

# Privatizacija obveščevalne dejavnosti v sodobnem varnostnem okolju

Jaroš Britovšek, Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana

Dejan Ulcej

Andrej Sotlar, Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana

## Povzetek

### Namen prispevka

Cilj prispevka je opozoriti na pojav privatizacije obveščevalne dejavnosti na varnostnem področju. Kateri so tisti ključni dejavniki, ki so pripeljali do privatizacije obveščevalne dejavnosti, kdo so tisti, ki izvajajo zasebno obveščevalno dejavnost in kako se obveščevalna dejavnost države razlikuje od obveščevalne dejavnosti zasebnih subjektov, so ključna vprašanja, s katerimi se bomo ukvarjali v tem prispevku. Analizirali bomo tudi pravno podlago za razvoj obveščevalne dejavnosti zasebnih subjektov v Republiki Sloveniji.

### Metodologija

Pregled temeljne literature o obveščevalni dejavnosti in pravnih aktov ter analiza primerov podjetij, za katere menimo, da opravljajo obveščevalno dejavnost.

### Ugotovitve

Obveščevalna dejavnost v zasebnem sektorju je realnost, dokaz za to pa so predvsem podjetja, ki nudijo storitve pridobivanja, analiziranja in posredovanja končnih obveščevalnih informacij, kar je glavno delo obveščevalnih služb. Pomembna razlika, ki loči državno in zasebno obveščevalno dejavnost leži v pooblastilih države, da lahko pri pridobivanju podatkov – ob določenih pogojih – posega v človekove pravice. Ustavno-pravni red Republike Slovenije omogoča razvoj zasebnih obveščevalnih podjetij in opravljanje obveščevalne dejavnosti.

### Praktična uporabnost

Prispevek je namenjen tako državnim kot tudi gospodarskim subjektom. Zavedanje o obstoju zasebne obveščevalne dejavnosti lahko bistveno vpliva na obnašanje države in na delo gospodarskih družb v konkurenčnem okolju. V prispevku so predstavljeni ključni pravni okvirji za opravljanje zasebne obveščevalne dejavnosti v Republiki Sloveniji.

### Izvirnost/pomembnost prispevka

S prispevkom želimo opozoriti na pojav obveščevalne dejavnosti zasebnih subjektov v svetu. Pridobivanje informacij s strani države lahko pomeni tudi poseg v človekove pravice, zato je pomemben nadzor nad takšno dejavnostjo. Pridobivanje informacij s strani zasebnih subjektov pa po drugi strani odpira vprašanje nadzora in etike.

**Ključne besede:** Obveščevalna dejavnost, privatizacija, liberalizem, informacijska revolucija, zasebna obveščevalna podjetja.

## 1 Uvod

Obveščevalna dejavnost je dolgo veljala za monopolno domeno države. Po hladni vojni, ko sta začela intenzivno odvijati procesa liberalizacije in globalizacije, so se v svetu začele pojavljati zasebne varnostne službe, ki so državni monopol varnosti počasi začele prevzemati nase. Podobno se je začelo dogajati tudi na obveščevalnem področju.

Pridobivanje in analiziranje informacij, pomembnih za odločanje, so ključni elementi obveščevalne dejavnosti. V svetu so se pojavila analitična podjetja, možganski trusti in druge organizacije, ki svojim uporabnikom nudijo informacije glede različnih področij. Poleg tega so se v večjih korporacijah začeli ustanavljati posebni oddelki, ki so zadolženi za zbiranje in analiziranje informacij pomembnih za poslovanje. Nekatera podjetja za zaščito svojih poslov najemajo tudi detektive, ki preverjajo in zbirajo informacije o različnih subjektih (konkurentih, partnerjih). Takšni in podobni indici nakazujejo na pojav privatizacije obveščevalne dejavnosti.

## 2 Teorija obveščevalne dejavnosti

Obveščevalna dejavnost je bila vedno zavita v meglo in prikrita očem akademske javnosti. Do pred nekaj let so bili edini, ki so posvečali večjo pozornost tej aktivnosti le novinarji in zgodovinarji. Problem pri razumevanju obveščevalne dejavnosti se kaže že pri samem pojmovanju. V celinski Evropi se pojem povezuje z obveščanjem, zbiranjem informacij. Tako imamo Slovenci pojem »obveščati«, pri Nemcih najdemo besedo »nachrichten«, ki bi v dobesednem prevodu pomenila novice. Rusi govorijo o »razvedki«, ki je najbližje slovenskemu pojmu poizvedovanje. Zelo razširjen je pojem »intelligence«, ki se uporablja v angleško govorečih državah. Jelen (2008: 193) ugotavlja, da se »intelligence« nanaša tako na obveščanje kot na inteligentnost, saj bi dobeseden prevod pomenil inteligenco. Po njegovem mnenju angleščina ponuja edinstveno rešitev, kjer bi vsakršen prevod bil omejevalen. Že Sherman Kent (1949), eden prvih teoretikov in tudi praktikov obveščevalne dejavnosti, je trdil, da pod pojmom »intelligence« razumemo tako znanje in tip organizacije, ki proizvaja to znanje, kot tudi dejavnost te organizacije. Iz tega lahko razumemo, kaj je imel v mislih Jelen, ko je govoril o omejenosti prevajanja. V naši terminologiji razumemo »intelligence« kot obveščevalno informacijo oziroma produkt, obveščevalno službo ter obveščevalno dejavnost (Britovšek, 2008).

V tem članku bomo uporabljali pojem obveščevalna dejavnost. Natančno definirati, kaj obveščevalna dejavnost je, je enako težko, kot najti teoretično podlago za to dejavnost. Nekateri avtorji grede celo tako daleč, kjer pravijo, da nobena od dozdajšnjih definicij obveščevalne dejavnosti ne vzdrži v praksi (Kahn, 2006). V slovenski literaturi najpogosteje najdemo definicijo, ki razume obveščevalno dejavnost v ožjem in v širšem smislu (Anžič, 1997; Purg, 1995; Šaponja, 1999). V ožjem smislu obveščevalna dejavnost zajema javno ali tajno pridobivanje podatkov, njihovo analizo ter interpretacijo. V širšem smislu pa poleg tega poznamo še tajne akcije in protiobveščevalno dejavnost (Purg, 1995). Pri tem je potrebno opozoriti, da tajne akcije in tajno pridobivanje podatkov ni eno in isto. Razlika je v tem, da tajne akcije dajo poudarek na tajnosti dejavnosti, pri tajnem pridobivanju podatkov pa gre za tajnost naročnika kot tudi samo dejavnost.

Podobno definicijo oziroma teoretično podlago predlaga Loch K. Johnson (2008: 33–53), ki pravi, da mora teorija obveščevalne dejavnosti zajemati temeljne dimenzije, ki jo sestavljajo. Sicer poudari, da izhaja iz ameriške izkušnje, vendar menimo, da dobro zajame bistvo obveščevalne dejavnosti. Kot prvo dimenzijo opiše obveščevalni cikel, ki predstavlja matrico komunikacije in delovanja med izdelovalci obveščevalnih produktov (obveščevalni agenti) in njihovih uporabnikov (načrtovalci in izvajalci politik). Prvi element obveščevalnega ciklusa je *načrtovanje in usmerjanje*, kjer se morajo upravljavci odločiti katere podatke ali informacije je potrebno zbrati. Ideal predstavljajo informacije, ki napovedujejo prihodnost. Naslednji korak je *pridobivanje podatkov*, kjer se na podlagi prejšnjih usmeritev lahko upravljavci odločijo, katero metodo bodo uporabili za pridobitev potrebnih podatkov. Ko smo pridobili podatke, sledi *procesiranje*, kajti pridobljeni podatki ali informacije so navadno v obliki, ki je težko berljiva za uporabnike. Ker pa sama informacija uporabniku ne pove nič, je potrebno s pomočjo specializiranih, dobro izurjenih poznavalcev določenega okolja ali področja, *analizirati in oceniti* informacije. Pridobljen, analiziran končni produkt nato *posredujemo* uporabnikom, kar je glavni namen cikla. Pri tem je potrebno upoštevati, da mora biti produkt relevanten in uporaben.

Johnson poleg obveščevalnega ciklusa poudarja tudi vlogo tajnih akcij, protiobveščevalne dejavnosti ter nadzora nad obveščevalno dejavnostjo. Tajne akcije razume kot agresivno vlogo obveščevalnih služb, ki želijo vplivati na določene dogodke. Pri tem je potrebno omeniti, da tajne akcije ne opravljajo

vse obveščevalne službe in kot take ne predstavljajo esencialen del obveščevalne dejavnosti. Po drugi strani pa je protiobveščevalna dejavnost pomemben element obveščevalne dejavnosti. Whitehead (2003) celo trdi, da je protiobveščevalna dejavnost »druga stran kovanca« obveščevalne dejavnosti. Če je naloga obveščevalne dejavnosti pridobivanje podatkov, je naloga protiobveščevalne dejavnosti zaščita podatkov. Protiobveščevalno dejavnost lahko delimo na pasivno in aktivno, kjer pasivna predstavlja klasične varnostne ukrepe za zaščito informacij kot so npr. ograja, računalniška zaščita in varnostna kultura, po drugi strani pa imamo aktivno protiobveščevalno dejavnost, ki je namenjena aktivnem odkrivanju, dezinformiranju in manipuliranju tuje obveščevalne dejavnosti (Britovšek, 2007). Zadnji element, nadzor nad obveščevalno dejavnostjo, je pomemben predvsem zaradi tega, ker imajo državne obveščevalne službe pooblastila, kot je npr. prisluškovanje, ki jim omogočajo poseganje v pravice človeka. Da ne bi prišlo do zlorab takšnih pooblastil je potrebno posebno pozornost posvečati nadzoru. Pred zlorabo pri pridobivanju podatkov pa ni ogrožena samo država. Kozmetično podjetje Proctor & Gamble je leta 2000 najelo podjetje za zbiranje informacij o konkurentih. Podjetje je za ta namen najelo več podizvajalcev, ki so brskali po smeteh podjetja Unilever ter z lažnim izdajanjem za tržne analitike pridobivali podatke o Unileverjevih proizvodih za nego las, cenovni politiki in datumih predstavitve izdelkov na trgu. Direktor Proctor & Gamble je zatrjeval, da je omenjene dejavnosti preklical takoj, ko je izvedel za njih. Podjetje Proctor & Gamble je priznalo takšno početje, vendar naj bi pridobivanje podatkov potekalo brez vednosti vodilnih v podjetju (Shah, 2001).

Obveščevalna dejavnost je potemtakem dejavnost obveščevalnega ciklusa, katerega glavni cilj je zadovoljiti uporabnika z relevantnimi in uporabnimi obveščevalnimi informacijami oziroma produkti. Proces obveščevalnega ciklusa hkrati spremlja protiobveščevalna dejavnost, katere glavni namen je zaščita lastnih informacij in procesa obveščevalnega ciklusa. V skladu z omenjeno definicijo lahko trdimo, da obveščevalna dejavnost ni samo domena države, temveč tudi drugih organizacij, ki izvajajo organizirano zbiranje in analiziranje informacij potrebnih za odločanje, hkrati pa skrbijo za zaščito lastnih informacij ter dejavnosti.

### 3 Spremembe varnostnega okolja

Ko govorimo o spremembi varnostnega okolja, imamo v mislih predvsem pojav novih oblik ogrožanja varnosti (vzrok) in odgovore nacionalno-varnostnih politik in mehanizmov na ta ogrožanja (posledica). Pri tem lahko razumemo »ogrožanje varnosti« kot *»kakršnokoli stanje, v katerem ni zagotovljen obstoj in uravnotežen razvoj nekega referenčnega objekta«* (Prezelj, 2002b: 623). Takšno pojmovanje ogrožanja varnosti je netradicionalistično, uveljavilo pa se je v obdobju po koncu hladne vojne. Glavni vzrok spremembe tiči v razpadu bipolarnega ideološkega sistema in v koncu konfrontacije Zahod–Vzhod, na podlagi katere so bili viri ogrožanja jasno definirani, določljivi in predvidljivi. Po letu 1991, konkretnije po političnem (dokončnem) razpustu Varšavskega pakta, teh virov ogrožanj ni bilo več, pojavile pa so se nove oblike ogrožanja varnosti, ki dejansko niso bile »nove«, saj so obstajale že prej, a jim nacionalno-varnostne politike niso posvečale toliko pozornosti. Za te »nove« vire ogrožanja so značilne večdimenzionalnost, transnacionalnost, nepredvidljivost in kompleksnost.<sup>1</sup> Robert D. Steele (2002a) na tem mestu govori o novi paradigmi ogrožanja. Ta zaobjema poleg »tradicionalističnih« nacionalnih držav tudi »netradicionalistične« nedejavne organizacije.<sup>2</sup> Pri konfrontaciji teh nedejavnih subjektov in držav je v ospredju princip asimetričnosti (nesorazmernosti), ko se v kontekstu bojevanja uporabljajo neprimerljive, neenake in različne metode, sredstva, koncepti in skupine ljudi za doseganje svojih ciljev (Steele, 2002a: IV; Svete, 2002: 22–25). Tovrstne oblike ogrožanja varnosti bi lahko poimenovali kot subjektne, saj se nanašajo delovanje subjekta. Po tej logiki potem lahko utemeljimo tudi objektne vire ogrožanja, ki imajo za referenco objekt. Vsebinsko so to predvsem pomanjkanje vodnih bogastev in energentov, pandemije (virusi), klimatske spremembe, ekološke katastrofe, itd. Takšna klasifikacija na objektne in subjektne vire

---

<sup>1</sup> O kompleksnosti groženj varnosti govorimo, ko stopnjevanje grožnje varnosti v eni dimenziji vpliva na stopnjevanje groženj varnosti iz drugih dimenzij, ne glede na nacionalne meje (Prezelj, 2002a: 428).

<sup>2</sup> Gre predvsem za kriminalne združbe, teroristične organizacije, versko-fundamentalistične skupnosti, militantne in uporniške grupacije, paradržavne organizacije, hekerje itd.

ogrožanja je lahko nekoliko pavšalna, saj so objektni viri ogrožanja običajno posledica subjektivnega delovanja, torej delovanja ljudi (npr. ekološka katastrofa je lahko posledica razlitja nafte iz tankerja, ki ga upravlja človek).

Poleg pojava oz. nastopa opisanih virov ogrožanja pa lahko navedemo še vsaj tri dejavnike, ki so vplivali na spremembe varnostnega okolja, in sicer: (1) prevlada svobodne trgovine in neoliberalističnih idej o globalnem gospodarstvu ter z njimi povezan prehod od geopolitike h geoekonomiji; (2) izgubljanje pomena države kot glavnega poroka varnosti posameznikom (državljanom) in civilnim organizacijam ter krepitev zasebnih organizacij; (3) informacijska revolucija in prost pretok informacij, idej, dela in kapitala, blaga, ljudi in nevarnosti. Vsi navedeni dejavniki, vključujoč dejavnik pojava novih virov ogrožanja, pomenijo generalizirane dejavnike sprememb varnostnega okolja, ki jih lahko poimenujemo *agensi sprememb varnostnega okolja*. Skupni vsebinski imenovalac vseh teh dejavnikov je odprtost (angl. openness) (Ulcej, 2008: 35).

Če govorimo o dejavnikih, ki so vplivali na spremembe varnostnega okolja, v katerega so s svojim delovanjem vpeti nacionalno-varnostni sistemi držav, potem lahko govorimo o teh dejavnikih tudi kot o agensih sprememb delovanja sodobnih nacionalno-varnostnih sistemov in posledično obveščevalne dejavnosti. Takšen deduktiven sklep se zdi na videz morda poenostavljen, vendar kot bomo videli v nadaljevanju, je glavni argument za privatizacijo obveščevalne dejavnosti prav v takšnem sklepu.

### 3.1 Neoliberalizem

Kadar govorimo neoliberalizmu največkrat mislimo na ekonomski liberalizem, kjer velja prepričanje, da se morajo države vzdržati poseganja v gospodarstvo ter prepustiti čim več svobode posameznikom, da delujejo na svobodnem trgu. Neoliberalizem ima svoje korenine v idejah Adama Smitha o »nevidni roki trga« in teoriji o razumevanju človeka v njegovih teorijah. Vendar se koncept neoliberalizma danes pojmuje kot novo paradigmo ekonomske teorije in politike – kot ideologijo modernega kapitalizma – in hkrati kot oživljanje ekonomske teorije Smitha iz 19. stoletja. Neoliberalizem je zamenjal koncept Keynesizma, katerega bistvo je bilo vmešavanje države na trgu, ki je bil na Zahodu glavni teoretični okvir ekonomije in politike med leti 1945 in 1970. Od takrat se verjame, da je Zahod v procesu neoliberalizma (Martinez, Garcia 2001).

Harvey (2005) pravi, da je neoliberalizem, kot prvo, teorija politične ekonomije, ki govori o tem, da je človeško blaginjo najlažje doseči z liberalizacijo posameznih podjetniških svoboščin in sposobnosti znotraj institucionalnega okvirja, ki ga karakterizirajo močne lastniške pravice, svoboden trg in svobodna trgovina. Vloga države je tako kreiranje in ohranjanje institucionalnega okvirja, ki omogoča takšno delovanje.

Martinezova in Garcia (2001) na kratko povzameta glavne točke neoliberalizma: (1) vladavina svobodnega trga; (2) zmanjševanje socialnih izdatkov; (3) deregulacija; (4) privatizacija; (5) zamenjava pojma »javnega dobrega« s pojmom »odgovornosti posameznika«. Pri tem bi posebej izpostavil proces privatizacije. Neoliberalni koncept podpira idejo o prodaji državnih podjetij, dobrin in storitev zasebnim investitorjem. V našem primeru gre za privatizacijo varnosti oziroma obveščevalne dejavnosti. Dodati moramo, da ne gre vedno za prodajo določenih storitev države, temveč za »outsourcing« ali demonopoliziranje nekaterih dejavnosti, kar pomeni, da lahko storitve opravljajo zasebniki namesto ali hkrati z državo.

### 3.2 Privatizacija varnosti

Kot že rečeno, država ni več glavni porok varnosti državljanom in njihovim organizacijam, ker ne more niti določati niti kvantificirati, koliko varnosti potrebuje posamezen državljan ali civilna organizacija, prav tako ne pozna njihovih potreb in želja po varnosti. Varnost si lahko v tem kontekstu razlagamo kot dobrino (storitev), po kateri se povprašuje. Potrebe po varnosti namreč naraščajo hitreje, kot jih država s svojim delovanjem dejansko lahko poteši oz. je obseg povpraševanja po varnosti večji kot obseg ponudbe varnosti s strani države (Bučar, 1997: 7). Več kot je bogastva na

svetu, večja je potreba po zavarovanju tega bogastva. Zaradi tega se na prostem trgu oblikujejo podjetja, ki storitve varnosti ponujajo za plačilo in s tem pokrivajo deficit državne ponudbe varnosti; imenujemo jih *zasebna varnostna podjetja* (ang. private security companies). Država se torej sooča z deetatizacijo in demonopolizacijo vloge države pri zagotavljanju varnosti, v te izpraznjene segmente ponudbe varnosti pa se vrvajo zasebni ponudniki varnosti. Takšno zmanjševanje vloge države pri financiranju, proizvodjanju ali distribuciji varnostnih storitev označujemo s sintagmo *privatizacija varnosti* (Ulcej, 2008: 23). Po mnenju Zalarja (1997: 41) moramo na privatizacijo varnosti gledati kot na povsem legitimno pravico in institucionalizirano možnost posameznika, da si s svojim delom prisvajajo dobrine zunanjega sveta. Ob tem se hitro pojavi vprašanje, ali je privatizacija varnosti potem res dobra rešitev za družbo? Odgovor je da in ne. Privatizacija tega področja prinaša več tržišča, bolj pestro in kakovostnejšo ponudbo varnostnih storitev, zmanjšuje javno porabo, zmanjša vmešavanje države in hitreje sledi potrebam državljanov. Po drugi strani pa – če citiramo Pečarja (1997: 15) – prinaša »*krizo zakonitosti, boj za obstanek, nelojalno konkurenco, vdiranje v zasebnost in kršitve človekovih pravic*«. Z ekonomskega vidika prinaša privatizacija varnosti več tržne učinkovitosti in manj družbene pravičnosti, kar je v tržnih gospodarstvih z nadvlado neoliberalizma povsem normalno.<sup>3</sup> Bistveno pri privatizaciji je – in mora ostati – to, da država dopušča možnosti za prosto oblikovanje trga varnostnih storitev, a hkrati obravnava varnost kot pravno kategorijo in s svojimi pravnimi inštrumenti zagotavlja nedotakljivost človekovih pravic.

### 3.3 Informacijska revolucija

Razvoj informacijsko-komunikacijske tehnologije (IKT) se je v zadnjih nekaj desetletjih sunkovito pospešil, čas med odkritjem in uporabo nove tehnologije pa se po Mooreovim zakonom skrajšuje. Napredek IKT pušča za sabo epohalne posledice, ki se kažejo predvsem v razvoju informacijsko-komunikacijskih kanalov, hitrem pretoku informacij po teh kanalih in premik k elektronskemu komuniciranju. Triglav (1996: 27–30) na tem mestu atraktivno govori o t.i. tehnoloških civilizacijah, po drugih strani pa ob tem »*revolucionarnem izrazoslovju*« opozarja na vladavino pravila nepredvidljivih posledic. Nepredvidljive posledice se kažejo v sprostitvi pretoka enormne količine informacij in vse večji dostopnosti do teh informacij vse širšim krogom ljudi. Dandanes smo že v fazi informacijske preobremenitve, s čimer je vse bolj vprašljiva tudi kredibilnost informacij. Trend informacijskega razvoja, ki je še posebej intenziven od sedemdesetih let prejšnjega stoletja, imenujemo informacijska revolucija. To pa ni le tehnološki trend, temveč tudi ekonomski in socialni. Peter Drucker (v Steele, 2002a: 31–32) o informacijski revoluciji pravi, da gre zdaj za revolucijo konceptov o pomenu in namenu informacij, medtem ko se »*tehnološki del*« odvija že več kot petdeset let.

Danes so informacije ključnega pomena za podjetje, državo, civilno organizacijo in posameznika. Informacije so vzvod delovanja, njihovo posedovanje pa pomeni moč – informacijsko moč. Same informacije kot take sicer še ne predstavljajo dejanske moči, če pa so povezane v znanje, ki ga posedujemo in ki si ga nekdo želi ali ga potrebuje, pa pomeni informacijsko moč; ta je ključna za odločanje in uspeh v kompleksnih okoljih (Svete, 2006: 106). Seveda pa imamo tukaj v mislih verodostojne informacije, torej tiste informacije, ki so bile pred »*spajanjem v znanje*« ločene od obilice nezanesljivih, neresničnih in pol- informacij.

Na področju obveščevalne dejavnosti dandanes poznamo (1) *javne informacije*, ki so prosto dostopne in predstavljajo 90 odstotkov vseh informacij v obveščevalni dejavnosti; (2) *sive informacije*, ki niso publicirane ali široko distribuirane, je pa dostop do njih legalen, pri čemer je treba vedeti le, da obstajajo in najti ustrezen komunikacijski kanal za njihovo pridobitev; te predstavljajo devet odstotkov vseh informacij v obveščevalni dejavnosti; (3) *tajne (črne) informacije*, ki se pridobivajo z vohunstvom in predstavljajo 0,9 odstotka vseh informacij v obveščevalni dejavnosti (Dedijer, 2005:

---

<sup>3</sup> Manj družbene pravičnosti je zato, ker vsakdo nima zmožnosti za nakup varnostnih storitev, zaradi česar je distribucija varnosti v družbi neenakomerna in skoncentrirana predvsem na bogatejše. S krepitvijo procesa privatizacije varnosti se premosorazmerno krepi tudi neenakomerna distribucija varnosti v prid bogatih.

128–129; Reed v Friedman, 2002: 17).<sup>4</sup> Iz tega vidika lahko rečemo, da sodobna obveščevalna dejavnost temelji na prosto dostopnih informacij oz. na t.i. odprtih virih (ang. open source), medtem ko tajne informacije predstavljajo le slab odstotek vseh informacij.<sup>5</sup> Informacije odprtih virov so večinoma ustvarjene za potrebe zasebnega sektorja, za objavami teh informacij in vzdrževanjem podatkovnih baz, v katerih se te informacije nahajajo, pa stoji zasebni kapital (podjetij, možganskih trustov). Dejavnost pridobivanja, analize in posredovanja obveščevalnih informacij, ki temeljijo na odprtih virih, imenujemo **obveščevalna dejavnost odprtih virov** (ang. open source intelligence).<sup>6</sup> To pa je tudi tisti del celotne obveščevalne dejavnosti, kjer zasebni sektor igra ključno vlogo, saj je povsem logično, da je tisti, ki financira izdelavo informacij, izdeluje informacije in distribuira te informacije, bolj učinkovit in uspešen kot tisti, ki se ukvarja zgolj s posameznimi fazami obveščevalne dejavnosti oz. se s tem sploh ne ukvarja. Takšno zmanjševanje vloge države pri financiranju, opravljanju in distribuciji obveščevalne dejavnosti na račun zasebnega sektorja poimenujemo **privatizacija obveščevalne dejavnosti** (Ulcej, 2008: 35).

#### 4 Primeri zasebnih obveščevalnih podjetij

Smith (2006) ugotavlja, da je bila rast obveščevalnih podjetij v zadnjem desetletju zelo visoka. Smith meni, da je glavni razlog v spoznanju podjetnikov, kar obveščevalne službe in politiki vedo že dalj časa – zbiranje relativno majhnih vendar pomembnih informacij lahko igra pomembno vlogo v procesu odločanja, kjer lahko spremeni potencialen neuspeh v uspeh. Dobre vladne odločitve lahko rešijo življenja, dobre poslovne odločitve pa lahko prihranijo milijone denarja in občutno povečajo dobiček. Ta podjetja aplicirajo obveščevalne metode v podjetjih, zbirajo informacije o posameznih tržiščih, o tveganjih – katere države so rizične, katere ne - ter seveda o konkurenci. Smith je naštel šest podjetij, ki opravljajo takšno dejavnost: Kroll, GPW, Aegis, Control Risk Group, Diligence in Hakluyt.

Prvo od velikih zasebnih obveščevalnih podjetij je podjetje *Kroll*, ki je bilo ustanovljeno leta 1972. Podjetje je od vsega začetka rekrutiralo nekdanje policiste, tožilce, obveščevalce, akademike, računovodje in novinarje. Kroll je bil omenjen v več aferah, kar je med drugim razlog, da so leta 2006 iz Iraka potegnili vso svoje varnostno osebje ter prodali varnostni oddelek. *GPW* je kratica za Grayson, Pender in Wordsworth, podjetje pa je bilo ustanovljeno s strani nekdanjih istoimenskih zaposlenih pri zasebni obveščevalni službi Kroll leta 2004. GPW je sicer manjše podjetje, vendar zatrjuje, da ima dobro in razširjeno mrežo operativcev po vsem svetu. *Aegis* družba je bila ustanovljena leta 2002 in je primarno zasebno varnostno podjetje, ki ga je ustanovil nekdanji pripadnik Kraljeve vojske Združenega Kraljestva. *Aegis* nudi tudi operativne obveščevalne naloge o določeni državi. Oddelek se ukvarja z geopolitično obveščevalno dejavnostjo, oceno ogrožanj in preiskovalne storitve. Vodi lastno bazo teroristov, ki jo dnevno posodablja. *Control Risk Group* je bilo eno prvih britanskih zasebnih obveščevalnih podjetij, ki je nastalo leta 1975, in je specializirano za analizo in oceno tveganj. Podjetje temelji na zbiranju in analizi podatkov iz javnih virov, kar lahko sicer nudi dobre strateške ocene, vendar ne nudi iste dodane vrednosti, ki jih ima pravočasna in relevantna informacija iz prve roke. Podjetje *Diligence* je bilo ustanovljeno leta 2000 s strani nekdanjih uslužbencev obveščevalnih služb (MI5, CIA, specialne sile Združenega Kraljestva). Poleg obveščevalnih storitev podjetjem nudi te storitve tudi tujim vladam. Čeprav je bilo ustanovljeno s strani nekdanjih uslužbencev, so kmalu začeli zaposlovati tudi pravnike, nekdanje policiste, bankirje, diplomate in celo raziskovalne novinarje. Vse z namenom, da zberejo čim več relevantnih informacij.

---

<sup>4</sup> Obstaja še četrti tip informacij. To so neobstoječe informacije, ki predstavljajo zgolj 0,1 odstotka vseh informacij v obveščevalni dejavnosti (Dedijer, 2005: 128–129).

<sup>5</sup> Ko govorimo o informacijah, imamo v mislih obveščevalne informacije, ki so obdelane in ovrednotene informacije in že namenjene za podporo pri odločanju (Shulsky v Steele, 1996: 221).

<sup>6</sup> Odprto obveščevalno dejavnost lahko definiramo kot organiziran proces, ki vključuje (1) iskanje, selekcioniranje in pridobivanje brezplačnih (ter kupovanje komercialnih) informacij iz raznolikih javno dostopnih virov, (2) preverjanje in verifikacijo, (3) procesiranje in analiziranje teh, (4) izdelavo končnih obveščevalnih informacij ter (5) njihovo pravočasno distribucijo določenemu občinstvu za posebne obveščevalne zahteve (Ulcej, 2008: 43).

Podjetje *Hakluyt* je bilo ustanovljeno leta 1995 s strani nekdanjih delavcev MI6 in je osredotočeno na pridobivanje visoko cenjenih komercialnih obveščevalnih informacij. Ime je dobilo po Richardu Hakluytu, geografu in kleriku iz 16. stoletja, ki je bil s strani Angležev poslan v Pariz, da bi zbiral informacije o Francozih in Špancih.

Poleg naštetih podjetij velja omeniti še podjetja kot so *Jane's Information Group*, *Stratfor*, in *Economist Intelligence Unit*. *Jane's Information Group* nudi svojim uporabnikom geopolitične ocene ogrožanj s strani terorizma in organizirane kriminalitete, kot tudi varnostne ocene zgradb, plinovodov ter pisarn na »občutljivih« območjih. *Stratfor* prav tako nudi geopolitične analize in ocene na področju varnosti. Po drugi strani nudi *Economist Intelligence Unit* večinoma gospodarske informacije in analize (Lewis, 2004).

Vsa našeta podjetja dokazujejo obstoj zasebnih obveščevalnih služb. Pri tem se porajajo pomembna vprašanja, kot je varovanje človekovih pravic, predvsem pa pravice do zasebnosti. V kolikor se bo opisan trend nadaljeval, bi lahko takšna podjetja občutno posegala v naše pravice. Obstajata dva odgovora na takšen problem, ali vrniti monopol obveščevalne dejavnosti nazaj državi ali poostri nadzor s strani države nad takšno dejavnostjo. Verjetno je prvi odgovor preveč konzervativen glede na razmere po hladni vojni, ki smo jih opisali.

## 5 Pravna osnova za zasebna obveščevalna podjetja v Republiki Sloveniji

Postavlja se vprašanje, ali imamo tudi v Sloveniji zasebna podjetja, ki se ukvarjajo z obveščevalno dejavnostjo? Če izhajamo iz koncepta zasebne obveščevalne organizacije, ki svoje delo opravlja za profit, potem je odgovor pritrdilen.<sup>7</sup> Profitne zasebne obveščevalne organizacije so večinoma registrirane kot podjetja, zato jih lahko poimenujemo kar *zasebna obveščevalna podjetja*.<sup>8</sup> V Sloveniji so taka podjetja inštituti (komercialni možganski trusti) in samozaposleni detektivi. V to skupino lahko štejemo tudi podjetja z internimi obveščevalnimi oddelki, ne glede na to, katero gospodarsko dejavnost opravljajo.<sup>9</sup>

Pravna podlaga za profitno obveščevalno dejavnost zasebnikov je utemeljena že v sami Ustavi Republike Slovenije, saj gre za (1) uresničevanje pravice do svobode dela (Ustava RS, 49. čl.) in (2) svobodne podjetniške pobude (Ustava RS, 74. čl.), ki je postala z odločbo Ustavnega sodišča z dne 9.6.1994 iztožljiva človekova pravica (Zalar, 1997: 46–47). »Obveščevalni podjetniki« morajo pri svojem delu poznati tako pravice kot tudi dolžnosti, ki izhajajo iz zakonodaje. Povedano drugače, vedeti morajo, kaj smejo in kaj ne. Glede osebnih podatkov in informacijske varnosti posameznika je poleg Ustave Republike Slovenije skorajda nujno poznati:

- Zakon o varstvu osebnih podatkov,
- Zakon o dostopu do informacij javnega značaja,
- Zakon o elektronskem poslovanju in elektronskem podpisu,
- Zakon o elektronskih komunikacijah,
- Splošni akt o razčlenjenem računu ter
- Kazenski zakonik Republike Slovenije (137., 138., 140, 143., 221., 237. in 306. člen).

<sup>7</sup> Koncept zasebne obveščevalne organizacije v opisanem kontekstu temelji na treh predpostavkah: (1) po Šaponji (1999: 24) so to obveščevalne organizacije v širšem smislu; (2) upoštevamo kriterij zasebnega lastništva; (3) te organizacije opravljajo obveščevalno dejavnost, temelječo na odprtih virih (izključujemo pridobivanje tajnih podatkov, torej pravico obveščevalni služb države) (Ulcej, 2008: 57).

<sup>8</sup> Zasebna obveščevalna podjetja so podjetja, ki se ukvarjajo s pridobivanjem in analizo podatkov in informacij iz javno dostopnih virov, nato pa končne obveščevalne informacije uporabljajo v komercialne namene. Lahko rečemo, da so to podjetja, ki se ukvarjajo z obveščevalno dejavnostjo odprtih virov za profit (Ulcej, 2008: 29–30).

<sup>9</sup> Po raziskavi, opravljeni s strani podjetja GfK Gral-Iteo leta 2003 v Sloveniji, ki je zajela 39 različnih podjetij, se je s poslovno in konkurenčno obveščevalno dejavnostjo ukvarjalo kar 60 odstotkov vseh podjetij z več kot 3,3 milijona evrov prihodka v letu 2003, 46 odstotkov podjetij s prihodkom v rangu od 830.000 evrov do 3,3 milijona evrov v letu 2003, ter 17 odstotkov podjetij z manj kot 830.000 evrov prihodka v letu 2003 (Vrenko Peruško, 2004).

Zasebna obveščevalna podjetja so pri pridobivanju podatkov in informacij omejena zgolj na odprte vire. Pridobivanje tajnih podatkov ali poslovnih skrivnosti je prepovedano in se sankcionira. Zakoni in členi zakonov, ki to področje urejajo in jih je smiselno poznati so:

- Zakon o gospodarskih družbah (39. in 40. člen),
- Zakon o tajnih podatkih,
- Zakon o industrijski lastnini (8. člen),
- Obligacijski zakonik (5. člen),
- Kazenski zakonik Republike Slovenije (142., 147.–149., 236., 238., 260., 287., 358. člen) ter
- Zakon o detektivski dejavnosti.

Navedena zakonodaja je le grob okvir za izvajanje obveščevalne dejavnosti zasebnega sektorja.<sup>10</sup> Kršitev kateregakoli od navedenih pravnih aktov ne pomeni le osnovo za sankcioniranje kršitelja, temveč tudi poseganje v človekove pravice, ki se obvarovane tudi z mednarodnimi konvencijami, ki jih je Republika Slovenija sprejela.

## 6 Zaključek

V zadnjih nekaj letih je potekala razprava o teoriji obveščevalne dejavnosti. Skupni konsenz med akademiki sicer še ni bil dosežen, vendar lahko po našem mnenju prepoznamo temeljne elemente, ki bi lahko predstavljali teoretično podlago obveščevalne dejavnosti. To zajema obveščevalni cikel, katerega cilj so relevantne in pravočasne informacije, ter protiobveščevalno dejavnost, ki ščiti dejavnost in informacije pred obveščevalnim ciklusom drugih subjektov.

Spremembe, kakršnim smo bili priča po koncu hladne vojne, so močno spremenile sodobno varnostno okolje. Vzpon netradicionalističnih virov ogrožanj je tako prisilil tvorce nacionalno-varnostnih sistemov k spremembi konceptov, ki so dominirali vse od konca druga svetovne vojne. S temi spremembami pa je bilo v zoperstavljanje grožnjam vneseno načelo asimetričnosti. Vzporedno z novo paradigmo ogrožanja sta k spremembam varnostnega okolja doprinesli še informacijska revolucija in zmaga neoliberalizma v svetu. Nekoč nedostopne informacije so čez noč postale dostopne, vsa ta tehnološko omogočena pretočnost pa je ob podpori globalizacije dala informacijam pomen in vrednost, ki jo s pridom izkoriščajo države, civilne organizacije in posamezniki. Neoliberalizem prav tako predstavlja pomembno teoretično podlago za spremembe varnostnega okolja in posledičen pojav privatizacije varnosti. Ena glavnih idej neoliberalizma je namreč manjšanje moči države in poudarjanje vloge in odgovornosti posameznika. Dejavnosti s področja varnosti, ki so bile v preteklosti monopol države, postajajo del zasebnega sektorja oz. del storitev na prostem trgu.

Na podlagi opisanih podjetij lahko ugotovimo, da se proces privatizacije odvija tudi na obveščevalnem področju, vendar ne gre toliko za predajo določene državne storitve zasebnem sektorju, kot za dodatno storitev, ki jo nudi zasebni sektor. Pri tem pa je potrebno ponovno opozoriti na možnosti kršenja človekovih pravic in nujnost urejanju tega pojava. V Sloveniji je zakonodaja na tem področju kar precizna, kar pa še ne pomeni, da je s tem onemogočeno obveščevalno delovanje zasebnikov. Bolj kot pravno ureditev pa Slovenija na področju zasebne obveščevalne dejavnosti potrebuje zavest, da je taka dejavnost povsem legitimna in nujna, predvsem pa, da je obveščevalna dejavnost zasebnih subjektov v državah Zahoda že nekaj časa realnost.

## 7 Literatura

- Anžič, A. (1997). Varnostni sistem Republike Slovenije. ČZ Uradni list Republike Slovenije. Ljubljana.
- Britovšek, J. (2007). Protiobveščevalna dejavnost v sodobni državi. Diplomsko delo. Ljubljana: Fakulteta za družbene vede.

---

<sup>10</sup> Podrobna analiza pravne podlage je predstavljena v Ulcej, 2008: 67–75.



- Britovšek, J. (2008). Možnosti proučevanja obveščevalne dejavnosti. Bled: Slovenski dnevi varstvoslovja. Dostopno na: <http://www.fvv.uni-lj.si/dv2008/zbornik/clanki/BritovsekJ.pdf> (25. maj 2009).
- Bučar, F. (1997). Varnost kot dobrina. V Zasebno varovanje in detektivska dejavnost: dileme in perspektive, ur. Andrej Anžič, 3–10. Ljubljana: Visoka policijsko-varnostna šola.
- Dedijer, S. (2005). Obveščevalna knjižnica v obveščevalnem živčnem sistemu Slovenije? Organizacija znanja 10 (3): 124–129.
- Friedman, R. S. (2002). Review Essay – Open Source Intelligence. V NATO Open Source Intelligence Reader, 17–23. Dostopno na: [http://www.oss.net/dynamaster/file\\_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf](http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf) (15. maj 2009).
- Harvey, D. (2005). A Brief History of Neoliberalism. Oxford: Oxford University Press.
- Jelen, L. (2008). Ekonomsko vohunstvo in upravljanja tveganj. V Podbregar, I. (ur.). Vohunska dejavnost in gospodarstvo. Ljubljana: Fakulteta za varnostne vede.
- Johnson K., L. (2009). Sketches for a theory of strategic intelligence. V Gill, P., Martin, S. (ur.). Intelligence Theory. New York: Routledge.
- Kahn, D. (2001). A Historical Theory of Intelligence. Intelligence and National Security 16(3). New York: Routledge.
- Kent, S. (1949). Strategic Intelligence for American World Policy. Princeton: Princeton University Press.
- Lewis, P. (2004). Companies Turn To Private Spies. Fortune. Dostopno na: [http://money.cnn.com/magazines/fortune/fortune\\_archive/2004/08/23/379380/index.htm](http://money.cnn.com/magazines/fortune/fortune_archive/2004/08/23/379380/index.htm) (26. maj 2009).
- Martinez, E., Garcia, A. (2001). What is »Neoliberalism«? A brief Definition. Dostopno na: <http://www.irtfcleveland.org/economicjustice/antiglobalization/WhatIsNeoLiberalism.pdf> (26. maj 2009).
- Pečar, J. (1997). Varnostnopolitični in nadzorstveni pogledi na zasebno varstvo. V Zasebno varovanje in detektivska dejavnost: dileme in perspektive, ur. Andrej Anžič, 11–22. Ljubljana: Visoka policijsko-varnostna šola.
- Prezelj, I. (2002a). Ogrožanje nacionalne varnosti Republike Slovenije in vključevanje v NATO. Teorija in praksa 39 (3): 426–441.
- Prezelj, I. (2002b). Konceptualizacija nacionalnih varnostnih interesov. Teorija in praksa 39 (4): 621–637.
- Purg, A. (1995). Obveščevalne službe. Ljubljana: ČZP Enotnost.
- Shah, S. (2001). P&G admits spies snooped on Unilever. The Independent. Dostopno na: <http://www.independent.co.uk/news/business/news/pampg-admits-spies-snooped-on-unilever-679819.html> (25. maj 2009).
- Smith, M. (2006). Private Intelligence Companies. How the Spooks Moved in on Big Business. Dostopno na: [http://money.cnn.com/magazines/fortune/fortune\\_archive/2004/08/23/379380/index.htm](http://money.cnn.com/magazines/fortune/fortune_archive/2004/08/23/379380/index.htm) (26. maj 2009).
- Steele, R. (1996). Private Enterprise Intelligence: Its Potential Contribution to National Security. V Intelligence Analysis and Assessment, ur. David A. Charters, Stuart Farson in Glenn P. Hastedt, 212–228. London, Portland: Frank Cass.
- Steele, R. (2002a). The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats. Carlisle: Strategic Studies Institute, U.S. Army War College.
- Svete, U. (2002). Vloga in pomen informacijske tehnologije v sodobnem asimetričnem vojskovanju. Magistrsko delo. Ljubljana: Fakulteta za družbene vede.

- Svete, U. (2006). Strateški značaj informacijsko-komunikacijske tehnologije u suvremenom međunarodnom okolišu. *Polemos: časopis za interdisciplinarna istraživanja rata i mira* 9 (2): 101–118. Zagreb: Hrvatsko sociološko društvo.
- Triglav, J. (1996). Informacijska revolucija. *Življenje in tehnika* 47: 27–39.
- Ulcej, D. (2008). Privatizacija obveščevalne dejavnosti. Diplomsko delo. Ljubljana: Fakulteta za družbene vede.
- Vrenko Peruško, I. (2004). Business intelligence: oči in ušesa uspešnih podjetij. Dostopno na: [http://www.gfk.si/4\\_2\\_lclank.php?cid=1210](http://www.gfk.si/4_2_lclank.php?cid=1210) (15. maj 2009).
- Whitehead, S. (2003). Corporate Counterintelligence – protecting business information. Dostopno na: <http://cbr.co.za/regular.aspx?pkIRegularId=1390> (25. maj 2009).
- Zalar, B. (1997). (Ne)legitimnost privatizacije državnega aparata prisile. V *Zasebno varovanje in detektivska dejavnost: dileme in perspektive*, ur. Andrej Anžič, 37–56. Ljubljana: Visoka policijsko-varnostna šola.