni ravni.

2 KOMPETENCE POLICIJSKIH VODIJ

Moderator okrogle mize je izpostavil, da je situacijski pristop k vodenju odločilnega pomena, vendar v praksi obstajajo različni pristopi k vodenju, ki niso vedno uspešni. Veliko vlogo pri vodstvenem uspehu odigrajo osebnostne lastnosti vodij. Razpravljavce je vprašal, v kolikšni meri je osebnost policijskih šefov pomembna za uspeh policijske organizacije.

Ogulin je pritrdil, da obstajajo različni vodje, sebe ocenjuje kot vpetega in prizadevnega, pri vodenju pa poudarja pomen dobrih odnosov. Sodelavce je treba poznati, zato so letni razgovori, v katerih se zaposlenemu poda možnost izraziti mnenje, izjemnega pomena. Pristop k vodenju v policiji mora temeljiti na

osebnem, odprtem odnosu, nudenju pomoči in mediaciji. Na PU NM poskušajo doseči popolno pokritost razgovorov za vse zaposlene, vendar žal nekateri policisti še vedno ne dosegajo pričakovanj. Sicer se je v zadnjih letih stanje izboljšalo, zato vodje ostajajo optimistični in nadaljujejo v začrtani smeri. Trenuten izziv je upravljanje dela in vedenja tistih zaposlenih, ki ne dosegajo ciljev.

Poleg izzivov strateškega in taktičnega nivoja so pomembna in zanimiva tudi tista vprašanja, s katerimi se sooča operativna raven. Policisti na PP in komandirji so tisti, ki poskrbijo za končno realizacijo ciljev. Tomislav Habulin je potrdil, da so letni razgovori izjemnega pomena pri ocenjevanju zaposlenih, saj je treba za pravi pristop k motiviranju poznati potrebe in stališča zaposlenih. Vsak ima namreč drugačno motivacijo. V odgovoru na vprašanje, kako voditi ljudi, da bodo naloge opravili kakovostno, pa je Habulin pojasnil, da je vodenje umetnost, saj je uspešnost odvisna od situacije. Poznamo toliko vodstvenih stilov, kolikor je policistov. Obstajajo različne enote – v nekaterih je več ljudi ali problemov, v drugih manj. Pri vodenju policijskih postaj je zato treba prilagoditi pristop. Najtežje je voditi manjše enote, ki imajo izjemno veliko obveznosti, od vodij pa se pričakuje opravljanje dela in izvajanje nalog z manjšim številom kadrov. Pri tem je Habulin izpostavil, da je zelo verjetno, da bo v Sloveniji zaposlenih vse manj policistov, medtem ko količina problemov ostaja enaka. Policija bo zato morala biti sposobna z manj narediti enako ali še več. Problem je ta, da je nadziranje kakovosti dela v popolnosti skoraj nemogoče, saj vodje niso prisotni pri izvajanju vseh policijskih postopkov. Posredno odgovarjanje komandirjev za napake policistov je zato nekoliko sporno. Za kakovostno vodenje v takšni organizaciji, kot je policija, je strokovno znanje ključno. Vodje morajo v znanju in veščinah presegati svoje sodelavce, saj je njihova naloga ocenjevati in nadzirati izvajalce. Ker je ogromno predpisov in omejitev, je še posebej pomembno poznavanje pravil glede uporabe policijskih pooblastil in delovno-pravnega področja. Kot primer, kako pomembne so organizacijske kompetence in pravna znanja, izpostavi izdelovanje delovnih razporedov, saj je treba pri tem uskladiti tako želje zaposlenih kot zakonske omejitve. Kot vodstveno težavo na operativni ravni je izpostavil tudi navodila, ki prihajajo od višjih instanc. Vsak nadzorni organ ima svoje apetite, ki jih morajo vodje na operativni ravni izpolnjevati, vendar so te zahteve pogosto neprilagojene okolju in specifikam posameznih enot. V odzivu na vprašanje, kakšne vzvode imajo na voljo za motiviranje kadrov in uveljavljanje lastnih stališč, ocenjuje, da je možnosti zelo malo.

Habulin je ocenil tudi proces opolnomočenja zaposlenih na policijski postaji z vidika policijskega dela v skupnosti. Po njegovem mnenju so vodje relativno dobro usposobljeni, saj se v Policijski akademiji izvajajo izobraževanja za bodoče vodje. Namestnica generalnega direktorja je temu pritrdila in pojasnila, da policisti načeloma zelo dobro ocenjujejo kompetence, integriteto in odnose svojih vodij. Ko se je v policiji začelo bolj resno govoriti o vodstvenih problemih, so komandirji policijskih postaj izrazili željo po izobraževanju policistov glede socialnih veščin. To so upoštevali – preko tečajev, ki jih v sodelovanju z vodjem Centra za etiko in integriteto izvajajo na lokalni ravni. Seveda obstajajo tudi takšni vodje, ki niso razvili pravih kompetenc, vendar to posledično vodi tudi v druge delovne in organizacijske probleme, zato se problematični vodstveni kader hitro opazi.

Dr. Lobnikar je pritrdil omenjenim ugotovitvam glede pomembnosti vodstvenih kompetenc, ki so na policijskem področju zelo specifične. Vprašanje pa je, ali so te kompetence tako specifične, da bi lahko enkrat govorili o subprofesiji v policijski organizaciji, s prilagojenim in specifičnim programom usposabljanja. Profesionalizacija policijskih šefov je smiselna, saj morajo vodje prenašati znanja na vodje policijskih okolišev in ostale zaposlene. Habulin je spomnil na združenje policijskih šefov, katerega namen je medsebojno povezovanje in spodbujanje, kakor tudi sodelovanje pri raziskavah in ocenah stanja. Trenutno združenje deluje v smeri profesionalizacije pri vodenju v policijskih vrstah. Namestnica generalnega direktorja je opisala program usposabljanja policijskih vodij v Policijski akademiji, ki je sestavljen iz sedmih modulov (komunikacijske veščine, reševanje konfliktov, delovno-pravno področje, vodenje ipd.) in je namenjen vsem trem vodstvenim ravnem. Veliko informacij in znanja pri tem usposabljanju črpajo iz CEPOL-a. Udeležba na programu je obvezna za zasedbo vodstvenega položaja, s čimer se zagotovi, da položaje prevzemajo kompetentne osebe. V tej razpravi je Ogulin izpostavil še vlogo akademskega okolja. Fakulteta za varnostne vede je npr. v preteklosti že pomagala pri postopkih usposabljanja in izobraževanja obstoječih vodstvenih kadrov, ki takšnih tečajev in programov v preteklosti niso obiskovali.

3 RAZVOJNI NAČRTI

Razprava na okrogli mizi se je nazadnje navezala še na vprašanje razvoja kariere v slovenski policiji. Ogulin je pojasnil, da je trenutna situacija zelo neugodna in destimulativna za zaposlene, se pa pripravlja nov sistem. Težava je predvsem v preveliki količini različnih delovnih mest, sistematizacija pa je posledično preveč razdrobljena in neurejena. Delovna mesta in zaposlitvene nivoje je treba poenostaviti, sistem mora biti jasen, ljudem pa je treba zagotoviti boljše možnosti napredovanja. Zavzeti se je treba tudi za boljše možnosti izobraževanja, predvsem na lokalnem nivoju.

Dr. Lobnikar je razpravo obrnil v smer aktualne problematike neenotnega vodenja. Univerzalna načela učinkovitega vodenja namreč narekujejo, da mora biti delegiranje enotno in izvirati iz enega samega mesta; trenutno pa v policijski organizaciji opažamo več virov vodenja – od policijskih šefov do politike in policijskih sindikatov. To posledično vpliva na legitimnost vodij in kaže na neprimerno vmešavanje tretjih akterjev v delo najpomembnejše varnostne organizacije. Namestnica generalnega direktorja se je z ugotovitvijo Lobnikarja strinjala in pojasnila, da si vodstvo zelo močno prizadeva razumeti in zastopati interese policistov, vendar je treba preprečiti rušenje dela, ki prihaja s strani tretjih akterjev. Posegov v vodenje policije, ki bi vplivali na stanje varnosti, policija in njeno vodstvo ne smeta in ne bosta dopustila. Z reakcijo na nedavne dogodke, povezane z delom policijskega sindikata, je bilo podano jasno stališče, da je glavni vodja policije izključno generalni direktor.

Habulin je potrdil, da je policijska stavka, ki je potekala pod vodstvom sindikata, povzročila veliko težav pri opravljanju obligatornega dela in prav tako vplivala na avtoriteto legitimnih vodij. V tej stavki je krožilo veliko napačnih informacij o tem, kakšne so pravice in naloge policistov med stavko, namen pa je

bil zgolj v izkazovanju moči sindikata. Veliko policistov je raje sledilo navodilom sindikata kot svojih formalnih vodij. Posledice so bile zelo negativne, sploh za državljane. Policisti so npr. za določene prekrške ljudem izrekali zgolj opozorila, po koncu stavke pa jih za enaka dejanja kaznovali. Takšen način izvajanja nalog med ljudmi povsem razumljivo ustvari zmedo in nezaupanje.

Ogulin je pritrdil mnenju Habulina, še posebej nerazumljivo pa se mu zdi prepričanje policistov, da stavka v obliki nekaznovanja ljudi škoduje državi in da se ji na ta način odreka finančni priliv preko glob. Ljudje namreč »privarčevani denar« zapravijo drugače in preko davkov vseeno prispevajo v blagajno. Ne glede na zmedo, ki je nastala v času stavke, je policija po njegovem mnenju dobro opravila svoje delo, sploh z vidika obvladovanja migracij. Glavni razlog pa je v tem, da je večini vodij uspelo ohraniti trezno glavo in razumsko razmišljanje. Ocenil je, da je bilo na letni ravni delo dobro opravljeno, razen na področju prometne varnosti. Tu je bila policija žal neučinkovita.

Namestnica generalnega direktorja je razpravo zaključila s priznanjem, da se je policija v tej stavki naučila pomembno lekcijo glede etike, integritete in spoštovanja. V tem času, v kombinaciji z migrantsko krizo, je bilo veliko pritiskov na policijo, dogajali so se tudi poskusi razdelitve – ustvarjanja sporov med nivoji. Kljub nekaterim prepričanjem, da ima lokalna raven največ moči in da sta regionalni in nacionalni nivo z vidika moči zanemarljiva, je policija še vedno povezana trinivojska struktura. Pokazalo se je, da imata preostala dva nivoja prav tako zelo velik vpliv. Na vseh treh nivojih delujejo uspešni vodje, vsi deli so tudi dovolj dobro usklajeni, da lahko ohranjajo jasno ter enotno linijo poveljevanja.

Kaja Prislan, Sara Kandolf

Državna regulativa v panogi detektivske dejavnosti: poročilo o okrogli mizi

V okviru 17. konference Dnevi varstvoslovja je Detektivska zbornica Republike Slovenije 8. 6. 2016 v Kranjski Gori organizirala okroglo mizo z naslovom »Državna regulativa v panogi detektivske dejavnosti«. Okroglo mizo sta moderirala Dušan Poslek in Žiga Primc, zataknilo pa se je pri razpravljavcih. Tako sta se vabilu Detektivske zbornice RS odzvala le njen predsednik Janko Trivunovič in dekan Fakultete za varnostne vede dr. Andrej Sotlar, žal pa so se opravičili predstavniki državnih organov, ki imajo pomembno regulatorno in nadzorstveno vlogo na področju detektivske dejavnosti od Ministrstva za notranje zadeve in Inšpektorata Republike Slovenije za notranje zadeve do Informacijske pooblaščenke in Ministrstva za javno upravo. Kakršnikoli so že bili razlogi za odsotnost predstavnikov države, je to pustilo grenak priokus med udeleženci okrogle mize, še posebej pa med detektivi, ki čutijo in opozarjajo, da v njihovi branži ni vse tako, kot bi lahko in moralo biti.

Namen okrogle mize je bil, da bi predstavniki državnih organov, detektivi in strokovnjaki javno spregovorili o odprtih vprašanjih, ki se dotikajo detektivske dejavnosti, saj se med detektivi vse bolj razrašča prepričanje, da razmere, ki trenutno vladajo v dejavnosti, ki jim daje kruh, počasi, a zanesljivo vodijo vsaj v slabšo kvaliteto, če ne celo v propad detektivske dejavnosti, pa čeprav je ta regulirana že več kot dve desetletji.

Moderator Dušan Poslek, ki je odprl okroglo mizo, je uvodoma povedal, da je detektivska dejavnost zbiranje, obdelava, posredovanje podatkov in informacij ter svetovanje na področju preprečevanja kaznivih ravnanj, ki ga za naročnikove potrebe opravlja detektiv, ki ima izdano licenco in izpolnjuje pogoje v skladu z Zakonom o detektivski dejavnosti (ZDD-1), ki je stopil v veljavo leta 2011 in je po mnenju detektivov in strokovnjakov dokaj zgledno uredil detektivsko delo, delovna področja in upravičenja, ki jih smejo uporabljati v detektivski dejavnosti.

Kot je dejal Dušan Poslek, do objave sodbe Upravnega sodišča leta 2013 večjih anomalij na področju detektivske dejavnosti detektivi niso opazili. V sodbi je med drugim zapisano, da določba ZDD-1, ki določa, da lahko določeno dejavnost opravlja detektiv, še ne pomeni, da tega ne sme opravljati nihče drug. Od citirane sodbe dalje pa se anomalije kažejo predvsem v poizkusih prevzemanja detektivskih storitev, navedenih v 26. členu ZDD-1, s strani pravnih in fizičnih oseb, ki ne izpolnjujejo pogojev, predpisanih v omenjenem zakonu. Pri tem se pravne osebe izgovarjajo, da pri opravljanju nalog iz 26. člena ne uporabljajo upravičenj iz 27. člena ZDD-1.

Sodba sama po sebi še ne bi bila tako problematična, če ji ne bi sledila različna mnenja državnih organov. V mnenju Ministrstva za notranje zadeve (v nadaljevanju MNZ) iz leta 2014 je med drugim zapisano, da je detektivska dejavnost vse, kar je v 26. členu navedeno kot detektivovo delovno področje, če

se z njo ukvarja detektiv. Vendar to ne pomeni, da te dejavnosti ne sme opravljati nihče drug. To pa je bistvo celotnega problema in zato je bila okrogla miza tudi organizirana.

V letu 2004 je Služba za zasebno varovanje in detektivsko dejavnost Ministrstva za notranje zadeve izdala mnenje, da gre tudi pri laični kontroli bolniške odsotnosti za poizvedovalno dejavnost. Neposredno izvajanje te dejavnosti pomeni poseg v posameznikovo zasebnost, ki je ustavno varovana pravica. Nadalje je bilo v mnenju MNZ zapisano, da gre za poizvedovalno dejavnost in da gre pri uporabi zbranih podatkov lahko za kršitev človekovega dostojanstva. Leta 2007 je Urad informacijskega pooblaščenca izdal dve mnenji. Zapisal je, da lahko kontrolo bolniške odsotnosti, kjer gre za opravilo obdelave osebnih podatkov, izvajajo le detektivi oziroma detektivske družbe in da gre pri kontroli za opravljanje dejavnosti, ki jo ureja Zakon o detektivski dejavnosti. Potem pa je prišla omenjena sodba Upravnega sodišča iz leta 2013, ki je vse postavila na glavo. Še istega leta je Urad informacijskega pooblaščenca izdal drugo mnenje, povsem nasprotno tistemu iz leta 2007. V mnenju je zapisal, da lahko kontrolo bolniške odsotnosti med drugim izvaja tako imenovani pogodbeni obdelovalec osebnih podatkov, ki je lahko katerakoli fizična ali pravna oseba, ki je usposobljena za opravljanje takšne dejavnosti, pri čemer ni pojasnjeno, kakšne pogoje mora izpolnjevati. Marca leta 2016 je informacijski pooblaščenec še enkrat posredno potrdil temu mnenju, ob tem pa po mnenju detektivov že nakazal smer, da morajo detektivi za izvajanje detektivske dejavnosti izpolnjevati strožje zahteve kot druge fizične ali pravne osebe, ki izvajajo dela iz njihove dejavnosti. Smiselno se je vprašati, ali je dopustno širjenje različnih del na druge subjekte.

Direktorat za policijo in druge varnostne naloge Ministrstva za notranje zadeve je v marcu in aprilu 2016 izdal dve mnenji, v katerih je dejansko prepisal omenjeno sodbo Upravnega sodišča. Med drugim je zapisal, da določba, da lahko detektiv opravlja neko dejavnost, še ne pomeni, da je ne sme opravljati nihče drug. Direktorat je prišel v kontradiktornost svojih lastnih stališč, saj je zapisal, da Zakon o detektivski dejavnosti ne daje detektivom izključne pravice, da lahko samo oni in na način, kot je zapisano v ZDD-1, opravljajo dela iz 26. člena, če so opredeljena v drugih predpisih. Kot je dejal Dušan Poslek, se detektivi sprašujejo, v katerih drugih predpisih je detektivska dejavnost še urejena. Ni namreč jasnega odgovora, kdo in na kakšen način še sme zbirati informacije na enak način kot detektivi.

26. člen ZDD-1 ureja, kaj smejo detektivi početi, 27. člen pa jasno določa njihova upravičenja, med drugim tudi, ko zbirajo podatke od oseb. Tega naj ne bi počel nihče drug. S takšnim mnenjem pa je Direktorat za policijo in druge varnostne naloge MNZ upravičenja detektivom omogočil tudi vsem ostalim osebam, ki ne izpolnjujejo pogojev po ZDD-1, s katerimi lahko posegajo tudi v človekove pravice in zasebnost. Direktorat je to pravico podelil potencialno tudi tistim, ki so bili kaznovani, ki niso bili varnostno preverjeni in ki imajo varnostne zadržke, saj ne potrebujejo nobenih tovrstnih dokazil.

Moderator Žiga Primc je razložil, da bo drugi del okrogle mize oziroma druga tematika delo detektivov za državne organe. V Zakonu o javnih uslužbencih je v 33.a členu namreč določeno, da ko predstojnik organa ugotovi oziroma oceni, da

zaposleni zlorablja bolniško odsotnost ali goljufa pri potnih stroških oziroma pri povračilu potnih stroškov na poti na delo ali z dela, lahko pooblasti enega ali več javnih uslužbencev, ali tretjo osebo ali detektiva, da preveri zgoraj opisano zlorabo oziroma goljufijo. Obenem pa je v 4. odstavku tega istega člena določeno, da je pred pričetkom nadzora treba tega uslužbenca opozoriti, da obstaja sum za njegovo kršitev. S tem členom, ko uslužbenca opozorimo, izničimo kakršnokoli možnost za uspešen nadzor oziroma za ugotovitev nepravilnosti. Vsi v detektivski stroki se sprašujejo, zakaj je ta člen sploh napisan v zakonu? A odgovora od predstavnikov Ministrstva za notranje zadeve še niso dobili.

V Detektivski zbornici RS se sprašujejo tudi, zakaj državni organi ne najemajo detektivov pri ugotavljanju drugih disciplinskih kršitev, kot so na primer alkoholiziranost na delovnem mestu, nelojalna konkurenca in druge kršitve, ki pa jih je z zakonom mogoče preiskovati brez predhodnega opozorila zaposlenemu. Na ta način vrtci, šole, zdravstvene ustanove in druge javne ustanove ne morejo kvalitetno nadzorovati zaposlenih z ozirom na domnevne kršitve, kar pa je v javnem interesu, saj so vsi posredni ali neposredni proračunski uporabniki. Detektivi si torej želijo odgovor, zakaj državni organi in ustanove njihovih storitev ne naročajo, saj bi s tem prihranili ogromno davkoplačevalskega denarja. Zavedati se moramo, da je javnih uslužbencev okoli 160.000, kar predstavlja kar velik odstotek od 800.000 delovno aktivnega prebivalstva.

Nastale razmere postavljajo pred detektive predvsem dva problema/izziva. Po eni strani jih moti nekritično in parcialno povzemanje sodbe Upravnega sodišča, kot pač nekemu državnemu organu v nekem trenutku najbolj ustreza, po drugi strani pa v tem vidijo ustvarjanje možnosti za razcvet nelojalne konkurence, ki za svoje delo ne potrebuje izpolnjevanja strogih pogojev za zbiranje informacij oziroma jih elegantno zaobide.

Vprašanje upravičenosti sodbe, na katero se sklicuje večina državnih organov, je tudi v tem, da ni preizkušena na drugi stopnji, hkrati pa se že ustvarja precedenčno razmišljanje, če že ne pravo iz ene same odločbe sodišča.

Dr. Sotlar je v svojem razmišljanju na začetku izpostavil, da je imel že pri sprejemanju trenutno veljavnega zakona določene pomisleke, ki so se nanašali na ureditev osebne zaznave in pa na težnjo države, da v zakon zapišemo vsako podrobnost, predvsem ko je šlo za področje zbiranja informacij. Ker je bil v sodbi Upravnega sodišča izpostavljen primer proti prislušnega pregleda, se je dr. Sotlar vprašal, ali so vsa področja v 26. členu ZDD-1 za detektive res ključnega pomena in ali ne bi bilo bolje ta področja na novo definirati in natančno določiti, katera dela smejo izvajati samo detektivi, tista manj pomembna in enostavnejša, kjer ne prihaja do poseganja v zasebnost in druge človekove pravice in podobno, pa prepustiti tudi drugim. Tudi g. Trivunovič je dejal, da je težko govoriti zgolj o eni sodbi, ki se s strani različnih državnih organov različno tolmači kot najpomembnejša zadeva detektivske dejavnosti, seveda pa ni nepomembna v smislu trenutnega dela in delovanja detektivov. Poudaril je, da se mu zdi razlikovanje zaposlenih glede na to, ali so javni uslužbenci ali uslužbenci v zasebnem sektorju glede zlorab bolniške odsotnosti in goljufanja pri potnih stroških, nerazumljivo in najmanj neutemeljeno.

Dr. Sotlar je dejal, da so tudi zelo visoki državni uradniki goljufali s potnimi stroški, torej jim je verjetno celo ustrezalo, če so bili sindikati glavni pobudniki takratnih pritiskov, da čim bolj otežijo možnost zbiranja informacij o tem, če in kdo krade državi ali ne. V resnici pa krademo sami sebi. Zanj je to škandal in če obstaja tudi diskrepanca glede obveznosti opozarjanja javnega uslužbenca glede suma goljufanja pri potnih stroških in pri bolniški odsotnosti, se človek sprašuje, kje je tukaj logika – če goljufaš, goljufaš, in ni pomembno koga in ali gre pri tem za stroške za prihod na delo ali bolniška odsotnost – vse se na koncu plačuje iz državnega proračuna. Dr. Sotlar zato detektive na tej točki popolnoma podpira.

Proti koncu okrogle mize sta se izpostavili še dve temi. Eno je odprl dr. Sotlar z vprašanjem, kako naj bodo področja zbiranja informacij detektivov zapisana v zakonu – kot vse, kar ni izrecno prepovedano ali kot samo tisto, kar je izrecno dovoljeno (kot to velja za državne organe). Oba pristopa imata svoje prednosti in slabosti, kajti predstavljajo na eni strani možnost zapiranja tržišča, po drugi strani pa večje tržišče in seveda tudi več konkurence.

Iz publike se je oglasil tudi dr. Miha Dvojmoč, ki predvsem razmišlja o nadzoru nad delom detektivov, kajti iz statističnih podatkov Inšpektorata RS za notranje zadeve zaznamo porast števila opravljenih inšpekcijskih nadzorov nad detektivi. Toda kje? Pri tistih, ki so to dejavnost registrirali in ki delajo. Enako velja na zasebnovarnostnem področju. Regulator je le en dejavnik, nadzornik je drug dejavnik. Če povlečemo vzporednico z zasebnim varovanjem, dobimo odgovor, ki je ravno tako problematičen, saj inšpektorat dela nekaj, regulator pa identične določbe zakonodaje tolmači po svoje in v duhu njihovega sprejemanja. Kaj je regulator rekel/razmišljal oziroma je v duhu priprave zakonodaje, inšpektorjev na terenu ne zanima, vsaj tako direktno iz njihovih ust. Zato tudi nekateri inšpektorji po Zakonu o inšpekcijskem nadzoru opravljajo inšpekcijski nadzor, kot jim paše, in tu manjka povezava inšpektorata z zbornico, da bi tudi na predlog zbornice inšpektorat opravil nadzor nad znanimi ali pa znanimi potencialnimi kršitelji ZDD. Mogoče bi morali razmisliti tudi v tej smeri. Z dr. Dvojmočem so se strinjali tudi nekateri drugi detektivi iz publike, ki so dodali še nekaj primerov izvajanja nadzora.

G. Poslek je povedal, da je težava v tem, kako Inšpektorat ta nadzor izvaja. Pridejo in vprašajo, ali se vi ukvarjate z detektivsko dejavnostjo. In če rečejo ne, potem niso v prekršku. G. Poslek je povedal, da je na inšpektorat posredoval seznam oseb, ki imajo registrirano detektivsko dejavnost, potem pa niso naredili terenskih postopkov, temveč so le pisno povprašali, ali opravljajo detektivsko dejavnost. Normalno, da so vsi rekli, da ne. Hkrati je g. Poslek tudi povedal, da se mu inšpektorat zdi brezzobi tiger, ker je veliko odločb predvsem proti »znanim« osebam odpravljenih na drugi stopnji, kot je na primer delovanje podjetja Draga Kosa za NLB.

G. Pečoler je povedal, da je podal prijavo zoper neko organizacijo. Čez 3 mesece je od inšpektorata dobil odgovor, da so jih povprašali in da ne delajo te dejavnosti. Super, to je res enkraten nadzor, saj je vse, kar naredijo, le to, da povprašajo.

Dr. Sotlar je povzel, da je zgrožen nad tem, kar posluša glede nadzora. Dejal je, da je sicer težko razpravljati o tem, ker predstavniki Inšpektorata RS za notranje

zadeve niso prisotni, vendar bi bilo prav zato prav, da bi prišli in iz prve roke slišali, kaj imajo na to temo povedati detektivi.

Kljub temu, da se predstavniki državnih organov niso udeležili, je bila okrogla miza zanimiva in polemična, predvsem pa je ponudila odkrito razpravo o trenutnem stanju na področju detektivske dejavnosti v Sloveniji, na katerega hote ali nehote v veliki meri vplivajo odločitve državnih organov.

Miha Dvojmoč

Mariborske vstaje – retrospektiva policijskih, tožilskih in sodnih postopkov zoper udeležence protestov: poročilo o okrogli mizi

17. dnevi varstvoslovja so ob koncu postregli z izjemno zanimivo in polemično okroglo mizo, ki je bila namenjena strokovni razpravi o dogajanju na tako imenovanih mariborskih vstajah leta 2012. V razpravi, ki se je osredotočila na uradne postopke zoper nekatere udeležence protestov, so sodelovali Vesna Lovrec, novinarka časnika Večer in podiplomska študentka na Fakulteti za varnostne vede, Jure Šega, odvetnik iz Maribora, in Zoran Cunk, višji kriminalistični inšpektor, zaposlen na Policijski upravi Maribor. Vsi trije sodelujoči so bili prisotni na t. i. tretji mariborski vstaji, prva dva kot udeleženca protestov, medtem ko je imel tretji pomembno vlogo pri opravljanju policijskih nalog in izvajanju pooblastil, bil pa je tudi priča tožilstva v sodnih postopkih zoper nekatere udeležence protestov. Okroglo mizo je povezoval dr. Benjamin Flander s Fakultete za varnostne vede Univerze v Mariboru. Organizator je k razpravi povabil tudi predstavnika državnega tožilstva, a so z Okrožnega tožilstva v Mariboru sporočili, da kot stranka nastopajo v sodnih postopkih v zvezi z dogodki v Mariboru, med katerimi nekateri še niso zaključeni, in da zato ne morejo in ne želijo javno izražati stališč v tej zadevi.

Moderator je v provokativnem uvodu v razpravo v šali »zamrznil« svoj položaj vodje programsko-organizacijskega odbora Dnevov varstvoslovja in spomnil na dogodke ob koncu leta 2012, ko se je v večjih slovenskih mestih zvrstilo več protestnih shodov. Za razliko od javnih zbiranj, o katerih so kolegi govorili na plenarni okrogli mizi dan poprej, na teh javnih zbiranjih ljudje – tako moderator – »niso prišli gledat, kako skače Peter Prevc, temveč so prišli z namenom, da bi izrazili nezadovoljstvo nad stanjem v slovenski politiki na državni in lokalni ravni«. Ta javna zbiranja so se od tistih, o katerih je bilo govora na začetku konference, po moderatorjevem mnenju razlikovala tudi po tem, da »so nekateri udeleženci poleg zalog alkohola s seboj, kot se je izkazalo, prinesli tudi zaloge granitnih kock« in ne nazadnje po tem, da »ta javna zbiranja večinoma niso bila prijavljena skladno z Zakonom o javnih zbiranjih«. Posebej je izpostavil shode 21. 11., 26. 11. in 3. 12. 2012, ki so bili *post festum* poimenovani »mariborske vstaje«. Na teh treh shodih je prišlo do hujših kršitev javnega reda in miru in do uporabe policijskih pooblastil zoper večje število občanov, med drugim do uporabe telesne sile, palice, solzivca in konjenice, na shodih 26. 11. in 3. 12. pa tudi do množičnih pridržanj. Moderator je uvod v razpravo sklenil z ugotovitvijo, da so dogodki v Mariboru naleteli na buren odziv v medijih, javnosti in politiki in da so bili po

aretacijah v večini primerov uvedeni uradni postopki, zoper nekatere udeležence protestov poleg policijskih tudi tožilski in sodni, pri čemer se nekateri do danes še niso končali oz. še niso pravnomočni.

Vesna Lovrec je v grobem povzela posledice protestov: na t. i. drugi mariborski vstaji (26. 11.) je bila prostost odvzeta 32 osebam, vložene so bile 4 kazenske ovadbe, zoper 3 osebe je tožilstvo vložilo obtožnico in vsi so bili obsojeni: dva pogojno na 7 oz. 8 mesečno zaporno kazen, eden, mladoletnik, pa na vzgojni ukrep. Tretje mariborske vstaje (3. 12.) naj bi se udeležilo med 10.000 in 15.000 ljudi. Prostost je bila odvzeta 119 osebam, vloženih pa je bilo 28 kazenskih ovadb. Policija in tožilstvo sta 16 osebam očitala kaznivo dejanje napada na uradno osebo, ko opravlja naloge varnosti po čl. 300 KZ-1, 12 osebam pa kaznivo dejanje sodelovanja v skupini, ki prepreči uradni osebi uradno dejanje po čl. 301 KZ-1. Policija je vseh 28 ovadenih oz. osumljenih privedla pred preiskovalnega sodnika, po sodnem pridržanju in zaslišanju je bil pripor odrejen za 25 oseb.

Lovrečeva je pojasnila, da sta zoper dvanajsterico in šestnajsterico potekali ločeni sojenji na mariborskem okrajnem in okrožnem sodišču. V izjemno turbulentnem sojenju dvanajsterici je sodišče sedem oseb spoznalo za krive in jim izreklo kazen 7 mesecev zapora. Višje sodišče v Mariboru je obsodilno sodbo spremenilo v pravnomočno oprostilno. Zoper to sodbo je Okrožno državno tožilstvo v Mariboru vložilo zahtevo za varstvo zakonitosti na Vrhovno sodišče RS, ki je ugotovilo, da je Višje sodišče pri odločanju kršilo Kazenski zakonik in Zakon o kazenskem postopku, ni pa Vrhovno sodišče pri tem poseglo v pravnomočno sodbo. Nastala je nenavadna situacija: obdolženci so bili pravnomočno oproščeni v sodnem postopku pred višjim sodiščem, za katerega je najvišje sodišče v državi ugotovilo, da je bil v njem kršen zakon. Lovrečeva je kot novinarka Večera dogajanje spremljala in o njem poročala. Ob rob povedanemu je pripomnila, da natančnejši vpogled v policijske, tožilske in še zlasti sodne postopke razkrije številna odstopanja od normalnih oz. običajnih praks v tovrstnih uradnih postopanjih.

Moderator Benjamin Flander je v nadaljevanju dejal, da je v nekaterih »nenormalnostih« uradnih postopkov moč prepoznati elemente kršitev ustavnih pravic. V sodnem postopku zoper dvanajsterico je sodišče med drugim sprejelo priznanje za KD, ki se obdolženemu sploh ni očitalo. O enem od obdolžencev oz. obtožencev v obrazložitvi obtožnega predloga ni bilo moč zaslediti niti stavka. Drug obdolženec je ves čas trdil, da je bil v času, ko naj bi storil kaznivo dejanje, v lokalu, kar je podkrepil s posnetkom varnostne kamere. Sodišče mu je prisluhnilo šele po devetih mesecih, pri čemer je večino tega časa preživel v priporu. Sodišče je tudi sicer vztrajno zavračalo dokazne predloge obrambe (npr. ogled amaterskih video posnetkov). Vesna Lovrec je pripomnila, da so bil krovni dokaz, s katerim je tožilstvo dokazovalo, da so obdolženi dejansko storili očitano kazniva dejanja, helikopterski posnetki, ki pa po njenem mnenju ne dokazujejo ničesar. S tem je sodišče po njenem mnenju dokazno breme preneslo na obrambo, ki je morala dokazovati nedolžnost svojih strank.

Tudi opravljanje policijskih nalog in izvajanje pooblastil na protestnih shodih je bilo po mnenju moderatorja daleč od idealnega, saj TV posnetki, zasebni video posnetki in izjave nekaterih udeležencev odpirajo vprašanje nesorazmerne uporabe prisilnih sredstev zoper nenasilne protestnike.

Zoran Cunk se z njim ni strinjal. Poudaril je, da je policija svoje naloge opravljala v izjemno zahtevnih okoliščinah, da se je na proteste skrbno pripravila ter da je svoja pooblastila izvajala zakonito in strokovno. Opozoril je, da smo bili na protestih 3. 12. 2012 priča nepredstavljivemu nasilju nekaterih protestnikov, ki se shoda očitno niso udeležili zato, da bi mirno protestirali. Policija je, kot je pojasnil Cunk, za vsak posamezen protestni shod pripravila načrt varovanja in le-tega nato tudi strokovno korektno izvrševala. 3. 12. 2012 je zaradi eskalacije nasilja razpustila shod, nasilne protestnike je pozvala, naj prenehajo z nasiljem in se razidejo ter jih opozorila, da bodo v nasprotnem primeru zoper njih uporabljena prisilna sredstva, kar se je na koncu tudi dejansko zgodilo. Cunk je posebej opozoril, da policija v ekstremnih okoliščinah, ki so nastale, prisilnih sredstev vključno s solzivcem v kritičnih trenutkih ni mogla dosledno uporabiti selektivno, saj v kaosu, ko so proti policistom letele granitne kocke in drugi nevarni predmeti, ni mogla dosledno razločiti med nasilneži in tistimi, ki so se ukazu naj se razidejo upirali pasivno. Kljub temu je izrazil prepričanje, da so pripadniki posebne policijske enote, uniformirani policisti in policisti v civilu svoje naloge opravili korektno, zakonito in strokovno. Zagotovil je, da je policija aretirala, pridržala in ovadila nasilneže in izgrednike, ne miroljubne udeležence protestov. Da so policisti v zahtevnih okoliščinah nasilnih protestov pooblastila izvajali zakonito, je – tako Cunk – potrdila tudi preiskava Komisije za razjasnitev okoliščin uporabe policijskih pooblastil, ki jo je imenoval direktor Policijske uprave Maribor.

Vesna Lovrec je menila, da je policija na protestih verjetno res ravnala formalno zakonito, da pa je ravno v tem težava, saj v kompleksni situaciji, ki je nastala v kritičnih trenutkih 3. 12. 2012, ne bi smela ravnati »by the book«, temveč bi morala upoštevati, da večina udeležencev mirno protestira, da so neizkušeni v prakticiranju te demokratične pravice in da so pravno neuki, tj. da ne poznajo zakonskih določil o posledicah razpusta shoda. Z njo se je strinjal tudi moderator, ki je ob tem opozoril, da v dani situaciji načelo sorazmernosti pomeni, da se proti mirnim protestnikom po razpustitvi shoda lahko uporabi le nujno potrebna sila za vzpostavitev javnega reda, in da neselektivna uporaba solzivca pomeni prekoračitev te nujno potrebne sile. Opozoril je tudi na koncept tako imenovane »dialoške policije« iz skandinavske teorije policijskega dela, iz katerega izhaja, da mora policija na demonstracijah slediti konceptu dialoga, torej komunicirati z množico in se ves čas prilagajati dogajanju v njej, saj je to podlaga za zmožnost razločevanja med tistimi posamezniki in skupinami, ki povzročajo nered ali so celo nasilni in tistimi, ki mirno protestirajo.

V razpravo se je nato vključil Jure Šega, ki je dejal, da lahko kot udeleženec protestov iz prve roke pove, da policija v določenih kritičnih trenutkih ni delovala pomirjevalno. Izpostavil je situacijo, ko so policisti izolirali večje število očitno nenasilnih udeležencev protestov in zoper njih uporabili solzivec. Glede množičnega prijetja na protestnem shodu 3. 12. 2012 je ocenil, da razplet sodnih postopkov, še posebej to, da je tožilstvo v številnih primerih odstopilo od pregona, postavlja načelno vprašanje zakonitosti prijetij. Opozoril je, da so številna prijetja temeljila na osebni prepoznavi obdolžencev, ki v sodnem postopku ni bila potrjena (s posnetkov je bilo mogoče prepoznati le enega od 28 kazensko ovadenih). Poleg tega policija s helikopterskimi in televizijskimi posnetki, ki so bili na sodišču predloženi kot dokaz, ob odločanju o pridržanjih sploh še ni razpolagala.

Šega je bil kritičen tudi do postopkov, v katerih je bil zoper 25 obdolžencev odrejen pripor. Odločbe so bile napisane po istem ključu, njihov skupni imenovalec pa je bila neprepričljiva pravna argumentacija obstoja pripornega razloga ponovitvene nevarnosti. Sodišče je slepo sledilo navedbam v uradnih zaznamkih, da so policisti prijeli tiste, ki so res storili očitana kazniva dejanja. Višje sodišče v Mariboru je o pritožbah zoper sklepe o priporu odločalo ves teden, čeprav je zakonski rok za odločitev 48 ur. Sodišče je v obrazložitvah sklepov med drugim navedlo tudi to, da ni imelo podlage za to, da bi podvomilo v resničnost izjav policistov, čeprav se je v zvezi z dogodki 3. 12. 2012 na zatožni klopi znašel policist, ki naj bi krivo pričal.

Mnenja razpravljavcev so se kresala tudi glede drugih vprašanj. V razpravo so se večkrat vključili strokovnjaki iz občinstva, ki so pomembno prispevali h kakovosti diskusije. Moderator je okroglo mizo sklenil z mislijo, da je bil namen omizja ponuditi odprto strokovno razpravo, ki bi prispevala k čim boljšemu razumevanju zahtevne problematike varovanja varnostno problematičnih javnih shodov ter nalog državnih organov in drugih subjektov v luči določb in načel, ki so zapisana v Ustavi Republike Slovenije. Iz dogodkov v Mariboru in dogajanja po njih smo se po moderatorjevem mnenju prakticiranja demokracije in vladavine prava v zaostrenih družbenih razmerah učili tako pristojni predstavniki državnih organov kot tudi državljani in občani.

Aleš Godec

Sarajevo – prestolnica raznolikosti in varnostnih posebnosti: strokovna ekskurzija magistrskih študentov Fakultete za varnostne vede v Sarajevo, maj 2016

Študenti 1. letnika magistrskega programa Fakultete za varnostne vede UM so v okviru predmeta Kriminologija in kriminalitetna politika od 11. do 13. maja 2016 v sklopu strokovne ekskurzije obiskali Sarajevo. Osemnajst rednih in izrednih študentov sta spremljala prof. dr. Gorazd Meško in doc. dr. Katja Eman, ki sta študentom podrobneje predstavila strokovne, zgodovinske in kulturne znamenitosti mesta ter opozorila na pomembnost kriminalitetne politike in kriminološke vidike zagotavljanja varnosti.

Sarajevo – mesto, kjer so ostanki preteklosti vidni še danes. Mesto, ki je z vidika varnostnih situacij prehodilo dolgo pot, doživelo preveč in preživelo, mesto, ki še vedno okreva. Svojo izkušnjo bosanske prestolnice smo začeli kje drugje kot na Baščaršiji. Zgodovinsko in kulturno središče mesta, kjer se kopičijo bazarji, srečujejo kulture, religije, ljudje različnih narodnosti. Čevabdžinica pri čevabdžinici, buregdžinica pri buregdžinici, ena verska zgradba pri drugi. Džamije, pravoslavne cerkve, sinagoga, frančiškanski samostan in še bi lahko našli kot dokaz verske dediščine. Pribežališče turistov, ki se izgubljajo med možnostmi, ki jih ponuja sarajevska kuhinja, in med trgovinami s spominki. Vse to predstavlja Baščaršija, kjer se čuti utrip celotnega mesta. Trk in sobivanje kultur sta značilna za kraj, poln spominkov, spominov in opominov. Kopica muzejev priča o zgodovini bosanskega Sarajeva, obiskovalec pa vpogled v težavno preteklost mesta dobi že na njegovih ulicah. Zaplate rdečega betona v razpokah, ki so jih povzročili minometni izstrelki, na mestih, kjer so umirali civilisti, enako na vojne čase še danes kažejo brazgotine na pročeljih stavb, stanovanjskih poslopij po celem mestu, podrti zidovi blokov, neobnovljene zgradbe.

Letos mineva dvajset let od konca obleganja Sarajeva, enega najdaljših obleganj v sodobni vojaški zgodovini, ki je bilo del vojne ob razglasitvi samostojnosti Bosne in Hercegovine (v nadaljevanju BiH). Danes nas spoznavanje Sarajeva ponovno popelje v preteklost, ko se ustavimo v muzeju Tunel, zdaj spominskem kompleksu, tedaj za mesto rešilni bilki, ki je bila speljana pod letališčem in linijo Združenih narodov z namenom dobavljanja surovin, nujnih za preživetje,

evakuacijo ranjencev ipd. Od t. i. tunela upanja, ki se je tedaj raztezal na skoraj 800 metrih dolžine, ob dobrem metru in pol višine ter metru širine, je danes za javnost odprt le del. Dovolj, da dobimo vpogled v obup(a)nost stanja, kompleksnost takratne varnostne situacije. Če ponazorimo s kritičnimi statističnimi podatki, ki pričajo o pomembnosti tega kraja za sarajevsko prebivalstvo pred dobrima dvema desetletjema – skozi tunel je bilo med Dobrinjo in Butmirjem prepeljanih več kot 19.000 ton hrane, skoraj 37 ton medicinskega in sanitetnega materiala zgolj za potrebe vojakov, več kot 549 ton vojaške opreme, 3.930 ton tehničnega materiala, 8.852 ton komercialnih dobrin in 4.516 ton drugih materialnih potrebščin (Tunel spasa, 2016).

Ozadje vojne nam predstavijo in v širši kontekst postavijo na sorodni fakulteti, ki jo kot eno od mnogih z varnostnega vidika nam zanimivih organizacij in institucij obiščemo naslednjo. Fakulteta za kriminalistiko, kriminologijo in varnostne študije je bila kot civilna institucija ustanovljena prav v času vojne, leta 1993, na srečanju pove naš sogovornik izr. prof. dr. Elmedin Muratbegović. Fakulteta prva postavi profesionalne standarde za zoperstavljanje protipravnim družbenim varnostnim tveganjem, kot del Univerze v Sarajevu pa je ta izobraževalna institucija bistveno prispevala k izobraževanju profesionalno usposobljenega kadra ljudi na področju uveljavljanja vladavine prava v BiH. Varnostne vede na tej fakulteti so dostopne študentom dodiplomskega in podiplomskega (magistrskega in doktorskega) študija, obenem si prizadevajo za razvoj pedagoškega in raziskovalnega dela, akademsko dejavnost strateško načrtujejo, ob tem pa sledijo načelom evropskega visokošolskega izobraževanja. V naslednjem študijskem letu fakulteta organizira mednarodno konferenco na temo terorizma, v letu 2018 pa gosti tudi konferenco evropskega združenja za kriminologijo (European Society of Criminology) (Fakultet za kriminalistiku, kriminologiju i sigurnostne studije, 2015).

O varnostnih ukrepih v ožji obliki, to je tistih, ki veljajo znotraj same zgradbe institucije, pa tudi tistih, postavljenih v širši kontekst, zvemo na predstavništvu Organizacije združenih narodov (OZN). Tam nam varnostno problematiko, s katero se danes soočajo zaposleni v predstavništvu OZN v Sarajevu in tisti na varnostnih misijah v tujini, predstavi Svetovalka za varnost OZN Sonja Jakič. Izvemo, kakšno vlogo ima organizacija na območju BiH danes. Plazovi, potepuški psi in aktualne migracije so le nekatere od aktualnih varnostnih situacij, s katerimi se soočata OZN in BiH, pri čemer v zvezi z migracijami Jakičeva pove, da je v primerjavi s Skandinavijo kot ciljnim območjem stanje v BiH kot tranzitni državi precej bolje organizirano. Razvojni program na področju prava in varnosti v BiH sicer nakazuje zadane številne cilje v regiji. Vključujejo vzpostavitev centralnega registra gibanja oborožitve, centralne baze podatkov za analize tveganj, varnostnega foruma skupaj z Republiko Srbijo, brezplačno pravno pomoč najbolj ogroženi in ranljivi populaciji, sistema strateške lokalne obnove v povezavi z naravnimi nesrečami in druga prizadevanja (UNDP in Bosnia and Herzegovina, 2012). Za Bosno sta sicer značilni tudi specifična politična raznolikost in kompleksnost.

Sledil je obisk Unicefove enote za zaščito otrok (Child Protection Unit), kjer sta predavatelja razložila ukrepe, ki jih Unicef danes uveljavlja na tem področju. Med drugim nudijo psihosocialno pomoč prizadetim v poplavah, zagotavljajo pa tudi podporo na področjih zdravja, prehrane in izobrazbe. Zavzemajo se za

zaščito otrok v sodnih postopkih – kot žrtev, prič ali storilcev protipravnih dejanj, ali kadar gre za vprašanje skrbništva. Poudarek dajejo na družbeno vključevanje in zaščito pred nasiljem, zavedajo pa se tudi pomena zgodnje razvojne faze in zagotavljanja optimalnih socialnih pogojev odraščanja (Unicef, n. d. A). Sarajevska izpostava Unicefa je začela delovati le tri mesece po začetku vojne v 90. letih prejšnjega stoletja. V povojnem obdobju se je Unicef soočal s posledicami, ki jih je vojna povzročila najbolj ranljivim skupinam prebivalstva (otrokom, mladim in ženskam), v zadnjih letih pa se premikajo od obnove k razvoju. Država kot taka je še vedno v tranziciji, zaradi česar je vzpostavljanje stabilnega in učinkovitega družbenega sistema zaščite otrok eden večjih izzivov, s katerimi se organizacija sooča (UNICEF, n. d. B).

Po obisku slovenskega veleposlaništva, ki v BiH deluje že od leta 1996 in kjer nas je toplo sprejel veleposlanik mag. Iztok Grmek, smo obiskali še oddelek za vojne zločine sodišča BiH. Sodnik pritožbenega oddelka Hilmo Vučinič je predstavil organizacijo in delovanje sodišča, katerega oddelka za vojne zločine ter organizirano kriminaliteto, gospodarsko kriminaliteto in korupcijo še danes obravnavata primere, ki so povezani z dogodki izpred dvajsetih let.

Obisk Sarajeva smo končali, kjer smo ga začeli – na Baščaršiji, ob pozivih k molitvi z bližnje mošeje, med spominki s podobami pokojnega Josipa Broza Tita in Vučka, maskote zimskih olimpijskih iger v Sarajevu leta 1984. Prepredeni z zgodovino mesta in njegovo sedanjostjo, opremljeni z novim, širšim znanjem o varnostnem dogajanju takrat in zdaj. Od vojnega dogajanja, s katerim je mesto zaznamovano še danes, obnove, v katero so bile vključene številne institucije in organizacije, do sodnega preganjanja, ki še vedno traja. Zahvaljujoč vsem, ki so si vzeli čas, da so skupini, ki ji je bila taka zgodovina prihranjena, predstavili raznolikost, multikulturnost in kompleksnost (varnostnega) okolja v BiH in Sarajevu, takrat in danes. Pa tudi jutri, saj poti, na kateri se je znašlo Sarajevo, še ni konec. Ostaja še veliko izzivov, tudi kriminoloških in varstvoslovnih.

Kristina Pavli

UPORABLJENI VIRI

Fakultet za kriminalistiku, kriminologiju i sigurnosne studije. (2015). *Osnivanje i uspostava Fakulteta*. Pridobljeno na http://www.fkn.unsa.ba/#!o-fakultetu/c24fs

Tunel spasa. (2016). *Tunel u brojevima*. Pridobljeno na http://tunelspasa.ba/#tunel-u-brojevima

UNDP in Bosnia and Herzegovina. (2012). *About UNDP in Bosnia and Herzegovina*. Pridobljeno na http://www.ba.undp.org/content/bosnia_and_herzegovina/en/home/operations/about_undp.html

Unicef. (n. d. A). *Bosnia and Herzegovina*. Pridobljeno na http://www.unicef.org/bih/

Unicef. (n. d. B). *Unicef in Bosnia and Herzegovina: History*. Pridobljeno na http://www.unicef.org/bih/overview_16393.html